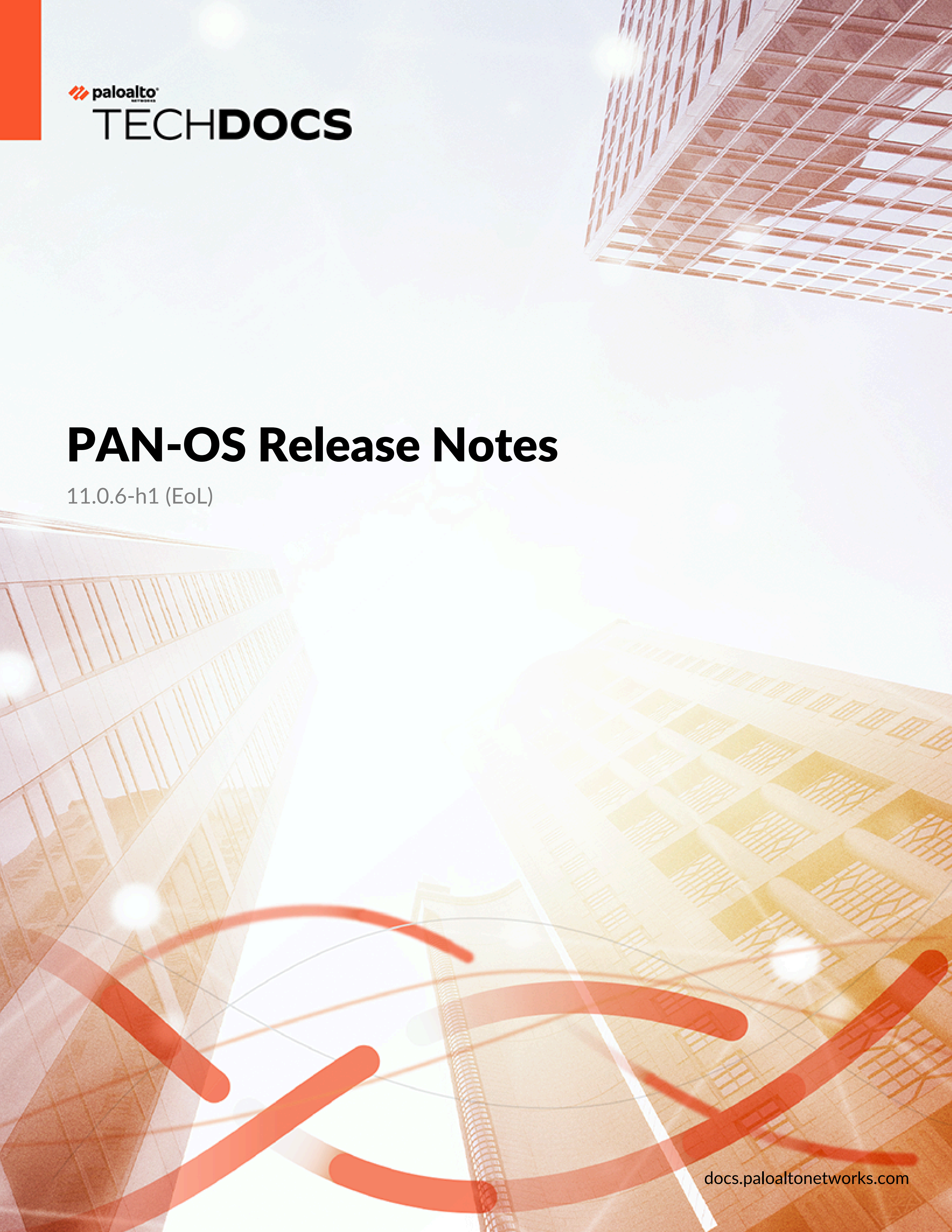
paloalto
TECHDOCS



PAN-OS Release Notes

11.0.6-h1 (EoL)

docs.paloaltonetworks.com

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

Last Revised

November 17, 2024

Table of Contents

Features Introduced in PAN-OS 11.0

Review new features introduced in Palo Alto Networks PAN-OS® 11.0 software.

Networking Features

New Networking Feature	Description
Software Cut Through Support for PA-400 and PA-1400 Series Firewalls (PAN-OS 11.0.4 and later 11.0 releases)	The PA-400 and PA-1400 Series firewalls have significantly improved latency.
PA-5420 Firewall Supports Additional Virtual Routers (PAN-OS 11.0.4 and later 11.0 releases)	The number of virtual routers supported on a PA-5420 firewall increased from 50 to 65. This increase allows you to have a virtual router for each virtual system on the firewall in the event that you configure more than 50 virtual systems.
Improved Throughput with Lockless QoS (PAN-OS 11.0.3 and later 11.0 releases)	The Palo Alto Networks QoS implementation now supports a new QoS mode called lockless QoS for PA-3410, PA-3420, PA-3430, PA-3440, PA-5410, PA-5420, PA-5430, and PA-5440 firewalls. For firewalls with higher bandwidth QoS requirements, the lockless QoS dedicates CPU cores to the QoS function that improves QoS performance, resulting in improved throughput and latency.
Increased Maximum Number of Security Zones for PA-1400 Series Firewalls (PAN-OS 11.0.2 and later 11.0 releases)	(PA-1400 Series firewalls only) The maximum number of security zones supported has increased from 50 to 150. The maximum number of security rules supported has increased from 1,500 to 5,000.
LSVPN Cookie Expiry Extension (PAN-OS 11.0.1 and later 11.0 releases)	You can now configure the cookie expiration period from 1 to 5 years, while the default remains as 6 months. The encrypted cookie stored on an Large Scale VPN (LSVPN) satellite expires after every 6 months. This causes the VPN tunnels associated with the satellite to go down, causing an outage until the satellite is re-authenticated to the LSVPN portal or gateway and a new cookie is generated. A re-authentication every six months causes administrative overhead, affecting productivity, network stability, and resources of the company. To reduce administrative overhead, we’ve extended the cookie expiration period from 6 months to 5 years.

New Networking Feature	Description
PPPoE Client Support on a Subinterface (PAN-OS 11.0.1 and later 11.0 releases)	The firewall extends PPPoE IPv4 client support to a subinterface so that the firewall can connect to an ISP that uses an IEEE 802.1Q VLAN tag on its PPPoE connections. The firewall as a PPPoE client receives its IPv4 address and other information from the PPPoE server. The firewall encapsulates PPPoE packets from a host in an 802.1Q frame before sending them to the ISP, and decapsulates PPPoE packets from the 802.1Q frame before sending them to the host.
Increased Maximum Number of Security Zones for PA-3400 Series Firewalls (PAN-OS 11.0.1 and later 11.0 releases)	(PA-3400 Series firewalls only) The maximum number of security zones supported on the PA-3410 and PA-3420 firewalls has increased from 40 to 200. The maximum number of security zones supported on the PA-3430 firewall has increased from 100 to 200.
Poll Timeout Improvement for PA-3400 and PA-5400 Series Firewalls (PAN-OS 11.0.1 and later 11.0 releases)	The PA-3400 and PA-5400 Series firewalls have improved latency when operating under low load.
Web Proxy (PAN-OS 11.0.0 and later 11.0 releases)	Some networks are designed around a proxy for compliance and other requirements. The Web Proxy capability available in PAN-OS 11.0 allows these customers to migrate to NGFW without changing their proxy network to secure web as well as non-web traffic. With web proxy available for both NGFW and Prisma Access, Palo Alto Networks helps you transition to a single, integrated security stack for web security across on-premises and cloud-delivered form factors. By configuring seamless synchronization between your on-premises proxy device and the cloud-based proxy, you can enable Prisma Access as a SASE solution for your SWG-based network architecture to ensure consistent policy application regardless of location.
DHCPv6 Client with Prefix Delegation	The firewall now supports a stateful DHCPv6 Client to obtain IPv6 addresses and other parameters. This feature also supports Prefix Delegation by assigning prefixes received from the DHCP server to configured pools. A prefix from the pool is distributed using SLAAC to a host-facing (inherited) interface.
IPSec Transport Mode	In addition to the default tunnel mode, you can now configure IPSec tunnels to use Transport Mode when encrypting host-to-host communications. Transport

New Networking Feature	Description
	mode encrypts only the payload while retaining the original IP header. You can use Transport mode to encrypt the management traffic with the most secure protocols.
Multicast Source Discovery Protocol on Advanced Routing Engine	The Advanced Routing Engine adds support for MSDP. MSDP interconnects multiple IPv4 PIM Sparse-Mode (PIM-SM) domains, enables the discovery of multicast sources in other PIM-SM domains, and reduces the complexity of interconnecting multiple PIM-SM domains by allowing PIM-SM domains to use an interdomain source tree.
BFD Support on PA-400 Series Firewalls	Bidirectional Forwarding Detection (BFD) support is extended to the PA-400 Series firewalls (PA-410, PA-440, PA-450, and PA-460 firewalls) for both the legacy routing engine and Advanced Routing Engine.
IPv4 and IPv6 Address Families Supported over a Single BGP Peering on Advanced Routing Engine	On the Advanced Routing Engine, BGP peer groups and peers now support both an IPv4 address family (AFI profile) for unicast SAFI and an IPv6 AFI profile for unicast SAFI over a single peering. This means that, regardless of whether the BGP local address and peer address are IPv4 or IPv6, the peering supports both IPv4 and IPv6 unicast routes being carried over a single BGP session that uses IPv4 or IPv6.
Power Over Ethernet (PoE)	PoE enables you to transfer electrical power from a supported firewall to a powered device. Using interfaces that have been configured for PoE, you can allocate power to multiple powered devices while still maintaining data transfer over an Ethernet connection. PoE is supported on many of the new models introduced with PAN-OS 11.0, including PA-1420, PA-1410, PA-445, and PA-415.
Persistent NAT for DIPP	Some applications, such as VoIP and video, use DIPP source NAT and may require STUN. DIPP NAT uses symmetric NAT, which may have compatibility issues with STUN. To alleviate those issues, persistent NAT for DIPP provides additional support for connectivity with such applications. When you enable persistent NAT for DIPP, the binding of a private source IP address and port to a specific public (translated) source IP address and port persists for subsequent sessions that arrive having that same original source IP address and port.

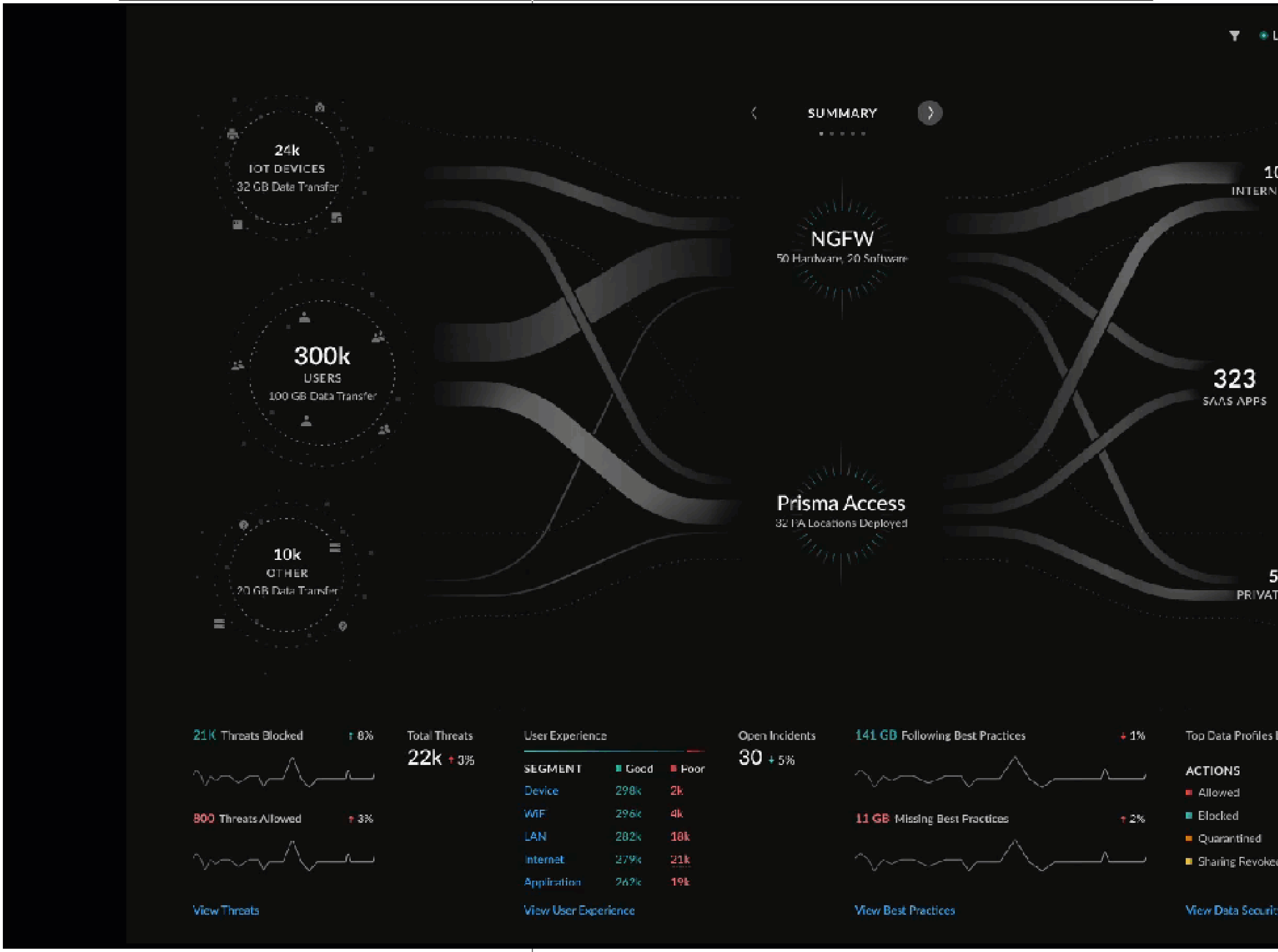
Panorama Features

New Panorama Feature	Description
Panorama Interconnect 2.0 PAN-OS 11.0.1 and later releases	Upgrade to Panorama Interconnect Plugin 2.0 is required to upgrade to PAN-OS 11.0. You must download the Panorama Interconnect Plugin 2.0.0 prior to install of PAN-OS 11.0.1 to successfully upgrade.
Zero Touch Provisioning 2.0.3 PAN-OS 11.0.1 and later releases	The Zero Touch Provisioning (ZTP) Plugin 2.0.3 release includes minor bug and performance fixes.
Admin-Level Commit with Policy Reordering PAN-OS 11.0.1 and later releases	You can perform admin-level commits even when there are pending changes that affect the order of a policy rulebase from other admins. This simplifies your configuration workflow because you don't have to coordinate commits with other administrators when your changes are unrelated to theirs and no longer requires you to wait for a Superuser admin to be available to do a full commit on Panorama.
Proactive BPA using AIOps for NGFW	The configuration commit processes on Panorama have been seamlessly integrated with the on-demand dynamic scale cloud plugin to perform BPA at the time of a commit and block it for your chosen set of checks. This allows you to fix any BPA violations in real-time and proceed with a clean bill of health. This smarter workflow eliminates any exposure that a compromised security posture could create.
Static Security Group Tag (SGT) for TrustSec plugin	The Panorama plugin for Cisco TrustSec now provides support for static SGT (Security Group Tags) retrieved from the Cisco ISE server. The static SGTs are used in the same way dynamic SGTs are currently used; IP addresses and tags are extracted and forwarded to the Panorama plugin framework, which then pushes them to the firewalls. Static SGTs can improve security posture when an endpoint does not authenticate through Cisco ISE.

Management Features

New Management Feature	Description
Skip Software Version Upgrade	You can now upgrade and downgrade standalone and Panorama managed devices running 10.1 or later more efficiently by skipping up to three software versions. You can skip either two major releases and one minor release, or one major release and two minor releases. The ability to skip multiple software releases during an upgrade or downgrade shortens the time needed for the maintenance window and enables you to take advantage of the latest PAN-OS innovations more quickly. This feature also enhances the capabilities of the multi-image download option and pre-install validation check, which reduces the number of steps in the process.
TLSv1.3 Support for Management Access	PAN-OS 11.0 introduces two management configuration options that let you define TLSv1.3 as your preferred TLS protocol and select a TLSv1.3 certificate. You can use the new settings to specify the TLS versions and certificates your management interface supports outside of SSL/TLS service profiles. For example, you can select `tlsv1.3_only` TLS mode for a faster, more secure connection that meets your regulatory requirements.
Multi-Vsys Capability for the PA-400 Series Firewalls	Multiple virtual systems featuring shared gateway support are now available for most PA-400 Series firewalls with a multi-vsys license. PA-440 firewalls support up to two virtual systems. PA-450 and PA-460 firewalls support up to five virtual systems.
Strata Cloud Manager Command Center	The Strata Cloud Manager Command Center is your new NetSec homepage; it is 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 how Prisma Access, your NGFWs, and your security services are protecting them.

New Management Feature	Description



SEGMENT	🟩 Good	🟥 Poor
Device	298k	2k
WiF	296k	4k
LAN	282k	18k
Internet	279k	21k
Application	262k	19k

The command center provides you with four different views, each with its own tracked data, metrics, and actionable insights to examine and interact with:

- **Summary:** A high-level look at all your network and security infrastructure. Monitor the traffic between your sources (users, IoT) and applications (private, SaaS), and see metrics onboarded security subscriptions.
- **Threats:** Dig deeper into anomalies on your network and block threats that are impacting your users. Review the traffic inspected on your network and see how threats are being detected and blocked

New Management Feature	Description
	around the clock by your Cloud-Delivered Security subscriptions. • **Operational Health:** Review incidents of degraded user experience on your network and see root-cause analysis of the issues and remediation recommendations. • **Data Security:** Find high-risk sensitive data and update data profiles to further secure your network. Review the sensitive data flow across your network and SaaS applications. When the command center surfaces an issue through one of these views that you should address or investigate (an anomaly, a security gap, a degraded user experience, something that impacts the security and health of your network), it provides a path to where you can take actions to further secure your network.
View Preferred and Base Releases of PAN-OS Software PAN-OS 11.0.5 and later 11.0 releases	The Panorama web interface now displays the preferred releases and the corresponding base releases of PAN-OS software. Before you upgrade or downgrade Panorama or PAN-OS, you can view the list of preferred and base releases and choose your preferred target PAN-OS release. Preferred releases offer the latest and the most advanced features and ensure stability and performance. When there are no preferred releases available, the corresponding base version is not displayed. If necessary, you can choose to view either preferred releases or base releases.

Certificate Management Features

Certificate Management Features	Description
Support for OCSP Verification through HTTP Proxy	If your network deployment includes a web proxy, you can now use the Online Certificate Status Protocol (OCSP) to check the validity of SSL/TLS certificates. The firewall forwards OCSP requests to your proxy server instead of directly to the OCSP responder. You'll need to configure an OCSP responder and specify OCSP as your certificate revocation status method.

Cloud Identity Features

New Cloud Identity Feature	Description
User Context for the Cloud Identity Engine	User Context for the Cloud Identity Engine provides unparalleled visibility into your user identification and device information (such as tags, quarantine lists, and mappings, which now includes IP-address-to-port number mappings from Terminal Server agents) and provides a simple yet precise way to redistribute that information to other firewalls and devices within your network through segmentation (for example, by region or use case). By enabling the service on your firewall and defining information distribution for your network segments in the Cloud Identity Engine, you can quickly locate critical information and ensure consistent user-based policy enforcement across your network. User Context represents the next expansion of User-ID in a unified interface on the Cloud Identity Engine and presents actionable user identity information at a glance.

Content Inspection Features

New Content Inspection Feature	Description
DNS Security Support for DoH (DNS-Over-HTTPS)	PAN-OS® can identify traffic contained in DoH (DNS-over-HTTPS) requests and apply DNS Security real-time protection measures. This allows you to secure all DoH traffic, which is quickly becoming the emerging standard of maintaining user privacy and data security, by leveraging the same DNS Security analytics used to defend your organization from a range of DNS-based threats.
Advanced Threat Prevention Support for Detecting Zero-Day Exploits	The Advanced Threat Prevention subscription now supports additional deep learning and heuristic analysis engines to prevent malicious zero-day Injection attacks (Inbound threats), such as SQLi and Command Injection attacks. These attacks target vulnerable applications that do not sufficiently validate, filter, or sanitize user-supplied data.
Support for Custom Layer 3 and Layer 4 Threat Signatures	PAN-OS® now supports user-defined custom threat signatures based on Layer 3 and Layer 4 header fields. This enables you to provide enhanced vulnerability coverage for old and/or deprecated TCP/IP stacks used in embedded devices, where signature protections are not readily available.

IoT Security Features

New IoT Security Feature	Description
IoT Security for Isolated Network Segments (PAN-OS 11.0.2 and later 11.0 releases)	You can deploy one or more Palo Alto Networks next-generation firewalls as hardened security telemetry gateways to logically connect firewalls in isolated network segments with Palo Alto Networks cloud-delivered security solutions. The security telemetry gateways block any attempted inbound internet connections to the isolated firewalls using either a single gateway or multiple gateways in a chain depending on your needs and the design of your network architecture.
IoT Security Policy Rule Recommendation Enhancements	New PAN-OS® and IoT Security configuration workflows make it easier to scale and manage policy rule recommendations. The names of recommended policy rules are now automatically generated. IoT Security automatically pushes activated policy rule sets to Panorama and next-generation firewalls. Panorama lets you import multiple rules at a time into multiple device groups, and firewalls let you import multiple rules at a time into your policy rulebase.
Improved DHCP Traffic Visibility for IoT Security	By extending DHCP traffic visibility further into your network, you can now discover and monitor even more devices than ever. IoT Security employs multiple methods to detect and monitor network activity and correlate it to individual devices. A particularly useful method is the examination of DHCP traffic, which allows IoT Security to associate dynamically assigned IP addresses with device MAC addresses and then add these devices to its inventory and track their network behavior. When it's difficult to route DHCP traffic in certain areas of the network to or through a firewall, there can be gaps in the coverage that IoT Security provides. To improve visibility into DHCP traffic that otherwise wouldn't reach the firewall, you can configure DHCP servers to send the firewall their server logs as syslog messages. The firewall then forwards the logs through the logging service to IoT Security.

Mobile Infrastructure Security Features

New Mobile Infrastructure Security Feature	Description
5G RADIUS Support for Intelligent Security (PAN-OS 11.0.2 and later)	Intelligent Security with RADIUS provides consistent information and identification for all subscribers, equipment, applications, and data based on context and subscriber activity. To correlate user equipment (UE) information with more types of 4G/5G traffic, the firewall can now inspect RADIUS traffic for enforcement of subscriber-level and equipment-level security policy. Intelligent Security with RADIUS allows enterprises to expand their zero-trust architecture to subscribers and equipment on 5G networks.
User Equipment (UE) to IP Address Correlation with PFCP for 5G Migration	Control and user plane separation (CUPS) architecture is a common configuration for networks undergoing transition from 4G/LTE to 5G; however, traffic inspection for both planes must be performed by the same firewall. User Equipment (UE) to IP Address Correlation with PFCP allows the firewall to extract user information and correlate it with the equipment ID or subscriber ID. It enables you to create granular security policies based on subscriber or equipment ID, as well as enhanced visibility through logging and reporting for applications and threats based on subscriber or equipment ID.

SD-WAN Features

SD-WAN features in PAN-OS 11.0.

New SD-WAN Feature	Description
Additional Private Link Types Support (PAN-OS 11.0.4 and later 11.0 releases)	The SD-WAN plugin 3.1.3 and later 3.1 releases provide four additional point-to-point private link types, **Private Link1**, **Private Link2**, **Private Link3**, and **Private Link4** along with the existing three private link types (**MPLS**, **Satellite**, **Microwave/Radio**) to configure in the SD-WAN Interface Profile. These private link types enable you to avail reliable providers for your remote regions to establish one to one connection with the overlay network and avoid provider outages.
Additional SD-WAN Hubs in VPN Cluster (PAN-OS 11.0.4 and later 11.0 releases)	The number of hubs to configure in a VPN cluster has been increased from 4 to 16. Only four of the 16 hubs can have the same hub priority within a VPN cluster due to ECMP.
SD-WAN IPv6 Basic Connectivity (PAN-OS 11.0.2 and later 11.0 releases)	The legacy routing engine now supports SD-WAN in a dual stack using IPv6 BGP loopback addresses for BGP peering; thus, you can establish IPv6 connectivity from the branch to the hub over an IPv4 SD-WAN tunnel. (IPv6 connectivity over DIA isn't supported.)
SD-WAN Plugin Support for Advanced Routing Engine	We have enhanced the SD-WAN plugin 3.1.0 to support logical routers for branches and hubs that use advanced routing engines. With SD-WAN plugin 3.1.0 configured with an advanced routing option, all SD-WAN related objects are automatically generated in logical routers rather than virtual routers. SD-WAN plugin 3.1.0 running PAN-OS 11.0 offers an advanced routing engine that relies on industry-standard configuration methodology, which facilitates the administrator tasks. It allows the creation of profiles that are used for different functions (such as, filtering, redistribution, and metric changes), all of which can be used across logical routers. These profiles provide finer granularity to filter routes for each dynamic routing protocol

New SD-WAN Feature	Description
	and improve route redistribution across multiple protocols.

Virtualization Features

New Virtualization Feature	Description
Hyperscale Security Fabric (HSF) 1.0 on CN-Series	With CN-Series Hyperscale Security Fabric (HSF) 1.0, you can now create a cluster of containerized next-gen firewalls that deliver a highly scalable and resilient next-gen firewall solution, eliminating the dependency on external load balancers for Mobile Service Providers deploying 5G networks.
Advanced Routing Engine Support on CN-Series	The Advanced Routing Engine is now supported on the CN-Series.
Key Management Service (KMS) Support for VM-Series	This release enables cloud native key managers, Azure Key Vault and AWS Secrets Manager, to store certificates for VM-Series firewalls.
Software Cut-through Based Offload on Software Firewalls	You can now configure software cut-through based offload on the VM-Series and CN-Series firewall. With the software cut-through based Intelligent Traffic Offload (ITO) service, the CN-Series firewall eliminates the tradeoff between network performance, security, and cost. The software cut-through based offload supports the GTP-U tunnel protocol. In the CN-Series, only the CN-Series as a Kubernetes CNF mode of deployment supports software cut-through based ITO. For more information, see Software Cut-through Based Offload on CN-Series Firewall.

Advanced WildFire Features

New WildFire Feature	Description
Intelligent Run-time Memory Analysis	Palo Alto Networks Advanced WildFire is a new cloud-based subscription service that detects and prevents modern evasive malware from entering your network by leveraging a new advanced analysis engine. Advanced WildFire is built on an extensible cloud architecture that operates in the WildFire global cloud to stealthily observe malware and apply the latest deep learning-derived analysis techniques, such as intelligent run-time memory analysis, dependency emulation, malware family fingerprinting, malware configuration file analysis, and more, to uncover and determine the true nature of a sample as it passes through your network. Observed malware threats generate WildFire signatures to identify and protect against future infections.
Hold Mode for WildFire Real Time Signature Lookup (Available in PAN-OS 11.0.2 and later)	You can now configure the firewall to hold packets for unknown files when performing WildFire real time signature lookups to prevent the first transfer of known malware.

GlobalProtect Features

The following table describes new GlobalProtect features introduced in PAN-OS 11.0. For features related to the GlobalProtect app, see the GlobalProtect App 6.1 Release Notes.

New GlobalProtect Feature	Description
End-user Notification about GlobalProtect Session Logout	You can now enable and customize end-user notifications about expiry of GlobalProtect app sessions on the gateway. These notifications inform the end users in advance when their app sessions are about to expire due to inactivity or expiry of the login lifetime and lets them know how much time is left before the app gets disconnected, preventing unexpected and abrupt app logout.

Hardware Features

New Hardware Feature	Description
PA-415 and PA-445 Firewalls	The PA-415 and PA-445 firewalls offer an improved price to performance ratio with features such as Power Over Ethernet (PoE) capability, fiber ports, higher scalability, and enhanced boot times.
PA-1400 Series Firewalls	The PA-1410 and PA-1420 are intended for distributed enterprises, branches, and small to mid-sized businesses. These models feature Power Over Ethernet (PoE) capability, power redundancy, and Multi-Gig ports.
PA-5440 Firewall	The PA-5440 is the highest scale fixed form-factor firewall that Palo Alto Networks currently offers. The PA-5440 can process more sessions and features higher threat capabilities.

Enterprise Data Loss Prevention Features

New Enterprise DLP Feature	Description
File Type Include or Exclude List for Data Filtering Profiles Requires PAN-OS 11.0.2 and DLP plugin 4.0.1	Enterprise Data Loss Prevention (E-DLP) now supports creating a file type include or exclude list for data filtering profiles configured for file-based inspection. This allows you to select one of two modes: • **Inclusion Mode**—Allow only specified file types be scanned by Enterprise DLP. • **Exclusion Mode**—Allow all supported files to be scanned by Enterprise DLP by default but excluding the file types you specify. Exclusion Mode includes True File Type Support and does not rely on file extensions to determine file types.
Enterprise DLP Plugin Upgrade Requires DLP plugin 4.0.0	Upgrade to Enterprise DLP Plugin 4.0 is required to upgrade to PAN-OS 11.0. The minimum supported PAN-OS version is PAN-OS 11.0. You must download the Enterprise DLP Plugin 4.0 prior to install of PAN-OS 11.0 to successfully upgrade.

Changes to Default Behavior

Review the changes to default behavior for PAN-OS 11.0.

- Changes to Default Behavior in PAN-OS 11.0

Changes to Default Behavior in PAN-OS 11.0

The following table details the changes in default behavior upon upgrade to PAN-OS® 11.0. You may also want to review the Upgrade/Downgrade Considerations before upgrading to this release.

Feature	Change
Minimum System Memory Requirement for the Panorama Virtual Appliance	Palo Alto Networks has increased the recommended Panorama virtual appliance memory requirement to a minimum of 64GB, up from 32GB. This impacts Panorama virtual appliances in Panorama and Log Collector mode to avoid any logging, management, and operational performance issues related to an under-provisioned Panorama virtual appliance. For new Panorama virtual appliance deployments, Palo Alto Networks recommends deploying the virtual machine with a minimum of 64GB. For existing Panroama virtual appliance deployments, See Increase the CPUs and Memory of the Panorama Virtual Appliance to increase the memory for an existing Panorama virtual appliance after successful upgrade to PAN-OS 11.0.
Custom Syslog Format	The maximum characters supported for a custom syslog format (**Device** > **Server Profiles** > **Syslog** and **Panorama** > **Server Profiles** > **Syslog**) is increased to 4,096 characters.
Panorama Memory Management	Rather than automatically restarting the Panorama management server, a critical system log (**Monitor** > **Logs** > **System**) is now generated to alert that a Panorama reboot (**Panorama** > **Setup** > **Operations**) is required when the `configd` process responsible for configuration management and Panorama operations encounters memory issues
Test SCP Server Connection	To test the SCP server connection when you schedule a configuration export (**Panorama** > **Schedule Config Export**) or log export (**Device** > **Scheduled Log Export**), a new pop-up window is displayed requiring you to enter the SCP server clear text**Password** and **Confirm Password** to test the SCP server connection and enable the secure transfer of data.

Feature	Change
	You must also enter the clear text SCP server **Password** and **Confirm Password** when you test the SCP server connection from the firewall or Panorama CLI. `admin>test scp-server-connection initiate <ip> username <username> password <clear-text-password>`
Panorama Management of Multi-Vsys Firewalls Upgrade to PAN-OS 11.0 using Skip Software Version Upgrade only	For multi-vsys firewalls managed by a Panorama managed server, configuration objects in the Shared device group are now pushed to a Panorama Shared configuration context for all virtual systems rather than duplicating the shared configuration to each virtual system to reduce the operational burden of scaling configurations for multi-vsys firewalls. As a result, you must delete or rename any locally configured firewall **Shared** object that has an identical name to an object in the **Panorama Shared** configuration. Otherwise, configuration pushes from Panorama fail after the upgrade and display the error `<object-name> is already in use`. The following configurations cannot be added to the Shared Panorama location and are replicated to the Panorama location of each vsys of a multi-vsys firewall. • Pre and Post Rules • External Dynamic Lists (EDL) • Security Profile Groups • HIP objects and profiles • Custom objects • Decryption profiles • SD-WAN Link Management Profiles
	Palo Alto Networks recommends that if a multi-vsys firewall is managed by Panorama, then all vsys configurations should be managed by Panorama. This helps avoid commit failures on the managed multi-vsys firewall and allows you to take

Feature	Change
	advantage of optimized shared object pushes from Panorama.

Limitations

Review limitations around Palo Alto Networks PAN-OS® 11.0 software.

- Limitations in PAN-OS 11.0

Limitations in PAN-OS 11.0

The following are limitations associated with PAN-OS 11.0.

Issue ID	Description
—	The following limitations apply for on-premises Explicit Proxy: • On-premises Explicit Proxy does not support multi-tenancy. • On-premises Explicit Proxy supports authentication using SAML and Kerberos. • On-premises Explicit Proxy requires decryption (TLS 1.3 is recommended). • On-premises Explicit Proxy requires port 8080. • On-premises Explicit Proxy requires PAC files to direct traffic to the on-premises Explicit Proxy. • On-premises Explicit Proxy supports customer-based hosting for their individual PAC files. • On-premises Explicit Proxy supports inbound proxy chaining with XFF and XAU HTTP headers. • On-premises Explicit Proxy supports HTTP/2 for Kerberos only; HTTP/2 for SAML is not supported in this release.
—	In Advanced Routing mode, BGP peer groups and peers allow IPv6 NLRI to be transported over an IPv6 MP-BGP peer and allow IPv6 NLRI to be transported over an IPv4 MP-BGP peer. If you want to use IPv4 multicast, you are limited to only IPv4 with that peer. The firewall does not support SAFI IPv6 multicast at all.
PLUG-10942	For CN-Series deployments using the Advanced Routing Engine with the Kubernetes 3.0.0 plugin, you must configure Advanced Routing manually on the template stack: **1.** Set the flag **`PAN_ADVANCED_ROUTING:"true"`** in the pan-cn-mgmt-configmap-0.yaml file. **2.** Manually enable Advanced Routing on the Panorama template, then commit and push the configuration.
PAN-265738	NAT is not configurable when HA clusters are configured. HA clusters do not support NAT.

Issue ID	Description
PAN-247465	(PA-7080 only) The firewall does not support Aquantia 10G SFP transceivers.
PAN-246825	ECMP is not supported for equal-cost routes where one or more of those routes has a virtual router or logical router as the next hop. None of the equal-cost routes will be installed in the Forwarding Information Base (FIB).
PAN-218067	By default, Next Generation firewalls and Panorama attempt to fetch the device certificate or Panorama device certificate with each commit even when the firewall is not using any Palo Alto Networks cloud service. You can prevent the firewall from attempting to fetch the device certificate for the following firewalls: • M-300 appliance • M-500 appliance • PA-400 Series firewalls • PA-1400 Series firewalls • PA-3400 Series firewalls • PA-5400 Series firewalls • PA-5450 firewall To disable, log in to the firewall CLI or Panorama CLI and enter the following command: `admin> request certificate auto-fetch disable`
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync on the peer firewall. This causes the HA settings to display as overridden despite no config override occurring.
PAN-215869	PAN-OS logs (**Monitor** > **Logs**) experience a significant delay before they are displayed if NetFlow (**Device** > **Server Profiles** > **NetFlow**) is enabled on an interface (**Network** > **Interface**). This may result in log loss if

Issue ID	Description
	the volume of delayed logs exceeds the logging buffer available on the firewall. The following firewalls are impacted: • PA-400 Series Firewalls • PA-800 Series Firewalls • PA-1400 Series Firewalls • PA-3200 Series Firewalls • PA-3400 Series Firewalls
PAN-205932	DHCPv6 Client with Prefix Delegation is currently incompatible with GlobalProtect. You cannot configure GP gateways with dynamic IPv6 addresses.
PAN-205166	(PA-440, PA-450, and PA-460 firewalls only) The CLI does not display system information about the power supply when entering the `show system environmentals` command. As a result, the CLI cannot be used to view the current status of the power adapter. **Workaround:** To manually interpret the status of the firewall's power adapter, verify that your power cable connections are secure and that the LED on the power adapter is on. If the LED is not illuminated even though the power cable connections are secure, your power adapter has failed.
PAN-197412	In IPSec transport mode, the traffic does not flow if you configure BGP routes in a tunnel interface. While using IPSec transport mode for BGP routes, configure the BGP routes on a physical interface (for example, ethernet 1/1) and not the tunnel interface. While IPSec tunnel mode for BGP routes works with the tunnel interface, IPSec transport mode for BGP routes works with the physical interface only.
PAN-196530	On the PA-5440 firewall, the valid range to configure the maximum number of site-to-site VPN tunnels is from 0 to 10,000. `admin@PA-5440# set import resource max-site-to-site-vpn-tunnels <0-10000>`

Issue ID	Description
PAN-192679	(PA-415 and PA-445 firewalls) The hardware can detect the presence of a power adapter but does not detect voltage or functionality. As a result, the firewall's Alarm feature is unavailable to the power supply and is only raised when the device reaches temperature limits. Furthermore, the firewall does not display power supply details in system logs or the CLI.

Associated Content and Software Versions

Review information about the associated content and software versions for Palo Alto Networks PAN-OS® 11.0 software.

- Associated Content and Software Versions for PAN-OS 11.0
- WildFire Analysis Environment Support for PAN-OS 11.0

Associated Content and Software Versions for PAN-OS 11.0

The following minimum software and content release versions are compatible with PAN-OS 11.0. To see a list of the next-generation firewall models that support PAN-OS 11.0, see the Palo Alto Networks® Compatibility Matrix.

Palo Alto Networks Software or Content Release Version	Minimum Compatible Version with PAN-OS 11.0
Panorama	11.0
User-ID Agent	11.0
Terminal Services (TS) Agent	11.0
GlobalProtect App	6.0
Applications and Threats Content Release Version	8635
SD-WAN Plugin	If you have installed the SD-WAN plugin, PAN-OS 11.0.1 requires the 3.1.1 plugin.

WildFire Analysis Environment Support for PAN-OS 11.0

The following WildFire guest VM images (analysis environments) are supported in the PAN-OS 11.0 release of WildFire. To upgrade the WildFire appliance, refer to: Upgrade a WildFire Appliance

WildFire Analysis Environment	WildFire VM ID	WildFire Appliance Guest VM Filename	Minimum Compatible PAN-OS Version
Windows XP (Adobe Reader 11, Flash 11, Office 2010)	vm-3	WFWinXpAddon3_m-1.0.1.xpaddon3	10.2.2 and later
Windows 7 x64 SP1 (Adobe Reader 11, Flash 11, Office 2010)	vm-5	WFWin7_64Addon1_m-1.0.1.7_64addon1	10.2.2 and later
Windows XP (Internet Explorer 8, Flash 11, Elink analysis support)	vm-6**	WFWinXpGf_m-1.0.1.xpgf	10.2.2 and later
Windows 10 x64 (Adobe Reader 11, Flash 11, Office 2010)	vm-7	WFWin10Base_m-1.0.1.10base	10.2.2 and later

- ** This WildFire guest VM image comes preinstalled and is not available on the Palo Alto Networks Support Portal for download.*
- *** This WildFire analysis environment is not selectable through the WildFire appliance CLI.*

PAN-OS 11.0.6 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.6.

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.

- PAN-OS 11.0.6 Known Issues
- PAN-OS 11.0.6-h1 Addressed Issues
- PAN-OS 11.0.6 Addressed Issues

PAN-OS 11.0.6 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.6. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-250062	Device telemetry might fail at configured intervals due to bundle generation issues.
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-252744	After upgrading PA-3200 Series, PA-5200 Series, or PA-7000 Series firewalls that are equipped with OCTEON 7x00 dataplane chips to PAN-OS 11.0.4 or 11.0.4-h1, the firewall might see continuous crashes, reboot repeatedly, and/or go into a non-functional state. **Workaround:** If you have already upgraded to one of those releases, downgrade to an earlier release or upgrade to PAN-OS 11.0.4-h2.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-234929	The tabs in the **ACC**, such as **Network Activity**, **Threat Activity**, and **Blocked Activity**, may not display any data when you apply a Time filter for the Last 15 minutes, Last Hour, Last 6 Hours, or Last 12 Hours. With the Last 24 Hours filter, the data displayed may not be accurate. Additionally, reports run against summary logs may not display accurate results.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.

Issue ID	Description
PAN-233677	(PA-3410, PA-3420, PA-3430, PA-3440, PA-5410, PA-5420, PA-5430, and PA-5440 firewalls) By enabling Lockless QoS feature, a slight degradation in App-ID and Threat performance is expected.
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.
PAN-220176	(PAN-OS 11.0.1-h2 hotfix) System process crashes might occur with VoIP traffic when NAT is enabled with Persistent Dynamic IP and Port settings.
PAN-216314	Upon upgrade or downgrade to or from PAN-OS 10.1.9 or 10.1.9-h1, offloaded application traffic sessions may disconnect after a period of time even if a session is active. The disconnect occurs after the application's default session timeout value is exceeded. This behavior affects only PAN-OS 10.1.9 and 10.1.9-h1. If you are on PAN-OS 10.1.9 and 10.1.9-h1, please use the following workaround. If you have already upgraded or downgraded to another PAN-OS version, use the following workaround in that version. **Workaround:** Run the CLI command **`debug dataplane internal pdt fe100 csr wr_sem_ctrl_ctr_scan_dis value 0`** to set the value to zero (0).
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`

Issue ID	Description
PAN-212978	The Palo Alto Networks firewall stops responding when executing an SD-WAN debug operational CLI command.
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are automatically unselected and any new tag created is applied to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207442	For M-700 appliances in an active/passive high availability (**Panorama** > **High Availability**) configuration, the `active-primary` HA peer configuration sync to the `secondary-`

Issue ID	Description
	`passive` HA peer may fail. When the config sync fails, the job Results is `Successful` (**Tasks**), however the sync status on the **Dashboard** displays as `Out of Sync` for both HA peers. **Workaround**: Perform a local commit on the `active-primary` HA peer and then synchronize the HA configuration. **1.** Log in to the Panorama web interface of the `active-primary` HA peer. **2.** Select **Commit** and **Commit to Panorama**. **3.** In the `active-primary` HA peer **Dashboard**, click **Sync to Peer** in the High Availability widget.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy. This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log forwarding to the disconnected Dedicated Log Collector is not impacted. **Workaround:** Restart the `mgmtsrvr` process on the Dedicated Log Collector. **1.** Log in to the Dedicated Log Collector CLI. **2.** Confirm the Dedicated Log Collector is disconnected from Panorama. `admin> show panorama-status` Verify the `Connected` status is no.

Issue ID	Description
	3. Restart the `mgmtsrvr` process. `admin> debug software restart process management-server`
PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. - DLP cloud service - Advanced Threat Protection inline cloud analysis service - Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204689	Upon upgrade to PAN-OS 11.0.1, the following GlobalProtect settings do not work: - **Allow user to disconnect GlobalProtect App** > **Allow with Passcode** - **Allow user to Disable GlobalProtect App** > **Allow with Passcode** - **Allow User to Uninstall GlobalProtect App** > **Allow with Password**
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with

Issue ID	Description
	vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector.

Issue ID	Description
	Workaround: Restart the log receiver service by running the following CLI command: `debug software restart process log-receiver`
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if: • A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. • A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types: **1.** Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. **2.** Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report.

Issue ID	Description
	3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.6-h1 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.6 Addressed Issues

Issue ID	Description
PAN-254181	(CN-Series firewalls only) Fixed an issue where firewall pods and application pods repeatedly restarted.
PAN-253400	Fixed an issue where the *logrcvr* process stopped responding.

PAN-OS 11.0.5 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.5.

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.

- PAN-OS 11.0.5 Known Issues
- PAN-OS 11.0.5-h2 Addressed Issues
- PAN-OS 11.0.5-h1 Addressed Issues
- PAN-OS 11.0.5 Addressed Issues

PAN-OS 11.0.5 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.5. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-250062	Device telemetry might fail at configured intervals due to bundle generation issues.
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-252744	After upgrading PA-3200 Series, PA-5200 Series, or PA-7000 Series firewalls that are equipped with OCTEON 7x00 dataplane chips to PAN-OS 11.0.4 or 11.0.4-h1, the firewall might see continuous crashes, reboot repeatedly, and/or go into a non-functional state. **Workaround:** If you have already upgraded to one of those releases, downgrade to an earlier release or upgrade to PAN-OS 11.0.4-h2.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-234929	The tabs in the **ACC**, such as **Network Activity**, **Threat Activity**, and **Blocked Activity**, may not display any data when you apply a Time filter for the Last 15 minutes, Last Hour, Last 6 Hours, or Last 12 Hours. With the Last 24 Hours filter, the data displayed may not be accurate. Additionally, reports run against summary logs may not display accurate results.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.

Issue ID	Description
PAN-233677	(PA-3410, PA-3420, PA-3430, PA-3440, PA-5410, PA-5420, PA-5430, and PA-5440 firewalls) By enabling Lockless QoS feature, a slight degradation in App-ID and Threat performance is expected.
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.
PAN-220176	(PAN-OS 11.0.1-h2 hotfix) System process crashes might occur with VoIP traffic when NAT is enabled with Persistent Dynamic IP and Port settings.
PAN-216314	Upon upgrade or downgrade to or from PAN-OS 10.1.9 or 10.1.9-h1, offloaded application traffic sessions may disconnect after a period of time even if a session is active. The disconnect occurs after the application's default session timeout value is exceeded. This behavior affects only PAN-OS 10.1.9 and 10.1.9-h1. If you are on PAN-OS 10.1.9 and 10.1.9-h1, please use the following workaround. If you have already upgraded or downgraded to another PAN-OS version, use the following workaround in that version. **Workaround:** Run the CLI command **`debug dataplane internal pdt fe100 csr wr_sem_ctrl_ctr_scan_dis value 0`** to set the value to zero (0).
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`

Issue ID	Description
PAN-212978	The Palo Alto Networks firewall stops responding when executing an SD-WAN debug operational CLI command.
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are automatically unselected and any new tag created is applied to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207442	For M-700 appliances in an active/passive high availability (**Panorama** > **High Availability**) configuration, the `active-primary` HA peer configuration sync to the `secondary-`

Issue ID	Description
	`passive` HA peer may fail. When the config sync fails, the job Results is `Successful` (**Tasks**), however the sync status on the **Dashboard** displays as `Out of Sync` for both HA peers. **Workaround**: Perform a local commit on the `active-primary` HA peer and then synchronize the HA configuration. 1. Log in to the Panorama web interface of the `active-primary` HA peer. 2. Select **Commit** and **Commit to Panorama**. 3. In the `active-primary` HA peer **Dashboard**, click **Sync to Peer** in the High Availability widget.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy. This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log forwarding to the disconnected Dedicated Log Collector is not impacted. **Workaround:** Restart the `mgmtsrvr` process on the Dedicated Log Collector. 1. Log in to the Dedicated Log Collector CLI. 2. Confirm the Dedicated Log Collector is disconnected from Panorama. `admin> show panorama-status` Verify the `Connected` status is `no`.

Issue ID	Description
	3. Restart the `mgmtsrvr` process. `admin> debug software restart process management-server`
PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. - DLP cloud service - Advanced Threat Protection inline cloud analysis service - Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204689	Upon upgrade to PAN-OS 11.0.1, the following GlobalProtect settings do not work: - **Allow user to disconnect GlobalProtect App** > **Allow with Passcode** - **Allow user to Disable GlobalProtect App** > **Allow with Passcode** - **Allow User to Uninstall GlobalProtect App** > **Allow with Password**
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with

Issue ID	Description
	vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector.

Issue ID	Description
	Workaround: Restart the log receiver service by running the following CLI command: `debug software restart process log-receiver`
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if: • A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. • A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types: 1. Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. 2. Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report.

Issue ID	Description
	3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.5-h2 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.5-h1 Addressed Issues

Issue ID	Description
PAN-261540	(PA-3400 Series firewalls only) Fixed an issue where the firewall did not fully reboot after upgrading to PAN-OS 11.0.5.

PAN-OS 11.0.5 Addressed Issues

Issue ID	Description
PAN-255868	(PA-3400 Series firewalls only) Fixed an issue where the firewall entered maintenance mode after enabling kernel data collection during the silent reboot.
PAN-255577	Fixed an issue where push scope changes remained empty and **Edit selections > OK** did not work for admin-based users after upgrading Panorama.
PAN-253317	(VM-Series firewalls on Microsoft Azure environments only) Fixed an issue where you were unable to log in to the firewall after a private data reset.
PAN-251563	Added CPLD enhancement to capture external power issues.
PAN-251013	Fixed an issue on the web interface where the **Virtual Router** and **Virtual System** configurations for the template incorrectly showed as **none**.
PAN-249019	Fixed an issue where the *all_pktproc* process stopped responding, which caused the firewall to become unresponsive.
PAN-248427	Fixed an issue where push operations took longer than expected to complete.
PAN-248105	Fixed an issue where the GlobalProtect SSL VPN tunnel immediately disconnected due to a keep-alive timeout.
PAN-247403	(Panorama virtual appliances only) Fixed an issue where the push scope CLI command took longer than expected, which caused the web interface to be slow.
PAN-246772	Fixed an issue on the firewall where the dataplane went down due to a path monitor failure caused by an OOM condition related to the *pan_task* process.
PAN-246431	Fixed an issue where a **Push to Device** operation remained at the state **None** when performing a selective push to device groups and templates that included both connected and disconnected firewalls.
PAN-246215	Fixed an issue where the sleep time for a suspended *pan_task* process caused configuration and policy updates to be blocked.

Issue ID	Description
PAN-245850	Fixed an issue on Panorama appliances in active/passive HA configurations where the firewalls entered an HA out-of-sync status and jobs failed on the passive appliance with the error message `Could not merged running config from file`.
PAN-245125	(VM-Series firewalls in Microsoft Azure environments only) Fixed an issue where file descriptors were not closed due to invalid configurations.
PAN-245041	Fixed an issue where the WF-500 appliance returned an error verdict for every sample in FIPS mode.
PAN-244907	Fixed an issue where ports did not go down when moving from an active state to a suspended state.
PAN-244894	Fixed an issue where turning off *mprelay* logging caused *mprelay* heartbeat failure.
PAN-244836	A knob was introduced to toggle the default behavior of BGP in the Advanced Routing stack to not suppress duplicate updates. By default, the prefix updates are suppressed for optimization.
PAN-244746	Fixed an issue where changes committed on Panorama were not reflected on the firewall after a successful push.
PAN-244622	Fixed an issue where FIB repush did not work with Advanced Routing enabled.
PAN-244548	Fixed an issue where ECMP sessions changed destination MAC addresses mid-session, which caused connections to be reset.
PAN-244227	Fixed an issue where inconsistent FIB entries across the dataplane were not detected.
PAN-243463	Fixed an issue where high Enhanced Application log traffic used excess system resources and caused processes to not work.
PAN-242309	Fixed an issue where a higher byte count (s2c) was observed for DNS-Base application.
PAN-241018	(VM-Series firewalls in Microsoft Azure environments only) Fixed a Data Plane Development Kit (DPDK) issue where interfaces remained in a link-down stage after an Azure hot plug event.
PAN-240596	Fixed an issue where *all_task* stopped responding due to an invalid memory address.

Issue ID	Description
PAN-240477	Fixed a temporary hardware issue that caused PAN-SFP-PLUS-CU-5M to not be able to link up on PA-3400 and PA-1400 Series firewalls.
PAN-240174	Fixed an issue where, when LSVPN serial numbers and IP address authentication were enabled, IPv6 address ranges and complete IPv6 addresses that were manually added to the IP address allow or exclude list were not usable after a restart of the *gp_broker* process or the firewall.
PAN-239662	Fixed an issue where the NSSA default route from the firewall was not generated to advertise even though the backbone area default route was advertised during a graceful restart.
PAN-239337	Fixed an issue where the log_index was suspended and corrupted BDX files flooded the index_log.
PAN-238625	Fixed an issue where, when the physical interface went down, the SD-WAN Ethernet connection state still showed **UP/path-monitor** due to the Active URL SaaS monitor connection state remaining UP/path-monitor.
PAN-238610	Fixed an issue with the Panorama virtual appliance where, after the *mgmtsrvr* restarted on the passive appliance, stale IP address tags were pushed to the connected firewalls with the message `clear all registered ip addresses`.
PAN-238592	(PA-3410 firewalls only) Fixed an issue where the firewall did not boot up after upgrading due to a TPM lockout condition that persisted for over 24 hours.
PAN-237991	Fixed an issue where the log collector sent fewer logs than expected to the syslog server.
PAN-237657	Fixed an issue with 100% CPU utilization in the *varrcvr* process that occurred during an incremental WildFire update.
PAN-237614	Fixed an issue on Panorama where the API command `request system disk add` failed.
PAN-237208	Fixed an issue where the *reportd* process stopped and the firewall rebooted.
PAN-236261	Fixed an issue where a proxy server was used for external dynamic list communication even when the dataplane interface was configured through service routes.

Issue ID	Description
PAN-236244	Fixed an issue where you were unable to select authentication profiles via the web interface.
PAN-235807	Fixed an issue where static ND entries were not reachable after a reboot.
PAN-235585	Fixed an issue where, when custom signatures and predefined signatures shared the same literal pattern part, the custom signature caused an incorrect calculation for the length of the predefined signature, which resulted in App-ID not detecting correctly.
PAN-234489	Fixed an issue where a User Principle Name (UPN) was incorrectly required in the pre-logon machine certificate.
PAN-234169	Fixed an issue where downloading files failed or was slower than expected due to malware scanning even when the session was matched to a Security policy rule with no Anti-Virus profile attached.
PAN-233684	Fixed an issue on Panorama where **Push to Devices** or **Commit and Push** operations took longer than expected on the web interface.
PAN-233207	Fixed an issue where the *configd* process stopped responding when a partial configuration revert operation was performed.
PAN-231439	Fixed an issue where, when a VoIP call using dynamic IP and NAT was put on hold, the audio became one-way due to early termination of NAT ports.
PAN-229832	Fixed an intermittent issue where MLAV and URL cloud connectivity were lost.
PAN-228624	Fixed an issue where FIB entries were deleted due to a *sysd* process connection error.
PAN-228386	Fixed an issue with session caching where the *reportd* process stopped responding due to null values.
PAN-228043	Fixed an issue on firewalls on active/active HA configurations where packets dropped during commit operations when forwarding traffic via an HA3 link when an Aggregate Ethernet interface or data interface was used as an HA3 link.
PAN-227641	Fixed an issue where **Preview Changes** and **Change Summary** when saving changes did not open a new window when clicked.

Issue ID	Description
PAN-227233	Fixed an issue where the combination signature aggregation criteria in a Vulnerability Protection profile was incorrectly blank even though a value was set.
PAN-226489	Fixed an issue where Panorama was unable to push scheduled Dynamic Updates to firewalls with the error message `Failed to add deploy job. Too many (30) deploy jobs pending for device`.
PAN-226260	Fixed an issue where support for CBC ciphers with some authentication algorithms was only available in FIPS mode.
PAN-226108	Fixed an issue where the *masterd* process was unable to start or stop the *sysd* process.
PAN-225963	Fixed an issue where the IP address-to-user mapping was not correct.
PAN-225228	Fixed an issue where filtering Threat logs using any value under **THREAT ID/NAME** displayed the error **Invalid term**.
PAN-223418	Fixed an issue where heartbeats to the *brdagent* process were lost, resulting in the process not responding, which caused the firewall to reboot.
PAN-222253	Fixed an issue on Panorama where policy rulebase reordering under **View Rulebase by Groups** (**Policy > <policy-rulebase>**) did not persist if you reordered the policy rulebase by dragging and dropping individual policy rules and then moved the entire tag group.
PAN-221571	Fixed an issue on the web interface where the Security policy rule hit count remained at 0 for some rules even though the Traffic logs showed live hits.
PAN-221041	Fixed an issue where the following error message was seen frequently in the system logs: `Clearing snmpd.log due to log overflow`.
PAN-221003	Fixed an issue where you were unable to uncheck firewalls in HA configurations from the device group when **Group HA Peers** was enabled.
PAN-220640	(PA-220 firewalls only) Fixed an issue where the firewall CPU percentage was miscalculated, and the values that were displayed were incorrect.

Issue ID	Description
PAN-220601	Fixed an issue with missing logs when one log collector in a log Collector Group became unreachable.
PAN-219690	Fixed an issue where GlobalProtect authentication failed when authentication was SAML with CAS and the portal was resolved with IPv6.
PAN-218521	M-600 Appliances in Log Collector mode only) Fixed an issue where Panorama continuously rebooted and became unresponsive, which consumed excessive logging disk space and prevented new log ingestion.
PAN-218331	Fixed an issue where you were unable to export or download packet captures from the firewall when context switching from Panorama.
PAN-217674	Fixed an issue where RADIUS authentication failed when the destination route of the service route was configured with an IPv4 address with more than 14 characters.
PAN-217489	Fixed an issue with firewalls in active/passive HA configurations where the passive firewall MAC flapping occurred when the passive firewall was rebooted.
PAN-215905	(PA-3400 Series firewalls only) Fixed an issue where silent packet drops were observed on interfaces.
PAN-215430	Fixed an issue where dynamic IP address NAT with SIP intermittently failed to convert RTP Predict sessions.
PAN-214682	Fixed an issue where the firewall sent incorrectly encoded the `supported_groups` extension in the Client Hello when acting as a forward proxy with decryption profile max version TLSv1.2.
PAN-213173	Fixed an issue where **Preview Changes** under **Scheduled Pushes** did not launch the **Change Preview** window.
PAN-212553	Fixed an issue where the *ikemgr* process stopped responding due to memory corruption, which caused VPN tunnels to go down.
PAN-209574	Fixed an issue with HTTP2 traffic where downloading large files did not work when decryption was enabled.
PAN-207972	Fixed an issue on the web interface where the BGP routing table did not display advertised routes.

Issue ID	Description
PAN-205482	Fixed an issue related to the *configd* process where Panorama displayed the error **Server not responding** when editing policy rules.
PAN-200946	Fixed an issue with firewalls in active/passive HA configurations where GRE tunnels went down due to recursive routing when the passive firewall was booting up. When the passive firewall became active and no recursive routing was configured, the GRE tunnel remained down.
PAN-196146	(VM-Series firewalls only) Fixed an issue where hostname validation failed due to the firewall not taking the hostname provided in `init.cfg`.
PAN-194968	Fixed an issue on the web interface where Antivirus updates were not able to be downloaded and installed unless Apps and Threads updates were downloaded and installed first, and the Antivirus content list displayed as blank. The resulting error message from the update server was also not reflected in the web interface.
PAN-174454	Fixed an issue where the firewall did not fetch group and user membership due to the Okta sync domain not matching the active directory sync domain.

PAN-OS 11.0.4 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.4.

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.

- PAN-OS 11.0.4 Known Issues
- PAN-OS 11.0.4-h6 Addressed Issues
- PAN-OS 11.0.4-h5 Addressed Issues
- PAN-OS 11.0.4-h2 Addressed Issues
- PAN-OS 11.0.4-h1 Addressed Issues
- PAN-OS 11.0.4 Addressed Issues

PAN-OS 11.0.4 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.4. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-252744	After upgrading PA-3200 Series, PA-5200 Series, or PA-7000 Series firewalls that are equipped with OCTEON 7x00 dataplane chips to PAN-OS 11.0.4 or 11.0.4-h1, the firewall might see continuous crashes, reboot repeatedly, and/or go into a non-functional state. **Workaround:** If you have already upgraded to one of those releases, downgrade to an earlier release or upgrade to PAN-OS 11.0.4-h2.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-234929	The tabs in the **ACC**, such as **Network Activity**, **Threat Activity**, and **Blocked Activity**, may not display any data when you apply a Time filter for the Last 15 minutes, Last Hour, Last 6 Hours, or Last 12 Hours. With the Last 24 Hours filter, the data displayed may not be accurate. Additionally, reports run against summary logs may not display accurate results.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.
PAN-233677	(PA-3410, PA-3420, PA-3430, PA-3440, PA-5410, PA-5420, PA-5430, and PA-5440 firewalls) By enabling Lockless

Issue ID	Description
	QoS feature, a slight degradation in App-ID and Threat performance is expected.
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.
PAN-222253 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	On the Panorama management server, policy rulebase reordering when you **View Rulebase by Groups** (**Policy** > **<policy-rulebase>**) does not persist if you reorder the policy rulebase by dragging and dropping individual policy rules and then moving the entire tag group.
PAN-221033	The firewall is responding to an ARP request for an IP address in the firewall's NAT address pool when that IP address isn't in the same subnet as the IP address of the ingress interface.
PAN-220176	(PAN-OS 11.0.1-h2 hotfix) System process crashes might occur with VoIP traffic when NAT is enabled with Persistent Dynamic IP and Port settings.
PAN-218521 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The ElasticSearch process on the M-600 appliance in Log Collector mode may enter a continuous reboot cycle. This results in the M-600 appliance becoming unresponsive, consuming logging disk space, and preventing new log ingestion.
PAN-216314	Upon upgrade or downgrade to or from PAN-OS 10.1.9 or 10.1.9-h1, offloaded application traffic sessions may disconnect after a period of time even if a session is active. The disconnect occurs after the application's default session timeout value is exceeded. This behavior affects only PAN-OS 10.1.9 and 10.1.9-h1. If you are on PAN-OS 10.1.9 and 10.1.9-h1, please use the following workaround. If you have already upgraded or downgraded to another PAN-OS version, use the following workaround in that version. **Workaround:** Run the CLI command **`debug dataplane internal pdt fe100 csr wr_sem_ctrl_ctr_scan_dis value 0`** to set the value to zero (0).
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync

Issue ID	Description
	on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`
PAN-212978	The Palo Alto Networks firewall stops responding when executing an SD-WAN debug operational CLI command.
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are

Issue ID	Description
	automatically unselected and any new tag created is applied to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207442	For M-700 appliances in an active/passive high availability (**Panorama** > **High Availability**) configuration, the `active-primary` HA peer configuration sync to the `secondary-passive` HA peer may fail. When the config sync fails, the job Results is `Successful` (**Tasks**), however the sync status on the **Dashboard** displays as `Out of Sync` for both HA peers. **Workaround**: Perform a local commit on the `active-primary` HA peer and then synchronize the HA configuration. **1.** Log in to the Panorama web interface of the `active-primary` HA peer. **2.** Select **Commit** and **Commit to Panorama**. **3.** In the `active-primary` HA peer **Dashboard**, click **Sync to Peer** in the High Availability widget.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy.

Issue ID	Description

	This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log forwarding to the disconnected Dedicated Log Collector is not impacted.
	Workaround: Restart the `mgmtsrvr` process on the Dedicated Log Collector.
	1. Log in to the Dedicated Log Collector CLI.
	2. Confirm the Dedicated Log Collector is disconnected from Panorama.
	`admin> show panorama-status`
	Verify the `Connected` status is `no`.
	3. Restart the `mgmtsrvr` process.
	`admin> debug software restart process management-server`

PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. • DLP cloud service • Advanced Threat Protection inline cloud analysis service • Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204689	Upon upgrade to PAN-OS 11.0.1, the following GlobalProtect settings do not work: • **Allow user to disconnect GlobalProtect App** > **Allow with Passcode**

Issue ID	Description
	- **Allow user to Disable GlobalProtect App** > **Allow with Passcode** - **Allow User to Uninstall GlobalProtect App** > **Allow with Password**
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-196146 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The VM-Series firewall on Azure does not boot up with a hostname (specified in an init-cgf.txt or user data) when bootstrapped.
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.

Issue ID	Description
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector. **Workaround:** Restart the log receiver service by running the following CLI command: `debug software restart process log-receiver`
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if:

Issue ID	Description
	- A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. - A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types: 1. Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. 2. Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report. 3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more

Issue ID	Description
	likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.4-h6 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.4-h5 Addressed Issues

Issue ID	Description
PAN-247511	A fix was made to address CVE-2024-3596.

PAN-OS 11.0.4-h2 Addressed Issues

Issue ID	Description
PAN-252744	(PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls) Fixed an issue where upgrading the firewall to PAN-OS 11.0.4 or PAN-OS 11.0.4-h1 caused the firewall to go into a non-functional state.

PAN-OS 11.0.4-h1 Addressed Issues

Issue ID	Description
PAN-252214	A fix was made to address CVE-2024-3400.

PAN-OS 11.0.4 Addressed Issues

Issue ID	Description
PAN-250686	Fixed an issue where selective push operations did not work when more than one admin user simultaneously performed changes and partial commits on Panorama.
PAN-249808	Fixed an issue where the *configd* process stopped responding when performing multidevice group pushes via XML API.
PAN-246707	Fixed an issue where failover was not triggered when multiple processes stopped responding.
PAN-245701	Fixed an issue where the returned values to SNMP requests for data port statistics were incorrect.
PAN-245690	Fixed an issue where the managed collectors health status on Panorama displayed as empty.
PAN-244493	Fixed a memory limitation with mapping subinterfaces to VPCE endpoints for GCP IPS, Amazon Web Services (AWS) integration with GWLB, and NSX service chain mapping.
PAN-243951	Fixed an issue on Panorama appliances in active/passive HA configurations where managed devices displayed as out-of-sync on the passive appliance when peer configuration changes were made to the SD-WAN configuration on the active peer.
PAN-242910	Fixed an issue where a custom based non-Superuser was unable to push to firewalls.
PAN-242627	Fixed an issue where selective push did not work.
PAN-242519	Fixed an issue where scheduled email reports failed if the @ symbol before the mail client was missing.
PAN-242027	Fixed an issue where the *all-task* process repeatedly restarted during memory allocation failures.
PAN-241164	(PA-410 firewalls only) Fixed an issue where system and configuration logs sent from the firewall to Panorama contained the serial number field instead of the firewall device name.
PAN-241141	Fixed an issue where creating more than one address object in the same XML API request resulted in a commit error.

Issue ID	Description
PAN-240618	Fixed an issue where configuration commits were successful even when dynamic peer IKE gateways configured on the same interface and IP address that did not have the same IKE Crypto profile.
PAN-240612	Fixed a kernel panic caused by a third-party issue
PAN-240487	Fixed an issue where fan speed increased significantly after upgrading the firewall.
PAN-240251	Fixed an issue where the *vldmgr* process incorrectly restarted during an Elasticsearch restart.
PAN-240225	Fixed an issue where authentication failed on web-based GlobalProtect portal.
PAN-240197	Fixed an issue where configuration changes made in Panorama and pushed to the firewall were not reflected on the firewall.
PAN-240166	Fixed an issue where, when explicit proxy was configured on the firewall, websites loaded more slowly than expected or did not load due to DNS using TCP.
PAN-239776	Fixed an issue where Panorama went into maintenance mode due to a GlobalProtect quota configuration that was under the minimum required quota.
PAN-239722	Fixed an issue where SNMP scans to the firewall took longer than expected and intermittently timed out.
PAN-239279	Fixed an issue where the SWG proxy did not accept new connections.
PAN-239256	Fixed an issue where ARP entries were unable to be completed for subinterfaces with SNAT configured.
PAN-239241	Extended the root certificate for WildFire appliances to December 31, 2032.
PAN-239200	Fixed an issue where the following Prisma Access SWG proxy upstream error was displayed when you attempted to access the proxy: `disconnect / reset before headers: reset reason: overflow`.
PAN-239144	Fixed an issue where the web interface was slower than expected when logging in, committing, and pushing changes after upgrading to PAN-OS 10.2.7.

Issue ID	Description
PAN-238949	Fixed a memory corruption issue where multiple processes stopped responding.
PAN-238643	Fixed an issue where a memory leak caused multiple processes to stop responding when VM Information Sources was configured.
PAN-238621	Fixed an issue where the HA3 link status remained down when updating the HA3 interface configuration when the AE interface was up.
PAN-238586	Fixed an issue where DNS resolution failure from the LFC resulted in WildFire public cloud connectivity failure.
PAN-238562	Fixed an issue where log collectors stopped responding when gathering reports from Panorama.
PAN-238508	Fixed an issue where the *routed* process created excessive logs in the log file.
PAN-237993	Fixed an issue where **Config Push Scheduler > Admin scope** changed to an admin ID instead of a 0 value, which caused a scheduled configuration push to work as a Selective push instead of a Full push.
PAN-237876	Extended the firewall Panorama root CA certificate which was previously set to expire on April 7th, 2024.
PAN-237678	Fixed an issue with firewalls in active/passive HA configurations where the passive firewall displayed the error message `Unable to read QSFP Module ID` when the passive link state was set to shutdown.
PAN-237562	Fixed an issue where firewalls generated link-change system logs for SFP ports even when no cable was connected to the ports.
PAN-237537	Fixed an issue where, when deleting CTD entries, the *all_pktproc* process stopped responding which resulted in dataplane failure.
PAN-237478	Fixed an issue where the Traffic log displayed 0 bytes for denied sessions.
PAN-237454	Fixed an issue where Panorama stopped redistributing IP address-to-username mappings when packet loss occurred between the distributor and the client.
PAN-237369	(PA-1420 firewalls only) Fixed an issue where the *all_task* process stopped responding, which caused the firewall to become unresponsive.

Issue ID	Description
PAN-236802	Fixed an issue on firewalls in HA configurations where unexpected failovers occurred.
PAN-236605	Fixed an issue where the *configd* process stopped responding due to a deadlock related to rule-hit-count.
PAN-235840	Fixed an issue where, after a configuration push from Panorama to managed firewalls, the status displayed as **None** and the push took longer than expected.
PAN-235737	Fixed an issue where the *brdagent* process stopped responding due to a sudden increase in logging to the bcm.log.
PAN-235628	Fixed an issue where you were not prompted for login credentials when you disconnected and connected back to the GlobalProtect portal when SAML authentication was selected along with single sign-on (SSO) and Single Log Out (SLO).
PAN-235557	Fixed an issue where uploads from tunnels, including GlobalProtect, were slower than expected when the inner and outer sessions were on different dataplanes.
PAN-235476	Fixed an issue where Threat logs from different Security zones were aggregated into one log.
PAN-235385	Enhanced wifclient cloud connectivity redundancy.
PAN-235168	Fixed an issue where disk space became full even after clearing old logs and content images.
PAN-235081	(VM-Series firewalls only) Fixed an issue where the firewall sent packets to its own interface after configuring NAT64.
PAN-234977	Fixed an issue where, when a Layer 2 interface that was a member of a VLAN was down, all traffic transmitted over the VLAN was dropped.
PAN-234459	Fixed an issue with the firewall web interface where local SSL decryption exclusion cache entries were not visible.
PAN-234290	Fixed an issue where the firewall displayed incorrect interface transfer rates when running the CLI command `show system state filter-pretty sys.s1.px` with a filter.
PAN-234279	Fixed an issue where the *ikemgr* process crashed due to an IKEv1 timing issue, which caused commits to fail with the following error message: `Client ikemgr requesting last config in`

Issue ID	Description
	`the middle of a commit/validate, aborting current commit.`
PAN-234238	Fixed an issue where a Security policy that referenced more than 30 HIP Profiles caused buffer overflow, which caused other Security policies with HIP Profiles to misidentified users and traffic was denied.
PAN-234190	Fixed an issue where the firewall incorrectly blocked URLs even when they matched the custom category.
PAN-234031	Fixed an issue on multi-core firewalls where the firewall displayed packets out of order when capturing packets on the transmit stage.
PAN-233957	(PA-5450 firewalls only) Fixed an issue where the NAT private pool was not used properly when enabling slot 6 DPC.
PAN-233833	Fixed an issue where enabling Jumbo frames resulted in software packet buffer depletion.
PAN-233789	Fixed an issue with push and commit and push operations where the user was not correctly bound to the scope, which caused all device groups to be selected for a selective push.
PAN-233780	(VM-100 firewalls only) Fixed an issue where commits failed due to the configuration memory limit.
PAN-233764	Fixed an issue where commits failed due to large inbound inspection certificates that exceeded the buffer size of 4,096 bytes.
PAN-233541	Fixed an issue where device group and template administrators with access to a specific virtual system were able to see logs for all virtual systems via Context Switch.
PAN-233517	Fixed an issue on Panorama where managed device templates and device groups took longer than expected to display in the **Push to Devices** window.
PAN-233463	Fixed an issue where the X-Forwarded-For (XFF) IP address value was not displayed in Traffic logs.
PAN-233390	Fixed an issue where the exclude-cache reason was incorrectly presented as `TLS13_UNSUPPORTED` instead of `SSL_CLIENT_CERT`.
PAN-233191	(PA-5450 firewalls only) Fixed an issue where the Data Processing Card (DPC) restarted due to path monitor failure after QSFP28 disconnected from the Network Processing Card (NPC).

Issue ID	Description
PAN-233039	Fixed an issue where GENEVE encapsulated packets coming from a GFE Proxy mapped to an incorrect Security policy rule.
PAN-232953	Fixed an issue where you were able to cancel the same commit repeatedly, which displayed the error message `Cannot stop job &lt;job&gt; at this time`.
PAN-232924	Fixed an issue on firewalls in active/passive HA configurations where the passive firewall was unable to retrieve SDB data for locally inserted SFP transceivers.
PAN-232800	Fixed an issue where critical disk usage for `/opt/pancfg` increased continuously and the system logs displayed the following message: `Disk usage for /opt/pancfg exceeds limit, &lt;value&gt; percent in use`.
PAN-232377	Fixed an issue where the `AddrObjRefresh` job failed when the *useridd* process restarted.
PAN-232358	(PA-5450 firewalls only) Fixed an issue where the interface on QSFP28 ports did not go down when the Tx cable was removed from the QSFP28 module.
PAN-232290	(PA-5200 Series firewalls only) Fixed an issue where the First Packet Processor (FPP) did not acknowledge a query to find the owner for fragmented packets, tunnel packets, and other scenarios when the packet slot and dataplane owner was unknown.
PAN-232250	Fixed an issue where, when SSH service profiles for management access were set to **None**, the reported output was incorrect.
PAN-232132	Fixed an issue where DNS response packets were malformed when an antispyware Security Profile was enabled.
PAN-231698	Fixed an issue where you were unable to set the Dynamic Updates schedule threshold to an empty value.
PAN-231552	Fixed an issue where traffic returning from a third-party Security chain was dropped.
PAN-231507	(PA-1400 Series firewalls only) Fixed an issue where, when an HSCI interface was used as an HA2 interface, HA2 packets were intermittently dropped on the passive firewall, which caused the HA2 connection to flap due to missing HA2 keepalive messages.

Issue ID	Description
PAN-231480	Fixed an issue where the firewall CLI output for GlobalProtect log quota settings did not match the settings configured on the Panorama web interface.
PAN-231459	(PA-5450 firewalls only) Fixed an issue where a large number of invalid source MAC addresses were shown in drop-stage packet captures.
PAN-231395	Fixed an intermittent issue where the OCSP query failed.
PAN-231329	Fixed an issue where the *logrcvr* process stopped responding due to a corrupt log in the forwarding pipeline.
PAN-231295	Fixed an issue where the *logrcvr* process stopped when running the `hints-max` CLI command.
PAN-231169	(PA-220 firewalls only) Fixed an issue where an unused plugin incorrectly used memory.
PAN-231148	Fixed an issue where no DHCP option list was defined when using GlobalProtect.
PAN-230813	Fixed an issue where flex memory leak caused decryption failure and commit failure with the error message `Error preparing global objects failed to handle CONFIG_UPDATE_START`.
PAN-230746	Fixed an issue on the web interface where device groups with a large number of managed firewalls displayed the **Policy** page more slowly than expected.
PAN-230656	(Firewalls in HA configurations only) Fixed an issue where a split brain condition occurred on both firewalls after booting up any firewall, and an HA switchover occurred after booting up a firewall with a higher HA priority even when no preemptive option was enabled on the firewall.
PAN-230377	Fixed an issue where FEC support was not enabled by default for PAN-25G-SFP28-LR modules.
PAN-230363	(PA-7050 firewalls with SMC-B only) Fixed an issue where the management interface was reported as up even when MGT-A and MGT-B were both down.
PAN-230362	Fixed an issue where the firewall truncated the payload of a TCP Out of Order segment with a FIN flag.

Issue ID	Description
PAN-230359	Fixed an issue where SAML authentication failed with the error message `Failed to verify signature against certificate` when `ds:KeyName` was in the IdP metadata.
PAN-230198	Fixed an issue where URL logs were duplicated on Cortex Data Lake.
PAN-230106	Fixed an issue where the firewall was unable to retrieve the most current external dynamic list information from the server due to hostname resolution failure.
PAN-230092	Fixed an issue where the *routed* process stopped responding when committing routing-related changes if Advanced routing was enabled.
PAN-230039	Fixed an issue where migrating from an Enterprise License Agreement (ELA) to a Flexible VM-Series License failed with a deactivation error message.
PAN-229952	Fixed an issue where the **print PDF** option did not work (**Panorama > Managed Devices > Health**).
PAN-229950	Fixed an issue where custom response pages for the GlobalProtect login page did not load and displayed a 404 Not Found error.
PAN-229874	Fixed an issue where the firewall was unable to form OSPFv3 adjacency when using an ESP authentication profile.
PAN-229873	(PA-7050 firewalls only) Fixed an issue related to *brdagent* process errors.
PAN-229866	Fixed an issue where the *reportd* process stopped responding.
PAN-229824	Fixed an issue where **Device History** was not visible under **Managed Devices Summary**.
PAN-229606	Fixed an issue where the *brdagent* process stopped responding after an upgrade due to initialization failure.
PAN-229398	Fixed an issue where the Management Processor Card (MPC) stopped responding.
PAN-229315	Fixed an issue where Octets in NetFlow records were always reported to be 0 despite having a nonzero packet count.
PAN-229307	Fixed an issue where half closed SSL decryption sessions stayed active, which caused software packet buffer depletion.

Issue ID	Description
PAN-229115	Fixed an issue on the web interface where the screen was blank after logging in to Panorama.
PAN-229080	Fixed an issue where the new management IP address on the interface did not take effect.
PAN-229072	Fixed an issue where GlobalProtect did not automatically connect to an internal gateway after an endpoint was woken.
PAN-229069	Fixed an issue where clientless VPN portal users were unable to access clientless applications due to an SSL renegotiation being triggered.
PAN-228998	Fixed an issue where multiple license status checks caused an internal process to stop responding.
PAN-228775	Fixed an issue where the CLI command `show bonjour interface` did not display any output.
PAN-228457	(PA-7000 firewalls only) Fixed an issue where the GTP logs forwarded from the firewall to the log collector did not include the pcap.
PAN-228442	Fixed an issue on firewalls in active/passive HA configurations where sessions did not fail over from the active firewall to the passive firewall when upgrading PAN-OS.
PAN-228342	Fixed an issue where objects in the running configuration appeared to be deleted under the push scope preview.
PAN-228323	Fixed an issue where a large number of Panorama management server cookies were created in the Redis database when the Cloud-Service plugin sent an authentication request every second, and logging in to or using Panorama was slower than expected.
PAN-228277	Fixed an issue where commits took longer than expected.
PAN-227998	Fixed an issue where the *zebra* process stopped responding due to memory corruption.
PAN-227939	Fixed an issue where the *all_task* process stopped responding due to high wifclient memory usage, which caused the firewall to reboot.
PAN-227887	Fixed an issue where IP address checksums were calculated incorrectly.
PAN-227804	Fixed an issue where memory corruption caused the *comm* process to stop responding.

Issue ID	Description
PAN-227774	Fixed an issue where commits failed with the error message `Management server failed to send phase 1 to client logrcvr`.
PAN-227539	Fixed an issue where excess WIF process memory use caused processes to restart due to OOM conditions.
PAN-227522	Fixed an issue where **shared** application filters that had application object overrides were overwritten by predefined applications.
PAN-227517	Fixed an issue related to the IPv6 character limit for the source address in static route path monitoring.
PAN-227510	Fixed an issue where the error message `Failed to establish GRPC connection to UrlCat service: failed to start grpc connection` was displayed in the system log when the Advanced URL Filtering license was applied but not configured.
PAN-227397	Fixed an issue where selective pushes on Panorama removed a previously pushed configuration from the firewalls.
PAN-227368	Fixed an issue where the GlobalProtect app was unable to connect to a portal or gateway and GlobalProtect Clientless VPN users were unable to access applications if authentication took more than 20 seconds.
PAN-227344	Fixed an issue on Panorama where **PDF Summary Reports** (**Monitor > PDF Reports > Manage PDF Summary**) displayed no data and were blank when predefined widgets were included in the summary report.
PAN-227305	Fixed an issue where SCEP certificate generation failed when a service route was used to reach the SCEP server.
PAN-227064	Fixed an issue with high availability (HA) sync failure when performing a partial commit after creating a Security policy via REST API.
PAN-227058	Fixed an issue where traffic did not match Security policy rules with the destination as FQDN and instead hit the default deny rule.
PAN-226923	Fixed an issue where an excessive tab displayed *Device > Setup** when using Simplified Chinese.
PAN-226860	Fixed an issue where macOS X-Auth clients disconnected prematurely from the GlobalProtect gateway during a Phase 2 re-key event.
PAN-226768	Fixed an issue where, when the GlobalProtect app was installed on iOS endpoints and the gateway was configured to accept cookies, the

Issue ID	Description
	app remained in the **Connecting** stage after authentication, and the GlobalProtect log displayed the error message `User is not in allow list`. This occurred when the app was restarted or when the app attempted to reconnect after disconnection.
PAN-226626	Fixed an issue where the firewall generated numerous *logrcvr* error messages related to NetFlow.
PAN-226470	Fixed an issue where previewing changes for selective admins took longer than expected or displayed the error message `commands succeeded with no output`.
PAN-226128	Fixed an issue where selective push failed on Panorama after deleting shared objects that were referenced in multi-device group environments with the error message: `Schema validation failed. Please try a full push.`
PAN-226021	Fixed an issue where content push operations failed for a URL category **Scanning Activity**.
PAN-225975	Fixed an issue where the CLI command `show system disk details` was not available.
PAN-225394	Fixed an issue on the firewall where SNMP incorrectly reported high packet descriptor usage.
PAN-225337	Fixed an issue on Panorama related to Shared configuration objects where configuration pushes to multi-vsys firewalls failed.
PAN-225203	Fixed an issue where the Log Forwarding Card (LFC) did not honor the negotiated MSS on the logging connection.
PAN-225110	Fixed an issue with firewalls in HA configurations where HA configuration syncs did not complete or logging data was missing until firewall processes were manually restarted or the firewalls were rebooted.
PAN-225094	Fixed an issue where performing a commit operation failed and the following error message was displayed: `failed to handle CUSTOM_UPDATE`.
PAN-225090	Fixed an issue on Panorama where **Commit and Push** was grayed out when making changes to a template or device group.
PAN-225082	Fixed an issue where GlobalProtect quarantine-delete logs were incorrectly shown on passive firewalls.

Issue ID	Description
PAN-225013	(PA-5450 firewalls only) Fixed an issue where the firewall rebooted unexpectedly when a Network Card was on Slot 2 instead of a DPC.
PAN-224955	Fixed an issue where the *devsrvr* process stopped responding when Zone Protection had more than 255 profiles.
PAN-224954	Fixed an issue where, after upgrading and rebooting a Panorama appliance in Panorama or Log Collector mode, managed firewalls continuously disconnected.
PAN-224938	Fixed an issue where the CLI command settings for `set system setting logging max-log-rate` did not persist after a *mgmtsrvr* process restart.
PAN-224882	Fixed an issue where the session end reason was incorrectly logged as `decrypt-cert-validation` for allowed sessions when the decryption profile was configured for a no-decrypt policy.
PAN-224788	Fixed an issue where the `Power Supplies` was not present in the `show system environmentals` CLI command output.
PAN-224772	Fixed a high memory usage issue with the *mongodb* process that caused an OOM condition.
PAN-224656	Fixed an issue where the *devsrvr* process caused delays when Dynamic Address Groups with large entry lists were being processed during a commit, which caused commits to take longer than expected.
PAN-224500	Fixed an issue where IPv6 addresses in XFF were displayed in Traffic logs.
PAN-224424	(PA-3440 firewalls only) Fixed an issue where you were unable to set the link speed as 25Gbps from the drop-down in the template for Ethernet ports 1/23 through 1/26.
PAN-224405	Fixed an issue where the *distributord* process repeatedly stopped responding.
PAN-224404	Fixed an issue where a memory leak caused decryption failures when SSL Forward Proxy was configured.
PAN-224365	Fixed an issue where excessive network path monitoring messages were generated in the system logs.

Issue ID	Description
PAN-224354	Fixed an issue where a memory leak related to the *distributord* process occurred when connections flapped for IP address-to-username mapping redistribution.
PAN-224067	Fixed an issue where cookie authentication did not work for GlobalProtect when an authentication override domain was configured in the SAML authentication profile.
PAN-223914	Fixed an issue on Panorama where the *reportd* process unexpectedly stopped responding.
PAN-223856	(PA-800 Series firewalls only Fixed an issue where the GlobalProtect SSL tunnel failed.
PAN-223855	Fixed an issue where the `show running ippool` CLI command output displayed incorrect used and available NAT IP address pools on DIPP NAT policy rules in multidataplane firewalls.
PAN-223798	Fixed an issue on the firewall where, when Advanced Routing was enabled, PIM join messages were not sent to the RN due to a missing OIF.
PAN-223559	Fixed an issue where unexpected characters appeared in the text of GlobalProtect application authentication prompts when the GlobalProtect portal or gateway had a RADIUS authentication profile.
PAN-223796	(PA-7000 Series firewalls with Log Forwarding Cards (LFC) only) Fixed an issue where multiple OOM conditions occurred which caused a system restart.
PAN-223559	Fixed an issue where unexpected characters appeared in the text of GlobalProtect application authentication prompts when the GlobalProtect portal or gateway had a RADIUS authentication profile.
PAN-223481	(PA-5450 firewalls only) Fixed an issue where the *all_pktproc* process stopped responding when the firewall was on PAN-OS 10.1.9-h3 or a later release.
PAN-223432	Fixed an issue where SSL decryption for HTTP/2 sessions failed when enabling **Send handshake messages to CTD for inspection** (**Device > Setup > Session > Decryption Settings > SSL Decryption Settings**).
PAN-223365	Fixed an issue where Panorama was unbale to query any logs if the Elasticsearch health status for any log collector was degraded.

Issue ID	Description
PAN-223271	Fixed an issue where the file transfer of large zipped and compressed files had the App-ID `unknown-tcp`.
PAN-223263	Fixed an issue on the web interface where the system clock for **Mexico_city** was displayed in CDT instead of CST on the management dashboard.
PAN-223259	Fixed an issue where selective pushes failed with the error message `Failed to generate selective push configuration. Unable to retrieve last in-sync configuration for the device, either a push was never done or version is too old. Please try a full push.`
PAN-223172	Fixed an issue on Panorama where host IDs manually added to the device quarantine list were unexpectedly removed.
PAN-223094	Fixed an issue where fragmented TCP traffic was dropped due to an IP address ID conflict over the SD-WAN tunnel.
PAN-222662	Fixed an issue where the CLI command `debug log-card-interface pint slot <x> host <host>` did not return any information when attempting to ping the Log Forwarding Card (LFC).
PAN-222586	(PA-5410, PA-5420, and PA-5430 firewalls only) Fixed an issue where **Filter** drop-downs, **Forward Method**, and **Correlation** log settings (**Device > Log Settings > Correlation**) were not displayed.
PAN-222188	A CLI command was introduced to address an issue where SNMP monitoring performance was slower than expected, which resulted in `snmpwalk` timeouts.
PAN-222089	Fixed an issue where you were unable to context switch from Panorama to the managed device.
PAN-221973	Fixed an issue where the same user connected to multiple SSL VPN connections and one of the sessions stopped working.
PAN-221938	Fixed an issue with network packet broker sessions where the broker session and primary session timeouts were out of sync, which caused traffic drops if the broker session timed out when the primary session was still active.
PAN-221897	Fixed an issue where duplicate entries were not detected during commits, which caused routing engine failure.

Issue ID	Description
PAN-221881	Fixed an issue where log ingestion to Panorama failed, which resulted in missing logs under the **Monitor** tab.
PAN-221857	Fixed an issue where users were unable to log in to the GlobalProtect app using SAML authentication after upgrading to PAN-OS 10.2.3-h4, and the GlobalProtect logs displayed the following error message: `Username from SAML SSO response is different from the input`.
PAN-221728	Fixed an issue where selective pushes did not work after upgrading to PAN-OS 10.2.4.
PAN-221428	Fixed a memory leak issue where the packet buffer count continuously increased and the firewall required a restart to clear the buffers.
PAN-221190	(PA-800 Series firewalls only) Fixed an issue where the firewall rebooted due to I2C errors when unsupported optics were inserted in ports 5-8.
PAN-221186	Fixed an issue where BGP aggregate routes were not created and discard routes were not installed in the routing table.
PAN-221162	Fixed an issue where previewing changes before pushing to devices displayed a pop-up with the message: `Command succeeded with no output`.
PAN-221015	(M-600 Appliances only) Fixed an issue where ElasticSearch processes did not restart when the appliance was rebooted, which caused the managed collector ES health status to be downgraded.
PAN-220931	(Panorama appliances in FIPS-CC mode only) Fixed an issue where scheduled email reports did not contain PDF attachments.
PAN-220907	(VM-Series firewalls only) Fixed an issue where large packets were dropped from the dataplane to the management plane, which caused OSPF neighborship to fail.
PAN-220881	Fixed an issue where the CLI command `show logging-status` did not correctly display the last log created and forwarded timestamps.
PAN-220659	Fixed an issue on the firewall where scheduled antivirus updates failed when external dynamic lists were configured on the firewall.
PAN-220619	Fixed an issue where the correct device filter did not apply when filtering **Targets** and **Target/Tags** (**Device Group** > **Policies**).

Issue ID	Description
PAN-220553	Fixed an issue where, after enabling Advanced Routing Engine, the backup default route was not installed in the FIB table if static path monitoring went down.
PAN-220500	(PA-5450 and PA-400 firewalls only) Fixed an issue where the `request shutdown system` CLI command did not completely shut down the system.
PAN-220239	Fixed an issue where certificate-based logins to Panorama via the web interface failed.
PAN-219851	Fixed an issue where you were unable to export SAML metadata when configuring SAML authentication.
PAN-219768	Fixed an issue where you were unable to filter data filtering logs with **Threat ID/NAME** for custom data patterns created over Panorama.
PAN-219585	Fixed an issue where enabling `syslog-ng` debugs from the root caused 100% disk utilization.
PAN-219494	Fixed an issue with the firewall where adding **Parent-App** under **Application Filter** for Security policy rules did not add dependent applications.
PAN-219415	Fixed an issue where BGP routes were installed in the routing table even when the option to install routes was disabled in the configuration.
PAN-219351	Fixed an issue where the *all_pktproc* process stopped responding during Layer 7 processing.
PAN-219260	(M-Series appliances only) Fixed an issue where the management interface flapped due to low memory reserved for kernel space.
PAN-219251	Fixed an issue where the `ctd_dns_wait_pkt_drop` counter increase was greater than expected.
PAN-219222	Fixed an issue where spaces in a certificate name caused imports to fail.
PAN-219113	Fixed an issue where, when a port on the NPC was configured for log forwarding, the ingress traffic on the card was sent for processing to the LPC, and the LPC card was reloaded when the ingress volume of traffic was high.

Issue ID	Description
PAN-218873	Fixed an issue where a HIP mask was reused when an existing IP address user mapping was updated by a new IP address user mapping that had a different username but the same IP address.
PAN-218694	Fixed an issue where SaaS PR was reimported to the shared location and policy objects were not updated with new updates coming from the SaaS cloud.
PAN-218659	Fixed an issue where Security zones under Interfaces displayed as **none** for dynamic group and template admin users in a read-only admin role.
PAN-218652	Fixed an issue on Panorama where the HA virtual address was not created for firewalls in active/active HA configurations.
PAN-218620	Fixed an issue where scheduled configuration exports and SCP server connection testing failed.
PAN-218611	Fixed an issue where the device telemetry region was not updated on the firewall when pushed from the Panorama template stack.
PAN-218555	Fixed an issue where the firewall did not receive dynamic address updates pushed from Panorama during initial registration to Panorama.
PAN-218352	Fixed an issue where Panorama was slower than expected when WildFire deployment was scheduled every minute to a large number of devices.
PAN-218119	Fixed an issue where the firewall transmitted packets with an incorrect source MAC address during commit operations.
PAN-218057	(PA-7000 Series firewalls only) Fixed an issue where internal path monitoring failed due to a heartbeat miss.
PAN-217728	Fixed an issue where uploading a certificate in a manual configuration option for SafenetHSM failed.
PAN-217652	Fixed an issue on Panorama where certificates created on Panorama were not pushed to the firewall with a selective push.
PAN-217619	Fixed an issue where supported Bi-DI transceivers were not recognized which caused ports to not come up.
PAN-217541	Fixed an issue where the *useridd* process stopped responding after a restart when HIP redistribution was enabled.

Issue ID	Description
PAN-217510	Fixed an issue where inbound DHCP packets received by a DHCP client interface that were not addressed to itself were silently dropped instead of forwarded.
PAN-217293	Fixed a rare issue where URLs were not accessible when the header length was greater than 16,000 over HTTP/2.
PAN-217289	Fixed an intermittent issue where HTTP/2 traffic caused buffer depletion.
PAN-217272	Fixed an issue where the DNS proxy log included an excessive number of the following error message: `Warning: pan_dnsproxy_log_resolve_fail: Failed to resolve domain name ** AAAA after trying all attempts to name servers`
PAN-217241	Fixed an issue where predict session conversion failed for RTP and RTCP traffic.
PAN-217205	Fixed an issue where the firewall did not clear port reused sessions for GlobalProtect traffic with proxy fast-session-delete enabled.
PAN-217155	Fixed an issue where syncs between Panorama and the Cloud Identity Engine (CIE) caused intermittent slowness when using the web interface due to a large number of groups in the CIE directory.
PAN-217123	Fixed an issue where, when log queries in the **yyyy/mm/dd** format displayed extra digits for the day and an error was not generated.
PAN-217064	Fixed an issue where commits took longer than expected when the DLP plugin was configured.
PAN-217024	Fixed an issue where fetching device certificates failed for internal DNS servers with the error message `ERROR Error: Could not resolve host: certificate.paloaltonetworks.com`.
PAN-216647	Fixed an issue where the `sysd` node was updated at incorrect times.
PAN-216230	Fixed an issue where the shard count reached up to 10% over the limit rather than staying under the limit.
PAN-216077	A CLI command was added to configure the FEC for PA-5450 breakout ports.
PAN-215583	Fixed an issue on firewalls in HA configurations where the primary firewall went into a nonfunctional state due to a timeout in the

Issue ID	Description
	`pan_comm` logs during the policy-based forwarding (PBF) parse, which caused an HA failover.
PAN-215576	Fixed an issue where the `userID-Agent` and `TS-Agent` certificates were set to expire on November 18, 2024. With this fix, the expiration date has been extended to January 2032.
PAN-215436	Fixed an issue with the web interface where the latest logs took longer than expected to display under **Monitor**.
PAN-214773	Fixed an issue where RTP packets traversing intervsys were dropped on the outgoing vsys.
PAN-214760	Fixed an issue where, when a firewall had more than 1,200 logical interfaces, commits failed with the error message: `Error pre-installing config failed to handle CONFIG_COMMIT`.
PAN-214311	Fixed an issue where users were able to add configurations via XML API even when a config lock was in place.
PAN-214177	Fixed an issue where template configurations were not properly pushed to the firewall during an export or push of the device configuration bundle.
PAN-213949	Fixed an issue where the VPN responder stopped responding when it received a CREATE_CHILD message with no security association (SA) payload.
PAN-213918	Fixed an issue where `mlav-test-pe-file.exe` was not detected by WildFire Inline ML.
PAN-213591	Fixed an issue where **Request Categorization Change** was not displayed under URL filtering logs when the Advanced URL Filtering license was applied.
PAN-213011	Fixed an issue where, when using multi-factor authentication (MFA) with RADIUS OTP, the challenge message **Enter Your Microsoft verification code** did not appear when accessing the GlobalProtect portal via browser.
PAN-212932	Fixed an issue where the firewall went into a restart loop with the following error message: `failed to get mgt settings candidate: configured traffic quota of 0 MB is less than the minimum 32 MB`.
PAN-212770	Fixed an issue on the firewall where the WildFire file size limit value did not match on the web interface and the CLI.

Issue ID	Description
PAN-212580	(PA-7050 firewalls only) Fixed an issue where disk space filled up due to files under `/opt/var/s8/lp/log/pan/` not being properly deleted.
PAN-212576	Fixed an issue where firewall HA clusters in active/active configurations with Advanced Routing enabled did not relay to ping requests sent to a virtual IP address.
PAN-211945	Fixed an issue where URL Filtering system logs showed the error message `CURL ERROR: bind failed with errno 124: Address family not supported by protocol` even though the PAN-DB cloud was connected.
PAN-211827	Fixed an issue where Dynamic Updates failed with the following error message: `CONFIG_UPDATE_INC: Incremental update to DP failed please try to commit force the latest config`.
PAN-211821	Fixed an issue on firewalls in HA configurations where committing changes after disabling the QoS feature on multiple Aggregate Ethernet (AE) interfaces caused the dataplane to go down.
PAN-211255	Fixed an issue third-party VPNC IPSec clients were disconnected after a few seconds for firewalls in active/active HA configurations.
PAN-210354	Fixed an issue where the *routedd* process stopped responding when executing the `show static-route path-monitoring` CLI command or when accessing the path monitoring records from the web interface (**Network > Virtual Router > More Runtime Stats > Static Routing**).
PAN-208085	Fixed an issue where the BFD peers were deleted during a commit from Panorama. This occurred because the *pan_comm* thread became deadlocked due to the same *sysd* object was handled during the commit.
PAN-207616	Fixed an issue on Panorama where, after selecting managed firewalls and creating a new tag, the managed firewalls were automatically unselected and any new tag that was created was applied to the managed firewalls for which you initially created the tag.
PAN-207092	Fixed an issue where logging in using default credentials after changing to FIPS-CC for NSX-T firewalls did not work.
PAN-207003	Fixed an issue where the *logrcvr* process NetFlow buffer was not reset which resulted in duplicate NetFlow records.

Issue ID	Description
PAN-206639	Fixed an issue where the LFC and NPC remained stuck during bootup.
PAN-206041	(PA-7050 firewalls only) Fixed an issue where the *ikemgr* process stopped responding.
PAN-205041	Fixed an issue where **DNS Security cloud service unavailable** logs did not indicate the service name, status code, or error message in the DNS proxy log.
PAN-202361	Fixed an issue where packets queued to the *pan_task* process were still transmitted when the process was not responding.
PAN-202095	Fixed an issue on the web interface where the language setting is not retained.
PAN-202008	Fixed an issue where Traffic logs exported to CSV files contained inaccuracies and were not complete.
PAN-198043	Fixed a rare issue where a`BuildXmlCache` job failed on the firewall.
PAN-196954	Fixed a memory leak issue related to the *distributord* process.
PAN-196840	Fixed an issue where exporting a Security policy rule that contained Korean language characters to CSV format resulted in the policy description being in a nonreadable format.
PAN-196395	(PA-5450 firewalls only) Fixed an issue where the firewall accepted 12 Aggregate Ethernet interfaces, but you were unable to configure interfaces 9-12 via the web interface.
PAN-194912	Fixed an issue where the CLI command `show applications list` did not return any outputs.
PAN-194006	Fixed an issue on Panorama where *Commit Push** and **Validate Push** operations during a **Push to Devices** did not handle the configuration for shared objects, which resulted in an invalid configuration being pushed.
PAN-193004	Fixed an issue where `/opt/pancfg` partition utilization reached 100%, which caused access to the Panorama web interface to fail.
PAN-192188	(PA-5450 firewalls only) Fixed an issue where the `show running resource-monitor ingress-backlogs` CLI command failed with the following error message: `Server error : Failed to intepret the DP response`.

Issue ID	Description
PAN-185249	Fixed an issue where **Template Stack** overrides (**Dynamic Updates > App & Threats > Schedule**) were not able to be reverted via the web interface.
PAN-182960	Additional error logs were added for an issue where, when multiple Panorama web interface sessions were opened, active lock did not show up on the web interface for any session.
PAN-172600	Fixed an issue where the CLI command `show rule-hit-count` did not provide all details of the rule from the device group.
PAN-171569	Fixed an issue where HIP matches were not recognized in an SSL decryption policy rule.

PAN-OS 11.0.3 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.3.

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.

- PAN-OS 11.0.3 Known Issues
- PAN-OS 11.0.3-h13 Addressed Issues
- PAN-OS 11.0.3-h12 Addressed Issues
- PAN-OS 11.0.3-h10 Addressed Issues
- PAN-OS 11.0.3-h5 Addressed Issues
- PAN-OS 11.0.3-h3 Addressed Issues
- PAN-OS 11.0.3-h1 Addressed Issues
- PAN-OS 11.0.3 Addressed Issues

PAN-OS 11.0.3 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.3. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-250062	Device telemetry might fail at configured intervals due to bundle generation issues.
PAN-243951	On the Panorama management sever in an active/passive High Availability (HA) configuration, managed devices (**Panorama** > **Managed Devices** > **Summary**) display as `out-of-sync` on the passive HA peer when configuration changes are made to the SD-WAN (**Panorama** > **SD-WAN**) configuration on the active HA peer. **Workaround:** Manually synchronize the Panorama HA peers. **1.** Log in to the Panorama web interface on the active HA peer. **2.** Select **Commit** and **Commit to Panorama** the SD-WAN configuration changes on the active HA peer. On the passive HA peer, select **Panorama** > **Managed Devices** > **Summary** and observe that the managed devices are now `out-of-sync`. **3.** Log in to the primary HA peer Panorama CLI and trigger a manual synchronization between the active and secondary HA peers. *request high-availability sync-to-remote running-config* **4.** Log back in to the active HA peer Panorama web interface and select **Commit** > **Push to Devices** and **Push**.
PAN-241536	On the Panorama management server, a user with an Admin Role is unable to modify or add filters to profiles under

Issue ID	Description
	Panorama > **Network** > **Routing** > **Routing Profiles** > **Filters**, despite having the necessary read and write privileges.
PAN-234408	Enterprise DLP cannot detect and block non-file based traffic for ChatGPT from traffic forwarded to the DLP cloud service from an NGFW.
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-242910 PAN-OS 11.0.3, 11.0.3-h1, 11.0.3-h3, and 11.0.3-h5	On the Panorama management server, Panorama administrators (**Panorama** > **Administrators**) that are assigned a custom Panorama admin role (**Panorama** > **Admin Roles**) with **Push All Changes** enabled are unable to push configuration changes to managed firewalls when **Managed Devices** and **Push For Other Admins** are disabled.
PAN-242837	Default login credentials and SSH fail after enabling FIPS-CC Mode on a firewall or Panorama after converting through the Maintenance Recovery Tool (MRT). The firewall or Panorama becomes stuck and requires a factory reset to recover.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-238769	FIPS-CC VM only. Upgrading to 10.1.10-h2 or 10.1.11 will change all locally created security Policy actions to Deny. Re-load the back-up config taken before upgrading or the last version to get the previous config back. Also, Unable to login to FIPSCC Mode devices with default credentials after converting the mode for 10.1.12 release , 10.2.7 release , 11.1.0 , 11.1.1, 11.0.3 versions.
PAN-234929	The tabs in the **ACC**, such as **Network Activity**, **Threat Activity**, and **Blocked Activity**, may not display any data when you apply a Time filter for the Last 15 minutes, Last Hour, Last 6 Hours, or Last 12 Hours. With the Last 24 Hours filter, the data displayed may not be accurate. Additionally, reports run against summary logs may not display accurate results.
PAN-231507 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On PA-1400 Series firewalls only, when an HSCI interface is used as an HA2 interface, HA2 packets are intermittently dropped on the passive device, which can cause the HA2 connection to flap due to missing HA2 keepalive messages. Workaround: use data ports configured as HA2 interface.

Issue ID	Description
PAN-228515	The EleasticSearch SSH flaps on the M-600 appliance in Panorama or Log Collector mode. This causes logs to not display on the Panorama management server (**Monitor** > **Logs**) and the Log Collector health status (**Panorama** > **Managed Collectors** > **Status**) to display as degraded.
PAN-227344	On the Panorama management server, PDF Summary Reports (**Monitor** > **PDF Reports** > **Manage PDF Summary**) display no data and are blank when predefined reports are included in the summary report.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.
PAN-225337 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On the Panorama management server, the configuration push to a multi-vsys firewall fails if you: **1.** Create a **Shared** and vsys-specific device group configuration object with an indentical name. For example, a **Shared** address object called `SharedA01` and a vsys-specific address object also called `SharedA01`. **2.** Reference the **Shared** object in another **Shared** configuration. For example, reference the **Shared** address object (`SharedA01`) in a **Shared** address group called `SharedAG1`. **3.** Use the **Shared** configuration object with the reference in a vsys-specific configuration. For example, reference the **Shared** address group (`SharedAG1`) in a vsys-specific policy rule. **Workaround:** Select **Panorama** > **Setup** > **Management** and edit the Panorama Settings to enable one of the following: • **Shared Unused Address and Service Objects with Devices**—This options pushes all **Shared** objects, along with device group specific objects, to managed firewalls. This is a global setting and applies to all managed firewalls, and may result in pushing too many configuration objects to your managed firewalls. • **Objects defined in ancestors will take higher precedence**—This option specifies that in the event of objects with the same name, ancestor object take precedence over

Issue ID	Description
	descendent objects. In this case, the **Shared** objects take precedence over the vsys-specific object. This is a global setting and applies to all managed firewalls. In the example above, if the IP address for the **Shared** `SharedA01` object was `10.1.1.1` and the device group specific `SharedA01` was `10.2.2.2`, the `10.1.1.1` IP address takes precedence. Alternatively, you can remove the duplicate address objects from the device group configuration to allow only the **Shared** objects in your configuration.
PAN-233677	(PA-3410, PA-3420, PA-3430, PA-3440, PA-5410, PA-5420, PA-5430, and PA-5440 firewalls) By enabling Lockless QoS feature, a slight degradation in App-ID and Threat performance is expected.
PAN-223365 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The Panorama management server is unable to query any logs if the ElasticSearch health status for any Log Collector (**Panorama** > **Managed Collector** is degraded. **Workaround:** Log in to the Log Collector CLI and restart ElasticSearch. `admin`**`debug elasticsearch es-restart all`**
PAN-227368 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The GlobalProtect app cannot connect to a portal or gateway and GlobalProtect Clientless VPN users cannot access applications if authentication takes longer than 20 seconds. **Workaround:** Increase the TCP handshake timeout to the maximum value of 60 seconds.
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.
PAN-222253 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	On the Panorama management server, policy rulebase reordering when you **View Rulebase by Groups** (**Policy** > **<policy-rulebase>**) does not persist if you reorder the policy rulebase by dragging and dropping individual policy rules and then moving the entire tag group.
PAN-221015	On M-600 appliances in Panorama or Log Collector mode, the `es-1` and `es-2` ElasticSearch processes fail to restart when the M-600 appliance is rebooted. The results in the Managed

Issue ID	Description
This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	Collector ES health status (**Panorama** > **Managed Collectors** > **Health Status**) to be degraded. **Workaround:** Log in to the Panorama or Log Collector CLI experiencing degraded ElasticSearch health and restart all ElasticSearch processes. `admin>`**`debug elasticsearch es-restart optional all`**
PAN-220176	(PAN-OS 11.0.1-h2 hotfix) System process crashes might occur with VoIP traffic when NAT is enabled with Persistent Dynamic IP and Port settings.
PAN-218521 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The ElasticSearch process on the M-600 appliance in Log Collector mode may enter a continuous reboot cycle. This results in the M-600 appliance becoming unresponsive, consuming logging disk space, and preventing new log ingestion.

PAN-217307	The following Security policy rule (**Policies** > **Security**) filters return no results:
	`log-start eq no`
	`log-end eq no`
	`log-end eq yes`

PAN-216314	Upon upgrade or downgrade to or from PAN-OS 10.1.9 or 10.1.9-h1, offloaded application traffic sessions may disconnect after a period of time even if a session is active. The disconnect occurs after the application's default session timeout value is exceeded. This behavior affects only PAN-OS 10.1.9 and 10.1.9-h1. If you are on PAN-OS 10.1.9 and 10.1.9-h1, please use the following workaround. If you have already upgraded or downgraded to another PAN-OS version, use the following workaround in that version. **Workaround:** Run the CLI command **`debug dataplane internal pdt fe100 csr wr_sem_ctrl_ctr_scan_dis value 0`** to set the value to zero (0).
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync

Issue ID	Description
	on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`
PAN-212978	The Palo Alto Networks firewall stops responding when executing an SD-WAN debug operational CLI command.
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are

Issue ID	Description
	automatically unselected and any new tag created is applied to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207442	For M-700 appliances in an active/passive high availability (**Panorama** > **High Availability**) configuration, the `active-primary` HA peer configuration sync to the `secondary-passive` HA peer may fail. When the config sync fails, the job Results is `Successful` (**Tasks**), however the sync status on the **Dashboard** displays as `Out of Sync` for both HA peers. **Workaround**: Perform a local commit on the `active-primary` HA peer and then synchronize the HA configuration. **1.** Log in to the Panorama web interface of the `active-primary` HA peer. **2.** Select **Commit** and **Commit to Panorama**. **3.** In the `active-primary` HA peer **Dashboard**, click **Sync to Peer** in the High Availability widget.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy.

Issue ID	Description

	This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log forwarding to the disconnected Dedicated Log Collector is not impacted.
	Workaround: Restart the `mgmtsrvr` process on the Dedicated Log Collector.
	1. Log in to the Dedicated Log Collector CLI.
	2. Confirm the Dedicated Log Collector is disconnected from Panorama.
	`admin> show panorama-status`
	Verify the `Connected` status is `no`.
	3. Restart the `mgmtsrvr` process.
	`admin> debug software restart process management-server`

PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. • DLP cloud service • Advanced Threat Protection inline cloud analysis service • Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204689	Upon upgrade to PAN-OS 11.0.1, the following GlobalProtect settings do not work: • **Allow user to disconnect GlobalProtect App** > **Allow with Passcode**

Issue ID	Description
	• **Allow user to Disable GlobalProtect App** > **Allow with Passcode** • **Allow User to Uninstall GlobalProtect App** > **Allow with Password**
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-196146 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The VM-Series firewall on Azure does not boot up with a hostname (specified in an init-cgf.txt or user data) when bootstrapped.
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.

Issue ID	Description
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector. **Workaround:** Restart the log receiver service by running the following CLI command: **`debug software restart process log-receiver`**
PAN-193004 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The Panorama management server fails to delete old IP Tag data. This causes the `/opt/pancfg` partition to reach maximum capacity which impacts Panorama performance.
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.

Issue ID	Description
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if: • A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. • A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types: 1. Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. 2. Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report. 3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is

Issue ID	Description
	configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.3-h13 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.3-h12 Addressed Issues

Issue ID	Description
PAN-253317	(VM-Series firewalls on Microsoft Azure environments only) Fixed an issue where you were unable to log in to the firewall after a private data reset.
PAN-246960	Fixed an issue where firewalls failed to fetch content updates from the Wildfire Private Cloud due to an **Unsupported protocol** error.
PAN-244648	(PA-5200 Series only) Fixed an issue where the firewall did not boot up after a factory reset, and, with FIPS mode enabled, the firewall rebooted into maintenance mode.
PAN-238769	(VM-Series firewalls in FIPS-CC mode only) Fixed an issue where upgrading Panorama caused all locally created Security policy rule actions to Deny.

PAN-OS 11.0.3-h10 Addressed Issues

Issue ID	Description
PAN-252214	A fix was made to address CVE-2024-3400.
PAN-246707	Fixed an issue where failover was not triggered when multiple processes stopped responding.
PAN-244493	Fixed a memory limitation with mapping subinterfaces to VPCE endpoints for GCP IPS, Amazon Web Services (AWS) integration with GWLB, and NSX service chain mapping.
PAN-240347	Fixed an issue with the web interface where the **Dashboard** and a **Device Group** policy rule took longer than expected to load.
PAN-240166	Fixed an issue where, when explicit proxy was configured on the firewall, websites loaded more slowly than expected or did not load due to DNS using TCP.
PAN-239279	Fixed an issue related to web proxy where the *masterd* process monitoring envoy process memory restarted when it reached an unexpected limit.
PAN-230746	Fixed an issue on the web interface where device groups with a large number of managed firewalls displayed the **Policy** page more slowly than expected.

PAN-OS 11.0.3-h5 Addressed Issues

Issue ID	Description
PAN-242561	Fixed an issue where GlobalProtect tunnels disconnected shortly after being established when SSL was used as the transfer protocol.
PAN-241772	Fixed an issue where, when TLSv1.3 was used, an incorrect error message `invalid padding` was displayed instead of the expected error message `Invalid server certificate`.
PAN-240786	Fixed an issue on firewalls in HA configurations where VXLAN sessions were allocated, but not installed or freed, which resulted in a constant high session table usage that was not synced between the firewalls. This resulted in a session count mismatch.
PAN-240487	Fixed an issue where fan speed increased significantly after upgrading the firewall.
PAN-240197	Fixed an issue where configuration changes made in Panorama and pushed to the firewall were not reflected on the firewall.
PAN-238996	Fixed an issue where commits did not complete and remained in a pending state due to a race condition. With this fix, the commit will fail after 60 seconds and not remain in a pending state.
PAN-238769	(VM-Series firewalls in FIPS-CC mode only) Fixed an issue where upgrading Panorama caused all locally created Security policy rule actions to Deny.
PAN-236120	Fixed an issue where the /opt/panlogs partition reached capacity due to the logdb-quota for the User-ID log folder not being matched.
PAN-234929	Fixed an issue where tabs in the **ACC** such as **Network Activity Threat Activity** and **Blocked Activity** did not display data when you applied a **Time** filter of **Last 15 Minutes**, **Last Hour**, **Last 6 Hours**, or **Last 12 Hours**, and the data that was displayed with the **Last 24 Hours filter** was not accurate. Reports that were run against summary logs also did not display accurate results.
PAN-232800	Fixed an issue where critical disk usage for /opt/pancfg increased continuously and the system logs displayed the following message: `Disk usage for /opt/pancfg exceeds limit, <value> percent in use.`

Issue ID	Description
PAN-231802	Fixed an issue where an Advanced Routing BGP session flapped with commits when BGP peer authentication was enabled.
PAN-230746	Fixed an issue on the web interface where device groups with a large number of managed firewalls displayed the **Policy** page more slowly than expected.
PAN-229691	Fixed an issue on Panorama where configuration lock timeout errors were observed during normal operational commands by increasing thread stack size on Panorama.
PAN-228515	Fixed an issue where the Elasticsearch cluster health status displayed as yellow or red due to Elasticsearch SSH tunnel flaps.
PAN-228187	Fixed an issue where the management server restarted due to the virtual memory exceeding the limit.
PAN-227397	Fixed an issue where selective pushes on Panorama removed a previously pushed configuration from the firewalls.
PAN-227368	Fixed an issue where the GlobalProtect app was unable to connect to a portal or gateway and GlobalProtect Clientless VPN users were unable to access applications if authentication took more than 20 seconds.
PAN-223798	Fixed an issue on the firewall where, when Advanced Routing was enabled, PIM join messages were not sent to the RN due to a missing OIF.
PAN-223259	Fixed an issue where selective pushes failed with the error message `Failed to generate selective push configuration. Unable to retrieve last in-sync configuration for the device, either a push was never done or version is too old. Please try a full push.`
PAN-220907	(VM-Series firewalls only) Fixed an issue where large packets were dropped from the dataplane to the management plane, which caused OSPF neighborship to fail.
PAN-220659	Fixed an issue on the firewall where scheduled Antivirus updates failed when external dynamic lists were configured on the firewall.
PAN-218928	Fixed an issue where the *reportd* process stopped responding after querying logs or generating ACC reports with some filters.

PAN-OS 11.0.3-h3 Addressed Issues

Issue ID	Description
PAN-239769	Fixed an issue where object references in a rule were renamed, and while doing a selective revert of the changes with **Commit changes by me** caused a reference error.
PAN-237876	Extended the firewall Panorama root CA certificate which was previously set to expire on April 7th, 2024.
PAN-235476	Fixed an issue where threat logs from different Security zones were aggregated into one log.
PAN-233039	Fixed an issue where GENEVE encapsulated packets coming from a GFE Proxy mapped to an incorrect Security policy rule.
PAN-231507	(PA-1400 Series firewalls only) Fixed an issue where, when an HSCI interface was used as an HA2 interface, HA2 packets were intermittently dropped on the passive firewall, which caused the HA2 connection to flap due to missing HA2 keepalive messages.
PAN-230092	Fixed an issue where the *routed* process stopped responding when committing routing-related changes if Advanced routing was enabled.
PAN-227568	When a device certificate is installed, renewed, or removed, the firewall will reconnect to the WildFire cloud to use the newest certificate.
PAN-227064	Fixed an issue with high availability (HA) sync failure when performing a partial commit after creating a Security policy via REST API.
PAN-226792	Fixed an issue where the *logrcvr* process stored older content versions in the shared memory even when newer content updates were installed.
PAN-225886	Fixed an issue where, when explicit proxy mode was enabled for the web proxy, intermittent errors and unexpected TCP reconnections occurred.
PAN-218620	Fixed an issue where scheduled configuration exports and SCP server connection testing failed.
PAN-215576	Fixed an issue where the `userID-Agent` and `TS-Agent` certificates were set to expire on November 18, 2024. With this fix, the expiration date has been extended to January 2032.

Issue ID	Description
PAN-202361	Fixed an issue where packets queued to the *pan_task* process were still transmitted when the process was not responding.
PAN-193004	Fixed an issue where `/opt/pancfg` partition utilization reached 100%, which caused access to the Panorama web interface to fail.

PAN-OS 11.0.3-h1 Addressed Issues

Issue ID	Description
PAN-237871	(WF-500 appliances and PAN-DB private cloud deployments only) Fixed an issue where the `root-cert` was set to expire on December 31, 2023. With this fix, the expiration date has been extended.

PAN-OS 11.0.3 Addressed Issues

Issue ID	Description
PAN-231823	A fix was made to address CVE-2024-5916.
PAN-233954	Fixed an issue where the firewall was unable to retrieve correct groups from the LDAP server.
PAN-232059	Fixed an issue with memory management when processing large certificates using TLSv1.3.
PAN-229691	Fixed an issue on Panorama where configuration lock timeout errors were observed during normal operational commands by increasing thread stack size on Panorama.
PAN-228877	(PA-7050 firewalls only) Fixed an issue with OOM conditions which caused slot restarts due to `pan_cmd` consuming more than 300 MB.
PAN-227639	Fixed an issue where the **ACC** displayed an incorrect DNS-base application traffic byte count.
PAN-227376	Fixed an issue where a memory overrun caused the *all_task* process to stop responding.
PAN-227179	Fixed an issue where routes were not updated in the forwarding table.
PAN-226418	A CLI command was added to address an issue where long-lived sessions aged out even when there was ongoing traffic.
PAN-226198	Fixed an issue on Panorama where the *configd* process repeatedly restarted when attempting to make configuration changes.
PAN-225920	Fixed an issue where duplicate predict sessions didn't release NAT resources.
PAN-225183	Fixed an issue where SSH tunnels were unstable due to ciphers used as part of the high availability SSH configuration.
PAN-225169	Added a CLI command to view Cortex Data Lake queue usage.
PAN-224145	Fixed an issue in multi-vsys environments where, when Panorama was on a PAN-OS 10.2 release and the firewall was on a PAN-OS 10.1 release, commits failed on the firewall when inbound inspection mode was configured in the decryption policy rule.

Issue ID	Description
PAN-223852	Fixed an issue where *all_pktproc* stopped responding when network packet broker or decryption broker chains failed.
PAN-223741	Fixed an issue where the *mprelay* process stopped responding, which caused a slot restart when another slot rebooted.
PAN-223501	(PA-5200 Series and PA-7000 Series firewalls only) Fixed an issue where diagnostic information for the dataplane in the dp-monitor.log file was not complete.
PAN-223488	Fixed an issue where closed ElasticSearch shards were not deleted, which resulted in shard purging not working as expected.
PAN-223457	Fixed an issue where, if the number of group queries exceeded the Okta rate limit threshold, the firewall cleared the cache for the groups.
PAN-223317	Fixed an issue where SSL traffic failed with the error message: `Error: General TLS protocol error`.
PAN-223185	Fixed an issue where the *distributord* process stopped responding.
PAN-222957	Fixed an issue where managed firewalls did not reflect changes pushed by users who were not in a superuser role.
PAN-222941	Fixed an issue where viewing the latest logs took longer than expected due to log indexer failures.
PAN-222533	(VM-Series firewalls on Microsoft Azure and Amazon Web Services (AWS) environments) Added support for high availability (HA) link monitoring and path monitoring.
PAN-222418	Fixed an issue where the firewall intermittently recorded a reconnection message to the authentication server as an error, even if no disconnection occurred.
PAN-222162	Fixed an issue where the `show transceiver <interface>` CLI command showed the RX and TX powers as 0.00 mW.
PAN-221984	(VM-Series firewalls in Microsoft Azure environments only) Fixed an issue where an interface went down after a hotplug event and was only recoverable by restarting the firewall.
PAN-221836	Fixed an issue where improper SNI detection caused incorrect URL categorization.

Issue ID	Description
PAN-221787	Fixed an issue where a User Principal Name (UPN) was incorrectly required in the pre-logon machine certificate.
PAN-221647	Fixed an issue where the **Apps seen** value was not reflected on Panorama.
PAN-221577	Fixed an issue where a static route for a branch or hub over the respective virtual interface was not installed in the routing table even when the tunnel to the branch or hub was active.
PAN-221208	Fixed an issue where the tunnel monitor was unable to remain up when zone protection with Strict IP was enabled and NAT Traversal was applied.
PAN-221126	Fixed an issue where Email server profiles (**Device > Server Profiles > Email and Panorama > Server Profiles > Email**) to forward logs as email notifications were not forwarded in a readable format.
PAN-220910	Fixed an issue where an internal management plane NIC caused a kernel panic when doing a transmit due to the driver reinitializing under certain failure or change conditions on the same interface during transmit.
PAN-220899	Fixed an issue where you were unable to choose the manual GlobalProtect gateway.
PAN-220747	Fixed an issue where logs were not visible after restarting the log collector.
PAN-220626	Fixed an issue where system warning logs were written every 24 hours.
PAN-220448	Fixed an issue where the GlobalProtect client connection remained at the prelogin stage when Kerberos SSO failed and was unable to fall back to the realm authentication.
PAN-220401	Fixed an issue where, during a reboot, an unexpected error message was displayed that the syslog configuration file format was too old.
PAN-220281	(PA-7080 firewalls only) Fixed an issue where autocommitting changes after rebooting the Log Forwarding Card (LFC) caused the *logrcvr* process to fail to read the configuration file.
PAN-220180	Fixed an issue where configured botnet reports (**Monitor > Botnet**) were not generated.

Issue ID	Description
PAN-219813	Fixed an issue where the configuration log displayed incorrect information after a multidevice group **Validate-all** operation.
PAN-219659	Fixed an issue where root partition frequently filled up and the following error message was displayed: `Disk usage for / exceeds limit, xx percent in use, cleaning filesystem`.
PAN-219644	Fixed an issue where firewalls that forwarded logs to a syslog server over TLS (**Objects > Log Forwarding**) used the default Palo Alto Networks certificate instead of the configured custom certificate.
PAN-219623	Fixed an issue where, when a multidynamic group validate job was pushed on the firewall, logs displayed **Panorama push** instead of **ValidateAll push**.
PAN-219498	Fixed an issue where the **Threat ID/Name** detail in Threat logs was not included in syslog messages sent to Splunk.
PAN-219300	Fixed an issue where the task manager displayed only limited data.
PAN-219253	Fixed an issue where, after making changes in a template, the **Commit and Push** option was grayed out.
PAN-218988	Fixed an issue in FIPS mode where, when importing a certificate with a new private key, and the certificate used the name of an existing certificate on the Panorama, the following error message was displayed: `Mismatched public and private keys`.
PAN-218947	Fixed an issue where logs were not displayed in Elasticsearch under ingestion load.
PAN-218697	Fixed an issue where the ElasticSearch status frequently changed to red or yellow after a PAN-OS upgrade.
PAN-218663 and PAN-181876	A fix was made to address CVE-2024-2433
PAN-218404	Fixed an issue where *ikemgr* stopped responding due to receiving `CREATE_CHILD` messages with a malformed SA payload.
PAN-218340	Fixed an issue where selective pushes to template stack and multi device group pushes caused a buildup of resident memory, which caused the *configd* process to stop responding.

Issue ID	Description
PAN-218318	Fixed an issue where the firewall changed the time zone automatically instead of retrieving the correct time zone from the NTP server.
PAN-218273	Fixed an issue where TCP keepalive packets from the client to the server weren't forwarded when SSL decryption was enabled.
PAN-218267	Fixed an issue where a commit and push operation from Panorama to managed firewalls did not complete or took longer to complete than expected.
PAN-218252	Fixed an issue where the slot-1 data processor showed the status as down during an SNMP query.
PAN-218107	Fixed an issue with ciphers used for SSH tunnels where packet lengths were too large, which made the SSH tunnel unstable.
PAN-218046	Fixed an issue where the **Virtual Routers** (**Network > Virtual Routers**) setting was not available when configuring a custom admin role (**Device > Admin Roles**).
PAN-218001	(PA-400 Series firewalls only) Fixed an issue where shutdown commands rebooted the system instead of correctly triggering a shutdown.
PAN-217650	(VM-Series firewalls and Panorama virtual appliances in Microsoft Azure environments only) Fixed an issue where management interface Speed/Duplex was reported as unknown.
PAN-217493	Fixed an issue where superusers with read-only privileges were unable to view SCEP object configurations.
PAN-217169	Fixed an issue where the *logrcvr* stopped forwarding logs to the syslog server after a restart.
PAN-217053	Fixed an issue where the *configd* process stopped responding after a selective push to multiple device groups failed.
PAN-216957	Fixed an issue where allow list checks in an authentication profile did not work if the group Distinguished Name contains the ampersand (&) character.
PAN-216775	Fixed an issue where the *devsrvr* process stopped responding at `pan_cloud_agent_get_curl_connection()` and the URL cloud could not be connected.

Issue ID	Description
PAN-216366	Fixed an issue where, when custom signatures used a certain syntax, false positives were generated on devices on a PAN-OS 10.0 release.
PAN-216214	(Panorama managed firewalls in active/active HA configurations only) Fixed an issue where the HA status displayed as **Out of Sync** (**Panorama** > **Managed Devices** > **Health**) if local firewall configurations were made on one of the HA peers. This caused the next HA configuration sync to overwrite the local firewall configuration made on the HA peer.
PAN-216048	Fixed an issue where, when upgrading from a PAN-OS 9.1 release to a PAN-OS 10.0 release, commits failed with the error message: `hip profiles unexpected here`.
PAN-215767	Fixed an issue where, after a high availability failover, IKE SA negotiation failed with the error message `INVALID_SPI`, which resulted in temporary loss of traffic over some proxy IDs.
PAN-215655	Fixed an issue where, after a multidynamic group push, Security policy rules with the target device tag were added to a firewall that did not have the tag.
PAN-215338	(PA-5400 Series firewalls only) Fixed an issue where the inner VLAN tag for Q-in-Q traffic was stripped when forwarding.
PAN-215317	Fixed an issue where the dataplane stopped responding unexpectedly with the error message `comm exited with signal of 10`.
PAN-215066	Fixed an issue on Panorama where push scope rendering caused the **Commit and Push** or **Push to Devices** operation window to hang for several minutes.
PAN-214990	Fixed an issue where firewall copper ports flapped intermittently when device telemetry was enabled.
PAN-214987	Fixed an issue where **Application Filter** names were not random, and they matched or included internal protocol names.
PAN-214815	Fixed an issue where SNMP queries were not replied to due to an internal process timeout.
PAN-214727	Fixed an issue where a memory leak related to the *useridd* process resulted in an OOM condition, which caused the process to stop responding.

Issue ID	Description
PAN-214669	Fixed an issue where FIN and RESET packets were sent in reverse order.
PAN-214463	Fixed an issue where IKE re-key negotiation failed with a third-party vendor and the firewall acting as the initiator received a response with the VENDOR_ID payload and the error message `unexpected critical payload (type 43)`.
PAN-214201	Fixed an issue where, after exporting custom reports to CSV format, the letter **b** appeared at the beginning of each column.
PAN-214186	Fixed an issue where category length was incorrect, which caused the dataplane to restart.
PAN-213956	Fixed an issue where the firewall interface did not go down even after the peer link/switch port went down.
PAN-213931	Fixed an issue where the *logrcvr* process cache was not in sync with the mapping on the firewall.
PAN-213296	Fixed an issue where Single Log-out (SLO) was not correctly triggered from the firewall toward the client, which caused the client to not initiate the SLO request toward the identity provider (IdP). This resulted in the IdP not making the SLO callback to the firewall to remove the user.
PAN-213162	Fixed an issue where an SD-WAN object was not displayed under a child device group.
PAN-213112	Fixed an issue where executing the `show report directory-listing` CLI command resulted in no output after upgrading to a PAN-OS 10.1 release.
PAN-212978	Fixed an issue where the firewall stopped responding when executing an SD-WAN debug CLI command.
PAN-212726	Fixed an issue where RTP/RTCP packets were dropped for SIP calls by SIP ALG when the source NAT translation type was persistent **Dynamic IP And Port**.
PAN-212577	(PA-5200 Series and PA-7080 firewalls only) Fixed an issue where commits took longer than expected when more than 45,000 Security policy rules were configured.
PAN-212240	Fixed an issue where packet capture was logged for an unknown application session when packet capture logging was disabled.

Issue ID	Description
PAN-212057	Fixed an issue where Advanced Threat Prevention caused SSL delays when no URL licenses were present.
PAN-211441	Fixed a memory leak issue related to SSL crypto operations that resulted in failed commits.
PAN-211398	Fixed an issue where dataplane processes stopped responding when handling HTTP/2 streams.
PAN-211384	Fixed an issue where the size of the `redisthost_1` in the Redis database continuously increased, which caused an OOM condition.
PAN-210640	Fixed an issue where applications were not displayed after authenticating into the clientless VPN.
PAN-210502	Fixed an issue where Panorama was unable to convert to PAN-OS 9.1 syntax for WF-500 appliances.
PAN-210456	Fixed an issue where high latency occurred on PA-850-ZTP when SSL decryption was enabled.
PAN-210452	Fixed an issue where application packet capture (pcap) was not generated when Security policy rules were used as a filter.
PAN-210429	(VM-Series firewalls only) Fixed an issue where the HTTP service failed to come up on DHCP dataplane interfaces after rebooting the firewall, which resulted in health-check failure on HTTP/80 with a 503 error code on the public load balancer.
PAN-210364	Fixed an issue where high latency was observed when accessing internal web applications, which interrupted development activities related to the web server.
PAN-209585	The Palo Alto Networks QoS implementation now supports a new QoS mode called lockless QoS for PA-3400, PA-5410, PA-5420, PA-5430, and PA-5440 firewalls. For firewalls with higher bandwidth QoS requirements, the lockless QoS dedicates cores to the QoS function that improves QoS performance, resulting in improved throughput and latency.
PAN-209375	Fixed an issue on the firewall where log filtering did not work as expected.
PAN-209288	Fixed an issue where generating certificates with SCEP did not work.

Issue ID	Description
PAN-209172	Fixed an issue where the firewall was unable to handle GRE packets for Point-to-Point Tunneling Protocol (PPTP) connections.
PAN-209108	Fixed an issue where a Panorama in Management Only mode was unable to display logs from log collectors due to missing schema files.
PAN-208567	Fixed an issue with email formatting where, when a scheduled email contained two or more attachments, only one attachment was visible.
PAN-208438	Fixed an issue on Panorama where Security policy rules incorrectly displayed as disabled.
PAN-208395	Fixed an issue where user authentication failed in multi-vsys environments with the error message `User is not in allowlist` when an authentication profile was created in a shared configuration space.
PAN-208316	Fixed an issue where user-group names were unable to be configured as the source user via the `test security-policy-match` command.
PAN-208240	Fixed an issue where, when attempting to replace an existing certificate, importing a new certificate with the same name as the existing certificate failed due to mismatched public and private keys.
PAN-208198	Fixed an issue with firewalls in active/passive HA configurations where, after rebooting the passive firewall, interfaces were briefly shown as powered up, and then shown as down or shutdown.
PAN-208090	Fixed an issue where the ACC report did not display data when querying the filter for the fields **Source** and **Destination IP**.
PAN-207604	Fixed an issue where system logs continuously generated the log message `Not enough space to load content to SHM`.
PAN-207577	Fixed an issue where **Panorama > Setup > Interfaces** was not accessible for users with custom admin roles even when the interface option was selected for the custom admin roles.
PAN-206765	Fixed an issue where log forwarding filters involving negation did not work.
PAN-205015	Fixed an issue where not all users were included in the user group after an incremental sync between the firewall and the Cloud Identity Engine.

Issue ID	Description
PAN-204868	Fixed an issue where disk utilization was continuously high due to the log purger not sufficiently reducing the utilization level.
PAN-204718	(PA-5200 Series firewalls only) Fixed an issue where, after upgrading to PAN-OS 10.1.6-h3, a TACACS user login displayed the following error message during the first login attempt: `Could not chdir to home directory /opt/pancfg/home/user: Permission denied`.
PAN-203611	Fixed an issue where URL categorization was not recognized for URLs that contained more than 100 characters.
PAN-202524	Fixed an issue where the session ID was missing in the session details section of the `ingress-backlogs` XML API output.
PAN-199819	Fixed an issue where, if a decryption profile allowed TLSv1.3, but the server only supported TLSv1.2, and the cipher used by the first connection to the server was a CBC SHA2 cipher suite, the connection failed.
PAN-198509	Fixed an issue where commits failed due to insufficient CFG memory.
PAN-198453	Fixed an issue where you were unable to resize the **Description** pop-up window (**Policies** > **Security** > **Prerules**).
PAN-198050	Fixed an issue where `Connection to update server is successful` messages displayed even when connections failed.
PAN-197339	Fixed an issue where template configuration for the User-ID agent was not reflected on the template stack on Panorama appliances on PAN-OS 10.2.1.
PAN-196345	Fixed an issue where scheduled dynamic content updates failed to be retrieved by managed firewalls from Panorama when connectivity was slow.
PAN-189328	Fixed an issue where traffic belonging to the same session was sent out from different ECMP enabled interfaces.
PAN-187989	Fixed an issue where a user who did not have permissions of other access domains were able to view the commit and configuration lock.
PAN-185360	Fixed an issue where, when Authentication Portal Authentication was configured, `l3svc_ngx_error.log` and `l3svc_access.log` did not roll over after exceeding 10 megabytes, which caused the root partition to reach full utilization.

Issue ID	Description
PAN-180082	Fixed an issue where errors in *brdagent* logs caused dataplane path monitoring failure.
PAN-177227	(VM-Series firewalls on Amazon Web Services environments only) Fixed an issue where traffic sent from a GENEVE tunnel to the firewall was dropped if the firewall attempted to encapsulate traffic into an IPSec tunnel.
PAN-169586	Fixed an issue where scheduled log view reports in emails didn't match the monitor page query result for the same time interval.
PAN-160633	(PA-3200 Series, PA-5200 Series, and PA-7000 Series firewalls only) Fixed an issue where the dataplane restarted repeatedly due to an internal path monitoring failure until a power cycle.

PAN-OS 11.0.2 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.2.

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.

- PAN-OS 11.0.2 Known Issues
- PAN-OS 11.0.2-h5 Addressed Issues
- PAN-OS 11.0.2-h4 Addressed Issues
- PAN-OS 11.0.2-h3 Addressed Issues
- PAN-OS 11.0.2-h2 Addressed Issues
- PAN-OS 11.0.2-h1 Addressed Issues
- PAN-OS 11.0.2 Addressed Issues

PAN-OS 11.0.2 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.2. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-250062	Device telemetry might fail at configured intervals due to bundle generation issues.
PAN-243951	On the Panorama management sever in an active/passive High Availability (HA) configuration, managed devices (**Panorama** > **Managed Devices** > **Summary**) display as `out-of-sync` on the passive HA peer when configuration changes are made to the SD-WAN (**Panorama** > **SD-WAN**) configuration on the active HA peer. **Workaround:** Manually synchronize the Panorama HA peers. **1.** Log in to the Panorama web interface on the active HA peer. **2.** Select **Commit** and **Commit to Panorama** the SD-WAN configuration changes on the active HA peer. On the passive HA peer, select **Panorama** > **Managed Devices** > **Summary** and observe that the managed devices are now `out-of-sync`. **3.** Log in to the primary HA peer Panorama CLI and trigger a manual synchronization between the active and secondary HA peers. *request high-availability sync-to-remote running-config* **4.** Log back in to the active HA peer Panorama web interface and select **Commit** > **Push to Devices** and **Push**.
PAN-234408	Enterprise DLP cannot detect and block non-file based traffic for ChatGPT from traffic forwarded to the DLP cloud service from an NGFW.

Issue ID	Description
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-242910	On the Panorama management server, Panorama administrators (**Panorama** > **Administrators**) that are assigned a custom Panorama admin role (**Panorama** > **Admin Roles**) with **Push All Changes** enabled are unable to push configuration changes to managed firewalls when **Managed Devices** and **Push For Other Admins** are disabled.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-231507 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On PA-1400 Series firewalls only, when an HSCI interface is used as an HA2 interface, HA2 packets are intermittently dropped on the passive device, which can cause the HA2 connection to flap due to missing HA2 keepalive messages. Workaround: use data ports configured as HA2 interface.
PAN-228515	The EleasticSearch SSH flaps on the M-600 appliance in Panorama or Log Collector mode. This causes logs to not display on the Panorama management server (**Monitor** > **Logs**) and the Log Collector health status (**Panorama** > **Managed Collectors** > **Status**) to display as degraded.
PAN-228273	On the Panorama management server in FIPS-CC mode, the ElasticSearch cluster fails to come up and the `show log-collector-es-cluster health` command displays the `status` is `red`. This results in log ingestion issues for Panorama in Panorama only or Log Collector mode.
PAN-227344	On the Panorama management server, PDF Summary Reports (**Monitor** > **PDF Reports** > **Manage PDF Summary**) display no data and are blank when predefined reports are included in the summary report.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.
PAN-225337 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On the Panorama management server, the configuration push to a multi-vsys firewall fails if you: 1. Create a **Shared** and vsys-specific device group configuration object with an indentical name. For example,

Issue ID	Description
	a **Shared** address object called `SharedA01` and a vsys-specific address object also called `SharedA01`. 2. Reference the **Shared** object in another **Shared** configuration. For example, reference the **Shared** address object (`SharedA01`) in a **Shared** address group called `SharedAG1`. 3. Use the **Shared** configuration object with the reference in a vsys-specific configuration. For example, reference the **Shared** address group (`SharedAG1`) in a vsys-specific policy rule. **Workaround:** Select **Panorama** > **Setup** > **Management** and edit the Panorama Settings to enable one of the following: • **Shared Unused Address and Service Objects with Devices**—This options pushes all **Shared** objects, along with device group specific objects, to managed firewalls. This is a global setting and applies to all managed firewalls, and may result in pushing too many configuration objects to your managed firewalls. • **Objects defined in ancestors will take higher precedence**—This option specifies that in the event of objects with the same name, ancestor object take precedence over descendent objects. In this case, the **Shared** objects take precedence over the vsys-specific object. This is a global setting and applies to all managed firewalls. In the example above, if the IP address for the **Shared** `SharedA01` object was `10.1.1.1` and the device group specific `SharedA01` was `10.2.2.2`, the `10.1.1.1` IP address takes precedence. Alternatively, you can remove the duplicate address objects from the device group configuration to allow only the **Shared** objects in your configuration.
PAN-223488 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Closed ElasticSearch shards are not deleted from the Panorama M-Series and virtual appliance. This causes the ElasticSearch shard purging to not work as expected, resulting in high disk usage.
PAN-223365 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The Panorama management server is unable to query any logs if the ElasticSearch health status for any Log Collector (**Panorama** > **Managed Collector** is degraded.

Issue ID	Description
	Workaround: Log in to the Log Collector CLI and restart ElasticSearch. `admindebug elasticsearch es-restart all`
PAN-227368 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The GlobalProtect app cannot connect to a portal or gateway and GlobalProtect Clientless VPN users cannot access applications if authentication takes longer than 20 seconds. **Workaround:** Increase the TCP handshake timeout to the maximum value of 60 seconds.
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.
PAN-222253 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	On the Panorama management server, policy rulebase reordering when you **View Rulebase by Groups** (**Policy** > **<policy-rulebase>**) does not persist if you reorder the policy rulebase by dragging and dropping individual policy rules and then moving the entire tag group.
PAN-221126 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Email server profiles (**Device** > **Server Profiles** > **Email** and **Panorama** > **Server Profiles** > **Email**) to forward logs as email notifications are not forwarded in a readable format. **Workaround:** Use a **Custom Log Format** to forward logs as email notifications in a readable format.
PAN-221015 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On M-600 appliances in Panorama or Log Collector mode, the `es-1` and `es-2` ElasticSearch processes fail to restart when the M-600 appliance is rebooted. The results in the Managed Collector ES health status (**Panorama** > **Managed Collectors** > **Health Status**) to be degraded. **Workaround:** Log in to the Panorama or Log Collector CLI experiencing degraded ElasticSearch health and restart all ElasticSearch processes. `admin>debug elasticsearch es-restart optional all`
PAN-220180 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Configured botnet reports (**Monitor** > **Botnet**) are not generated.

Issue ID	Description
PAN-220176	(PAN-OS 11.0.1-h2 hotfix) System process crashes might occur with VoIP traffic when NAT is enabled with Persistent Dynamic IP and Port settings.
PAN-219644 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Firewalls forwarding logs to a syslog server over TLS (**Objects** > **Log Forwarding**) use the default Palo Alto Networks certificate instead of the custom certificate configured on the firewall.
PAN-218521 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The ElasticSearch process on the M-600 appliance in Log Collector mode may enter a continuous reboot cycle. This results in the M-600 appliance becoming unresponsive, consuming logging disk space, and preventing new log ingestion.

PAN-217307	The following Security policy rule (**Policies** > **Security**) filters return no results:
	`log-start eq no`
	`log-end eq no`
	`log-end eq yes`

PAN-216314	Upon upgrade or downgrade to or from PAN-OS 10.1.9 or 10.1.9-h1, offloaded application traffic sessions may disconnect after a period of time even if a session is active. The disconnect occurs after the application's default session timeout value is exceeded. This behavior affects only PAN-OS 10.1.9 and 10.1.9-h1. If you are on PAN-OS 10.1.9 and 10.1.9-h1, please use the following workaround. If you have already upgraded or downgraded to another PAN-OS version, use the following workaround in that version. **Workaround:** Run the CLI command **`debug dataplane internal pdt fe100 csr wr_sem_ctrl_ctr_scan_dis value 0`** to set the value to zero (0).
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.

Issue ID	Description
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`
PAN-212978	The Palo Alto Networks firewall stops responding when executing an SD-WAN debug operational CLI command.
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are automatically unselected and any new tag created is applied

Issue ID	Description
	to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207442	For M-700 appliances in an active/passive high availability (**Panorama** > **High Availability**) configuration, the `active-primary` HA peer configuration sync to the `secondary-passive` HA peer may fail. When the config sync fails, the job Results is `Successful` (**Tasks**), however the sync status on the **Dashboard** displays as `Out of Sync` for both HA peers. **Workaround**: Perform a local commit on the `active-primary` HA peer and then synchronize the HA configuration. **1.** Log in to the Panorama web interface of the `active-primary` HA peer. **2.** Select **Commit** and **Commit to Panorama**. **3.** In the `active-primary` HA peer **Dashboard**, click **Sync to Peer** in the High Availability widget.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy. This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log

Issue ID	Description

	forwarding to the disconnected Dedicated Log Collector is not impacted.
	Workaround: Restart the `mgmtsrvr` process on the Dedicated Log Collector.
	1. Log in to the Dedicated Log Collector CLI.
	2. Confirm the Dedicated Log Collector is disconnected from Panorama.
	`admin> show panorama-status`
	Verify the `Connected` status is `no`.
	3. Restart the `mgmtsrvr` process.
	`admin> debug software restart process management-server`

PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. • DLP cloud service • Advanced Threat Protection inline cloud analysis service • Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204689	Upon upgrade to PAN-OS 11.0.1, the following GlobalProtect settings do not work: • **Allow user to disconnect GlobalProtect App** > **Allow with Passcode** • **Allow user to Disable GlobalProtect App** > **Allow with Passcode**

Issue ID	Description
	- **Allow User to Uninstall GlobalProtect App** > **Allow with Password**
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-196146 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The VM-Series firewall on Azure does not boot up with a hostname (specified in an init-cgf.txt or user data) when bootstrapped.
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall

Issue ID	Description
	running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector. **Workaround:** Restart the log receiver service by running the following CLI command: `debug software restart process log-receiver`
PAN-193004 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The Panorama management server fails to delete old IP Tag data. This causes the `/opt/pancfg` partition to reach maximum capacity which impacts Panorama performance.
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if:

Issue ID	Description
	- A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. - A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types: 1. Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. 2. Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report. 3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more

Issue ID	Description
	likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.2-h5 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.2-h4 Addressed Issues

Issue ID	Description
PAN-252214	A fix was made to address CVE-2024-3400.

PAN-OS 11.0.2-h3 Addressed Issues

Issue ID	Description
PAN-238792	Fixed the following device certificate issues: • The firewall was unable to automatically renew the device certificate. • Fetching device certificates failed incorrectly with the error message `OTP is not valid`. • Firewalls disconnected from Cortex Data Lake after renewing the device certificate. • The device certificate was not correctly generated on the log forwarding card (LFC). • WildFire cloud logs did not log thermite certificate usage status.
PAN-237876	Extended the firewall Panorama root CA certificate which was previously set to expire on April 7th, 2024.
PAN-231771	Fixed an issue where the firewall issued /box/getserv/ requests with PAN-OS 7.1.0 and did not take device certificates.
PAN-227568	When a device certificate is installed, renewed, or removed, the firewall will reconnect to the WildFire cloud to use the newest certificate.
PAN-215576	Fixed an issue where the `userID-Agent` and `TS-Agent` certificates were set to expire on November 18, 2024. With this fix, the expiration date has been extended to January 2032.

PAN-OS 11.0.2-h2 Addressed Issues

Issue ID	Description
PAN-230250	Fixed an issue where selected applications serving partial content were dropped when Inline Cloud Analysis in Anti-Spyware was enabled.
PAN-223787	(PA-400 Series and PA-1400 Series firewalls only) Fixed an issue where commits failed with the error message `Error unserializing profile objects failed to handle CONFIG_UPDATE_START`.
PAN-222957	Fixed an issue where managed firewalls did not reflect changes pushed by users that were not in a Superuser role.
PAN-218107	Fixed an issue with ciphers used for SSH tunnels where packet lengths were too large, which made the SSH tunnel unstable.
PAN-214942	Fixed an issue where SD-WAN traffic failed over to a non-member path after a flap of an SD-WAN virtual interface.
PAN-204868	Fixed an issue where disk utilization was continuously high due to the log purger not sufficiently reducing the utilization level.

PAN-OS 11.0.2-h1 Addressed Issues

Issue ID	Description
PAN-225184	Fixed an issue where disk space utilization was higher than expected due to excessive logging for a `KNI: Out of memory` event under a specific traffic load condition.
PAN-222712	(PA-5450 firewalls only) Fixed a low frequency DPC restart issue.
PAN-221984	(VM-Series firewalls in Microsoft Azure environments only) Fixed an issue where an interface went down after a hotplug event and was only recoverable by restarting the firewall.
PAN-220921	Fixed an issue where return tunnel traffic was dropped with the counter `flow_tunnel_encap_err` when **Enforce Symmetric Return** was enabled in a Policy Based Forwarding rule.
PAN-195439	(VM-Series firewalls in Microsoft Azure environments only) Fixed an issue where the dataplane interface status went down after a hotplug event triggered by Azure infrastructure.
PAN-193004	Fixed an issue where `/opt/pancfg` partition utilization reached 100%, which caused access to the Panorama web interface to fail.

PAN-OS 11.0.2 Addressed Issues

Issue ID	Description
PAN-231823	A fix was made to address CVE-2024-5916.
PAN-221708	Fixed an issue where temporary files remained under `/opt/pancfg/tmp/sw-images/` even after manually uploading the content or AV file to the firewall.
PAN-221519	(VM-Series firewalls only) Fixed an issue where the *all_task* process stopped responding due to DPDK driver compatibility issues.

PAN-219686	Fixed an issue where a device group push operation from Panorama failed with the following error on managed firewalls.
	`vsys -> vsys1 -> plugins unexpected here`
	`vsys is invalid`
	`Commit failed`

PAN-218644	Fixed an issue where the firewall generated incorrect VSA attribute codes when radius was configured with EAP based authentication protocols.
PAN-218335	Fixed an issue with hardware destination MAC filtering on the Log Processing Card (LPC) that caused the logging card interface to be susceptible to unicast flooding.
PAN-218264	(PA-3400 and PA-1400 Series firewalls only) Fixed an issue where packet drops occurred due to slow servicing of internal hardware queries.
PAN-217681	Fixed an issue caused by out of order TCP segments where the FIN flag and TCP data was truncated in a packet, which resulted in retransmission failure.
PAN-217581	Fixed an issue where the firewall did not initiate scheduled log uploads to the FTP server.
PAN-217493	Fixed an issue where superusers with read-only privileges were unable to view SCEP object configurations.
PAN-217484	Fixed an issue where the *rasmgr* process used 100% CPU due to a maximum duration timer not being set, which caused the GlobalProtect gateway to be unavailable.

Issue ID	Description
PAN-217477	Fixed an issue where the drop counter was incremented incorrectly. Drop counter calculations did not account for failures to send out logs from logrcvr/logd to syslog-ng.
PAN-217284	Fixed an intermittent issue where LACP flap occurred when the LACP transmission rate was set to **Fast**.
PAN-216996	Fixed an issue where, after upgrading Panorama to PAN-OS 10.1.9, multiple User-ID alerts were generated every 10 minutes.
PAN-216821	Fixed an issue where the *reportd* process stopped responding after upgrading an M-200 appliance to PAN-OS 11.0.1.
PAN-216710	Fixed an issue with firewalls in active/active HA configurations where GlobalProtect disconnected when the original suspected Active-Primary firewall became Active-Secondary.
PAN-216590	Fixed an issue where User-ID logs in Panorama displayed incorrect results for the filter `not (ugflags has user-group-found)`.
PAN-216360	Fixed an issue on Panorama where **No Default Selections** under **Push to Devices** was intermittently deselected after performing a commit operation.
PAN-216170	(PA-400 Series firewalls in HA configurations only) Fixed an issue where an HA switchover took longer than expected to bring up ports on the newly active firewall.
PAN-216036	Fixed an issue where the `all_pktproc` process stopped responding, which caused the firewall to enter a nonfunctional state.
PAN-215911	Fixed an issue that resulted in a race condition, which caused the *configd* process to stop responding.
PAN-215899	Fixed an issue with Panorama appliances in high availability (HA) configurations where configuration synchronization between the HA peers failed.
PAN-215857	Fixed an issue where the option to reboot the entire firewall was visible to vsys admins.
PAN-215808	Fixed an issue where after upgrading to PAN-OS 10.1, the log-forwarding rate towards the Syslog server was reduced. The overall log-forwarding rate has also been improved.

Issue ID	Description
PAN-215780	Fixed an issue where, changes to Zone Protection profiles made via XML API were not reflected in the Zone Protection configuration.
PAN-215778	Fixed an issue where API Get requests for `/config` timed out due to insufficient buffer size.
PAN-215503	Fixed a memory related issue where the `MEMORY_POOL` address was mapped incorrectly.
PAN-215496	Fixed an issue where 100G ports did not come up with BIDI QSFP modules.
PAN-215324	(PA-5400 Series firewalls with Jumbo Frames enabled only) Fixed an issue with CPU throttling and buffer depletion.
PAN-215315	Fixed an issue where the dataplane stopped responding due to ager and inline packet processing occurring concurrently on different cores for the same session.
PAN-215125	Fixed an issue where false negatives occurred for some script samples.
PAN-214925	Fixed an issue where temporary files remained in their temporary locations even after manually uploading the files to the firewall.
PAN-214889	Fixed an issue where commits took longer than expected due to application dependency checks.
PAN-214847	Fixed an issue where, when certificate authentication for admin user authentication was enabled, vulnerability scans that used usernames or passwords against the management interface reported a vulnerability due to a missing HSTS header in the **Access Denied** response page.
PAN-214634	Fixed an issue where an elink parser did not work.
PAN-214337	Fixed an issue on the firewall related to the `gp_broker` configuration transform that led to longer commit times.
PAN-214187	Fixed an issue where superreaders were able to execute the `request restart system` CLI command.
PAN-214100	Fixed an issue where selecting a threat name under *Threat Monitor* displayed the threat ID instead of the threat name.
PAN-214037	(PA-5440, PA-5430, PA-5420, and PA-5410 firewalls only) Fixed an issue where firewalls in active/active HA configurations experienced packet drop when running asymmetric traffic.

Issue ID	Description
PAN-214026	Fixed an issue where, when using an ECMP `weighted-round-robin` algorithm, traffic was not redistributed among the links proportionally as expected from the configuration.
PAN-213942	(PA-400 Series firewalls) Fixed an issue where the firewall required an explicit allow rule to forward broadcast traffic.
PAN-213932	Fixed an issue where, when an incorrect log filter was configured, the commit did not fail.
PAN-213746	Fixed an issue on Panorama where the Hostkey displayed as **undefined** if a SSH Service Profile Hostkey configured in a Template from the Template Stack was overridden.
PAN-212848	Fixed an issue where attempting to change the disk-usage cleanup threshold to 90 resulted in the error message `Server error : op command for client dagger timed out as client is not available`.
PAN-212726	Fixed an issue where RTP/RTCP packets were dropped for SIP calls by SIP ALG when the source NAT translation type was persistent **Dynamic IP And Port**.
PAN-212530	Fixed an issue on log collectors where root partition reached 100% utilization.
PAN-212409	Fixed an issue where there were duplicate IPSec Security Associations (SAs) for the same tunnel, gateway, or proxy ID.
PAN-211997	Fixed an issue where large OSPF control packets were fragmented, which caused the neighborship to fail.
PAN-211887	Fixed an issue on Panorama that caused recently committed changes to not be displayed when previewing the changes to push to device groups.
PAN-211843	Fixed an issue where renaming a Zone Protection profile failed with the error message `Obj does not exist.`
PAN-211602	Fixed an issue where, when viewing a WildFire Analysis Report via the web interface, the **detailed log view** was not accessible if the browser window was resized.
PAN-211519	Fixed an issue where RTP/RTCP packets were dropped for SIP calls by SIP ALG when the source NAT translation type was persistent **Dynamic IP And Port**.

Issue ID	Description
PAN-211422	Fixed an issue where the `show session packet-buffer-protection buffer-latency` CLI command randomly displayed incorrect values.
PAN-211242	Fixed an issue where missed heartbeats caused the Data Processing Card (DPC) and its corresponding Network Processing Card (NPC) to restart due to internal packet path monitoring failure.
PAN-211041	(Panorama virtual appliances only) Fixed an issue where DHCP assigned interfaces did not send `ICMP unreachable - Fragmentation needed` messages when the received packets were higher than the maximum transmission unit (MTU).
PAN-210921	(Panorama appliances in Legacy Mode only) Fixed an issue where **Blocked Browsing Summary by Website** in the user activity report contained scrambled characters.
PAN-210919	Fixed an issue where the Data Processing Card remained in a `Starting` state after a restart.
PAN-210875	Fixed an issue where the *pan_task* process stopped responding due to software packet buffer 3 trailer corruption, which caused the firewall to restart.
PAN-210736	Fixed an issue where configuration changes related to the SSH service profile were not reflected when pushed from Panorama. With this fix, the deletion of ciphers, MAC, and kex fields of SSH server profiles and HA profiles won't clear the values under template stacks and will retain the values configured from templates.
PAN-210661	Fixed an issue where firewalls disconnected from Cortex Data Lake after renewing the device certificate.
PAN-210563	Fixed an issue on Panorama where Security policy rules with a **Tag** target did not appear in the pre-rule list of a dynamic address group that was part of the tag.
PAN-209898	Fixed an issue where the *logrcvr* process stopped due to memory corruption.
PAN-209696	Fixed an issue where link-local address communication for IPv6, BFD, and OSPFv3 neighbors was dropped when IP address spoofing check was enabled in a Zone Protection profile.
PAN-209683	Fixed an issue where Panorama was unable to retrieve IP address-to-username mapping from a firewall on a PAN-OS 8.1 release.

Issue ID	Description
PAN-209660	Fixed an issue where a selective push from Panorama to multiple firewalls failed due to a missing configuration file, which caused a communication error.
PAN-209617	Fixed an issue with firewalls in active/passive HA configurations where the passive firewall created an incorrect SCTP association due to the HA sync messages from the active firewall having an incorrect value.
PAN-209275	Fixed an issue where Override cookie authentication into the GlobalProtect gateway failed when an allow list was configured under the authentication profile.
PAN-209021	Fixed an issue where packets were fragmented when SD-WAN VPN tunnel was configured on aggregate ethernet interfaces and sub-interfaces.
PAN-208877	Fixed an issue where the *all_task* process stopped responding when freeing the HTTP2 stream, which caused the dataplane to go down.
PAN-208737	Fixed an issue where domain information wasn't populated in IP address-to-username matching after a successful GlobalProtect authentication using an authentication override cookie.
PAN-208325	(PA-5400 Series, PA-3400 Series, and PA-400 Series only) Fixed an issue where the firewall was unable to automatically renew the device certificate.
PAN-208201	Fixed an issue on the firewall where the modified date and time was incorrectly updated after a commit operation, PAN-OS upgrade, or reboot.
PAN-207842	Fixed an issue where WildFire Analysis Reports were not visible when the WF-500 appliance was on private cloud.
PAN-207741	Fixed an issue where Large Scale VPN (LSVPN) Portal authentication failed with the error `invalid http response. return error(Authentication failed; Retry authentication` when the satellite connected to more than one portal.
PAN-207700	Fixed an issue where the `show system info` and `show system ztp status` CLI commands displayed a different Zero Touch Provisioning (ZTP) status if a firewall upgrade was initiated from Panorama before the initial commit push succeeded.
PAN-207562	Fixed an issue where the shard count displayed by the `show log-collector-es-cluster health` CLI command was higher than

Issue ID	Description
	the recommended limit. The recommended limit can be calculated with the formula 20* heap-memory * no-of-data-nodes.
PAN-206396	Fixed an issue where HIP report flip and HIP checks failed when a user was part of multiple user groups with different domains.
PAN-206333	Fixed an issue where the **Include/Exclude IP** filter under **Data Distribution** did not work correctly.
PAN-206253	(PA-1400 Series and PA-3400 Series firewalls only) Fixed an issue where the default log rate was too low and the maximum configurable log rate was incorrectly capped, which caused the firewall to not generate logs at more than 6826 logs per second.
PAN-205955	Fixed an issue where RAID rebuilds occurred even with healthy disks and a clean shutdown.
PAN-205513	Fixed an issue where the stats dump file generated by Panorama for a device firewall differed from the stats dump file generated by the managed device.
PAN-205086	Fixed an issue where DNS Security categories were able to be deleted from Spyware profiles.
PAN-204838	Fixed an issue where the `dot1q` VLAN tag was missing in ARP reply packets.
PAN-204718	(PA-5200 Series firewalls only) Fixed an issue where, after upgrading to PAN-OS 10.1.6-h3, a TACACS user login displayed the following error message during the first login attempt: `Could not chdir to home directory /opt/pancfg/home/user: Permission denied`.
PAN-204238	Fixed an issue where, when **View Rulebase as Groups** was enabled, the **Tags** field did not display a scroll down arrow for navigation.
PAN-204068	Fixed an issue where a newly created vsys (virtual system) in a template was not able to be pushed from Panorama to the firewall.
PAN-203330	Fixed an issue where the certificate for an External Dynamic List (EDL) incorrectly changed from invalid to valid, which caused the EDL file to be removed.
PAN-202963	Fixed an issue where the system log message `dsc HA state is changed from 1 to 0` was generated with the severity **High**. With this fix, the severity was changed to **Info**.

Issue ID	Description
PAN-202795	Fixed an issue where file identification failed with a large HTTP header.
PAN-201721	Fixed an issue with firewalls in HA configurations where HA setup generated the error `mismatch due to device update` during a content update even though the version was the same.
PAN-200019	Fixed an issue on Panorama where **Virtual Routers** (**Network > Virtual Routers**) was not available when configuring a custom Panorama admin role (**Panorama > Admin Roles**).
PAN-199557	Fixed an issue on Panorama where virtual memory usage exceeded the set limit, which caused the *configd* process to restart.
PAN-197121	Fixed an issue where incorrect user details were displayed under the **USER DETAIL** drop-down (**ACC > Network activity > User activity**).
PAN-196309	(PA-5450 firewalls only) Fixed an issue where a firewall configured with a Policy-Based Forwarding policy flapped when a commit was performed, even when the next hop was reachable.
PAN-195788	Fixed an issue where zip files did not download when applying Security inspection and the following error message displayed: `resources-unavailable`.
PAN-195695	Fixed an issue where the AppScope Summary report and PDF report export function did not work as expected.
PAN-192456	Fixed an issue where GlobalProtect SSL VPN processing during a high traffic load caused the dataplane to stop responding.
PAN-189666	Fixed an issue where GlobalProtect portal connections failed after random commits when multiple agent configurations were provisioned and configuration selection criteria using certificate profile was used.
PAN-187763	Fixed an issue where DNS Security logs did not display a threat category, threat name, or threat ID when domain names contained 64 or more characters.
PAN-187279	Fixed an issue where not all quarantined devices were displayed as expected.
PAN-184630	Fixed an issue where TLS clients, such as those using OpenSSL 3.0, enforced the TLS renegotiation extension (RFC 5746).

PAN-OS 11.0.1 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.1.

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.

- PAN-OS 11.0.1 Known Issues
- PAN-OS 11.0.1-h5 Addressed Issues
- PAN-OS 11.0.1-h4 Addressed Issues
- PAN-OS 11.0.1-h3 Addressed Issues
- PAN-OS 11.0.1-h2 Addressed Issues
- PAN-OS 11.0.1 Addressed Issues

PAN-OS 11.0.1 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.1. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-250062	Device telemetry might fail at configured intervals due to bundle generation issues.
PAN-243951	On the Panorama management sever in an active/passive High Availability (HA) configuration, managed devices (**Panorama** > **Managed Devices** > **Summary**) display as `out-of-sync` on the passive HA peer when configuration changes are made to the SD-WAN (**Panorama** > **SD-WAN**) configuration on the active HA peer. **Workaround:** Manually synchronize the Panorama HA peers. **1.** Log in to the Panorama web interface on the active HA peer. **2.** Select **Commit** and **Commit to Panorama** the SD-WAN configuration changes on the active HA peer. On the passive HA peer, select **Panorama** > **Managed Devices** > **Summary** and observe that the managed devices are now `out-of-sync`. **3.** Log in to the primary HA peer Panorama CLI and trigger a manual synchronization between the active and secondary HA peers. *request high-availability sync-to-remote running-config* **4.** Log back in to the active HA peer Panorama web interface and select **Commit** > **Push to Devices** and **Push**.
PAN-234408	Enterprise DLP cannot detect and block non-file based traffic for ChatGPT from traffic forwarded to the DLP cloud service from an NGFW.

Issue ID	Description
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-242910	On the Panorama management server, Panorama administrators (**Panorama** > **Administrators**) that are assigned a custom Panorama admin role (**Panorama** > **Admin Roles**) with **Push All Changes** enabled are unable to push configuration changes to managed firewalls when **Managed Devices** and **Push For Other Admins** are disabled.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-228515	The EleasticSearch SSH flaps on the M-600 appliance in Panorama or Log Collector mode. This causes logs to not display on the Panorama management server (**Monitor** > **Logs**) and the Log Collector health status (**Panorama** > **Managed Collectors** > **Status**) to display as degraded.
PAN-228273	On the Panorama management server in FIPS-CC mode, the ElasticSearch cluster fails to come up and the `show log-collector-es-cluster health` command displays the `status` is `red`. This results in log ingestion issues for Panorama in Panorama only or Log Collector mode.
PAN-227344	On the Panorama management server, PDF Summary Reports (**Monitor** > **PDF Reports** > **Manage PDF Summary**) display no data and are blank when predefined reports are included in the summary report.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.
PAN-225337 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On the Panorama management server, the configuration push to a multi-vsys firewall fails if you: **1.** Create a **Shared** and vsys-specific device group configuration object with an indentical name. For example, a **Shared** address object called `SharedA01` and a vsys-specific address object also called `SharedA01`. **2.** Reference the **Shared** object in another **Shared** configuration. For example, reference the **Shared** address object (`SharedA01`) in a **Shared** address group called `SharedAG1`.

Issue ID	Description
	3. Use the **Shared** configuration object with the reference in a vsys-specific configuration. For example, reference the **Shared** address group (`SharedAG1`) in a vsys-specific policy rule. **Workaround:** Select **Panorama** > **Setup** > **Management** and edit the Panorama Settings to enable one of the following: • **Shared Unused Address and Service Objects with Devices**—This options pushes all **Shared** objects, along with device group specific objects, to managed firewalls. This is a global setting and applies to all managed firewalls, and may result in pushing too many configuration objects to your managed firewalls. • **Objects defined in ancestors will take higher precedence**—This option specifies that in the event of objects with the same name, ancestor object take precedence over descendent objects. In this case, the **Shared** objects take precedence over the vsys-specific object. This is a global setting and applies to all managed firewalls. In the example above, if the IP address for the **Shared** `SharedA01` object was `10.1.1.1` and the device group specific `SharedA01` was `10.2.2.2`, the `10.1.1.1` IP address takes precedence. Alternatively, you can remove the duplicate address objects from the device group configuration to allow only the **Shared** objects in your configuration.
PAN-223488 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Closed ElasticSearch shards are not deleted from the Panorama M-Series and virtual appliance. This causes the ElasticSearch shard purging to not work as expected, resulting in high disk usage.
PAN-223365 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The Panorama management server is unable to query any logs if the ElasticSearch health status for any Log Collector (**Panorama** > **Managed Collector** is degraded. **Workaround:** Log in to the Log Collector CLI and restart ElasticSearch. `admindebug elasticsearch es-restart all`
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.

Issue ID	Description
PAN-222253 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	On the Panorama management server, policy rulebase reordering when you **View Rulebase by Groups** (**Policy** > **<policy-rulebase>**) does not persist if you reorder the policy rulebase by dragging and dropping individual policy rules and then moving the entire tag group.
PAN-221126 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Email server profiles (**Device** > **Server Profiles** > **Email** and **Panorama** > **Server Profiles** > **Email**) to forward logs as email notifications are not forwarded in a readable format. **Workaround:** Use a **Custom Log Format** to forward logs as email notifications in a readable format.
PAN-221015 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On M-600 appliances in Panorama or Log Collector mode, the `es-1` and `es-2` ElasticSearch processes fail to restart when the M-600 appliance is rebooted. The results in the Managed Collector ES health status (**Panorama** > **Managed Collectors** > **Health Status**) to be degraded. **Workaround:** Log in to the Panorama or Log Collector CLI experiencing degraded ElasticSearch health and restart all ElasticSearch processes. `admin>debug elasticsearch es-restart optional all`
PAN-220180 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Configured botnet reports (**Monitor** > **Botnet**) are not generated.
PAN-220176	(PAN-OS 11.0.1-h2 hotfix) System process crashes might occur with VoIP traffic when NAT is enabled with Persistent Dynamic IP and Port settings.
PAN-219644 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Firewalls forwarding logs to a syslog server over TLS (**Objects** > **Log Forwarding**) use the default Palo Alto Networks certificate instead of the custom certificate configured on the firewall.
PAN-218521 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The ElasticSearch process on the M-600 appliance in Log Collector mode may enter a continuous reboot cycle. This results in the M-600 appliance becoming unresponsive, consuming logging disk space, and preventing new log ingestion.

Issue ID	Description

PAN-217307	The following Security policy rule (**Policies** > **Security**) filters return no results:
	`log-start eq no`
	`log-end eq no`
	`log-end eq yes`

PAN-216821 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	The `reportd` process crashes after you successfully upgrade an M-200 appliance to PAN-OS 10.2.4.
PAN-216314	Upon upgrade or downgrade to or from PAN-OS 10.1.9 or 10.1.9-h1, offloaded application traffic sessions may disconnect after a period of time even if a session is active. The disconnect occurs after the application's default session timeout value is exceeded. This behavior affects only PAN-OS 10.1.9 and 10.1.9-h1. If you are on PAN-OS 10.1.9 and 10.1.9-h1, please use the following workaround. If you have already upgraded or downgraded to another PAN-OS version, use the following workaround in that version. **Workaround:** Run the CLI command **`debug dataplane internal pdt fe100 csr wr_sem_ctrl_ctr_scan_dis value 0`** to set the value to zero (0).
PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local commit on one of the HA firewalls triggers an HA config sync on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.
PAN-215778	On the M-600 appliance in Management Only mode, XML API Get requests for `/config` fail with the following error due to exceeding the total configuration size supported on the M-600 appliance. `504 Gateway timeout`
PAN-215082	M-300 and M-700 appliances may generate erroneous system logs (**Monitor** > **Logs** > **System**) to alert that the M-Series appliance memory usage limits are reached.

Issue ID	Description
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-209937 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	Certificate-based authentication for administrator accounts may be unable to log into the Panorama or firewall web interface with the following error: `Bad Request - Your browser sent a request that this server could not understand`
PAN-208325 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	The following NextGen firewalls and Panorama management server models are unable to automatically renew the device certificate (**Device** > **Setup** > **Management** or **Panorama** > **Setup** > **Management**). • M-300 and M-700 • PA-410 Firewall • PA-415 and PA-445 Firewalls • PA-440, PA-450, and PA-460 Firewalls • PA-1400 Series • PA-3400 Series • PA-5410, PA-5420, and PA-5430 Firewalls • PA-5440 Firewall • PA-5450 Firewall

Issue ID	Description
	Workaround: Log in to the firewall CLI or Panorama CLI and fetch the device certificate. `admin>`**`request certificate fetch`**
PAN-208189 This issue is now resolved. See PAN-OS 11.0.1-h2 Addressed Issues.	Traffic fails to match and reach all destinations if a Security policy rule includes FQDN objects that resolve to two or more IP addresses.
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are automatically unselected and any new tag created is applied to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207442	For M-700 appliances in an active/passive high availability (**Panorama** > **High Availability**) configuration, the `active-primary` HA peer configuration sync to the `secondary-passive` HA peer may fail. When the config sync fails, the job Results is `Successful` (**Tasks**), however the sync status on the **Dashboard** displays as `Out of Sync` for both HA peers.

Issue ID	Description
	Workaround: Perform a local commit on the `active-primary` HA peer and then synchronize the HA configuration. 1. Log in to the Panorama web interface of the `active-primary` HA peer. 2. Select **Commit** and **Commit to Panorama**. 3. In the `active-primary` HA peer **Dashboard**, click **Sync to Peer** in the High Availability widget.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy. This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log forwarding to the disconnected Dedicated Log Collector is not impacted. **Workaround:** Restart the `mgmtsrvr` process on the Dedicated Log Collector. 1. Log in to the Dedicated Log Collector CLI. 2. Confirm the Dedicated Log Collector is disconnected from Panorama. `admin> show panorama-status` Verify the `Connected` status is `no`.

Issue ID	Description
	3. Restart the `mgmtsrvr` process. `admin> debug software restart process management-server`
PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. • DLP cloud service • Advanced Threat Protection inline cloud analysis service • Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204689	Upon upgrade to PAN-OS 11.0.1, the following GlobalProtect settings do not work: • **Allow user to disconnect GlobalProtect App** > **Allow with Passcode** • **Allow user to Disable GlobalProtect App** > **Allow with Passcode** • **Allow User to Uninstall GlobalProtect App** > **Allow with Password**
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-199557	On M-600 appliances in an Active/Passive high availability (HA) configuration, the `configd` process restarts due to a

Issue ID	Description
	memory leak on the `Active` Panorama HA peer. This causes the Panorama web interface and CLI to become unresponsive. **Workaround:** Manually reboot the `Active` Panorama HA peer.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-196146 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The VM-Series firewall on Azure does not boot up with a hostname (specified in an init-cgf.txt or user data) when bootstrapped.
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`

Issue ID	Description
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector. **Workaround:** Restart the log receiver service by running the following CLI command: `debug software restart process log-receiver`
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if: • A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. • A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types:

Issue ID	Description
	1. Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. 2. Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report. 3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-182734 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	On an Advanced Routing Engine, if you change the IPSec tunnel configuration, BGP flaps.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.1-h5 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.1-h4 Addressed Issues

Issue ID	Description
PAN-252214	A fix was made to address CVE-2024-3400.

PAN-OS 11.0.1-h3 Addressed Issues

Issue ID	Description
PAN-238792	Fixed the following device certificate issues: • The firewall was unable to automatically renew the device certificate. • Fetching device certificates failed incorrectly with the error message `OTP is not valid`. • Firewalls disconnected from Cortex Data Lake after renewing the device certificate. • The device certificate was not correctly generated on the log forwarding card (LFC). • WildFire cloud logs did not log thermite certificate usage status.
PAN-237876	Extended the firewall Panorama root CA certificate which was previously set to expire on April 7th, 2024.
PAN-231771	Fixed an issue where the firewall issued /box/getserv/ requests with PAN-OS 7.1.0 and did not take device certificates.
PAN-227568	When a device certificate is installed, renewed, or removed, the firewall will reconnect to the WildFire cloud to use the newest certificate.
PAN-215576	Fixed an issue where the `userID-Agent` and `TS-Agent` certificates were set to expire on November 18, 2024. With this fix, the expiration date has been extended to January 2032.

PAN-OS 11.0.1-h2 Addressed Issues

Issue ID	Description
PAN-217431	(PA-5400 Series firewalls with DPC (Data Processing Cards) only) Fixed an issue with slot 2 DPCs where URL filtering did not work as expected after upgrading to PAN-OS 10.1.9.
PAN-216710	Fixed an issue with firewalls in active/active high availability (HA) configurations where GlobalProtect disconnected when the original suspected Active-Primary firewall became Active-Secondary.
PAN-215899	Fixed an issue with Panorama appliances in HA configurations where configuration synchronization between the HA peers failed.
PAN-215496	Fixed an issue where 100G ports did not come up with BIDI QSFP modules.
PAN-215461	Fixed an issue where the packet descriptor leaked over time with GRE tunnels and keepalives.
PAN-211870	Fixed an issue where path monitoring failure occurred, which caused high availability failover.
PAN-211519	Fixed an issue where RTP/RTCP packets were dropped for SIP calls by SIP ALG when the source NAT translation type was persistent **Dynamic IP And Port**.
PAN-210607	Fixed an issue where enabling Inline Cloud Analysis on Anti-Spyware, Vulnerability Protection, or URL Filtering Security profiles caused the dataplane to stop responding.
PAN-208189	Fixed an issue when traffic failed to match and reach all destinations if a Security policy rule includes FQDN objects that resolve to two or more IP addresses.
PAN-206007	Fixed an issue where a debug command generated an incomplete core file.
PAN-202450	Fixed an issue where the `device-client-cert` was set to expire on December 31, 2023. With this fix, the expiration date has been extended.

PAN-OS 11.0.1 Addressed Issues

Issue ID	Description
PAN-231823	A fix was made to address CVE-2024-5916.
PAN-216656	Fixed an issue where the firewall was unable to fully process the user list from a child group when the child group contained more than 1,500 users.
PAN-215911	Fixed an issue that resulted in a race condition, which caused the *configd* process to stop responding.
PAN-215488	Fixed an issue where an expired Trusted Root CA was used to sign the forward proxy leaf certificate during SSL Decryption.
PAN-210561	Fixed an issue where the *all_task* process repeatedly restarted due to missed heartbeats.
PAN-210513	Fixed an issue where Captive Portal authentication via SAML did not work.
PAN-210481	Fixed an issue where botnet reports were not generated on the firewall.
PAN-210449	Fixed an issue where the value for shared objects used in policy rules were not displayed on multi-vsys firewalls when pushed from Panorama.
PAN-210331	Fixed an issue where the firewall did not send device telemetry files to Cortex Data Lake with the error message `send the file to CDL receiver failed`.
PAN-210327	(PA-5200 Series firewalls only) Fixed an issue where upgrading to PAN-OS 10.1.7, an internal loop caused an increase in the packets received per second.
PAN-210237	Fixed an issue where system logs generated by Panorama for commit operations showed the severity as **High** instead of **Informational**.
PAN-210080	Fixed an issue where the *useridd* process stopped responding when add and delete member parameters in an incremental sync query were empty.
PAN-209799	Fixed an issue where logging was not disabled on passive nodes, which caused the `logrcvr` to stop responding.

Issue ID	Description
PAN-209491	Fixed an issue on the web interface where the **Session Expire Time** displayed a past date if the device time was in December.
PAN-209069	Fixed an issue where IP addresses in the **X-Forwarded-For** (XFF) field were not logged when the IP address contained an associated port number.
PAN-209036	Fixed an issue where the dataplane restarted, which led to slot failures occurring and a core file being generated.
PAN-208987	(PA-5400 Series only) Fixed an issue where packets were not transmitted from the firewall if its fragments were received on different slots. This occurred when aggregate ethernet (AE) members in an AE interface were placed on a different slot.
PAN-208922	A fix was made to address an issue where an authenticated administrator was able to commit a specifically created configuration to read local files and resources from the system (CVE-2023-38046).
PAN-208930	(PA-7000 Series firewalls only) Fixed an issue where auto-tagging in log forwarding did not work.
PAN-208902	Fixed an issue where, when a client sent a TCP/FIN packet, the firewall displayed the end reason as `aged-out` instead of `tcp-fin`.
PAN-208724	Fixed an issue where port pause frame settings did not work as expected and incorrect pause frames occurred.
PAN-208718	Additional debug information was added to capture internal details during traffic congestion.
PAN-208711	(PA-5200 Series firewalls only) The CLI command `debug dataplane set pow no-desched yes/no` was added to address an issue where the *all_pktproc* process stopped responding and caused traffic issues.
PAN-208537	Fixed an issue where the `licensed-device-capacity` was reduced when multiple device management license key files were present.
PAN-208525	Fixed an issue where Security policy rules with user groups did not match when Kerberos authentication was configured for explicit proxy.
PAN-208485	Fixed an issue where NAT policies were not visible on the CLI if they contained more than 32 characters.

Issue ID	Description
PAN-208343	Fixed an issue where telemetry regions were not visible on Panorama.
PAN-208157	Fixed an issue where malformed hints sent from the firewall caused the *logd* process to stop responding on Panorama, which caused a system reboot into maintenance mode.
PAN-207940	Fixed an issue where platforms with RAID disk checks were performed weekly, which caused logs to incorrectly state that RAID was rebuilding.
PAN-207740	Fixed an issue that resulted in a race condition, which caused the *configd* process to stop responding.
PAN-207738	Fixed an issue where the `ocsp-next-update-time` CLI command did not execute for leaf certificates with certificate chains that did not specify OCSP or CRL URLs. As a result, the next update time was 60 minutes even if a different time was set.
PAN-207663	Fixed a Clientless VPN issue where JSON stringify caused issues with the application rewrite.
PAN-207629	Fixed an issue where a selective push to firewalls failed if the firewalls were enabled with multiple vsys and the push scope contained shared objects in device groups.
PAN-207610	(PA-5200 Series and PA-7000 Series firewalls only) Fixed an issue where **Log Admin Activity** was not visible on the web interface.
PAN-207601	Fixed an issue where URL cloud connections were unable to resolve the proxy server hostname.
PAN-207426	Fixed an issue where a selective push did not include the **Share Unused Address and Service Objects with Devices** option on Panorama, which caused the firewall to not receive the objects during the configuration push.
PAN-207400	Fixed an issue on Octeon based platforms where fragmented VLAN tagged packets dropped on an aggregate interface.
PAN-207390	Fixed an issue where, even after disabling Telemetry, Telemetry system logs were still generated.
PAN-207260	A commit option was enabled for Device Group and Template administrators after a password change.

Issue ID	Description
PAN-207045	(PA-800 Series firewalls only) Fixed an issue where PAN-SFP-SX transceivers used on ports 5 to 8 did not renegotiate with peer ports after a reload.
PAN-206963	(M-700 Appliances only) A CLI command was added to check the status of each physical port of a bond1 interface.
PAN-206858	Fixed an issue where a segmentation fault occurred due to the *useridd* process being restarted.
PAN-206755	Fixed an issue when a scheduled multi-device group push occurred, the *configd* process stopped responding, which caused the push to fail.
PAN-206684	(PA-7000 Series firewalls with Log Forwarding Cards (LFCs) only) Fixed an issue where, after upgrading the firewall from a PAN-OS 10.0 release to a PAN-OS 10.1 release, the firewall did not duplicate logs to local log collectors or to Cortex Data Lake when a device certificate was already installed.
PAN-206658	Fixed a timeout issue in the Intel `ixgbe` driver that resulted in internal path monitoring failure.
PAN-206466	Fixed an issue where the push scope was displaying duplicate shared objects for each device group that were listed under the **shared-object** group.
PAN-206393	(PA-5280 firewalls only) Fixed an issue where memory allocation errors caused decryption failures that disrupted traffic with SSL forward proxy enabled.
PAN-206382	Fixed an issue where authentication sequences were not populated in the drop down when selecting authentication profiles during administrator creation in a template.
PAN-206251	(PA-7000 Series firewalls with Log Forwarding Cards (LFCs) only) Fixed an issue where the *logrcvr* process did not send the `system-start` SNMP trap during startup.
PAN-206233	Fixed an issue where the *pan_comm* process stopped responding when a content update and a cloud application update occurred at the same time.
PAN-206128	(PA-7000 Series firewalls with NPCs (Network Processing Cards) only) Improved debugging capability for an issue where the firewall restarted due to heartbeat failures and then failed with the following error message: `Power not OK`.

Issue ID	Description
PAN-206069	Fixed an issue where the firewall was unable to boot up on older Intel CPUs.
PAN-206017	Fixed an issue where the `show dos-protection rule` command displayed a character limit error.
PAN-206005	(PA-1400 Series, PA-3400 Series, and PA-5440 firewalls only) Fixed an issue where the `l7_misc` memory pool was undersized and caused connectivity loss when the limit was reached.
PAN-205877	(PA-5450 firewalls only) Added debug commands for an issue where a MAC address flap occurred on a neighbor firewall when connecting both MGT-A and MGT-B interfaces.
PAN-205829	Fixed an issue where logs did not display **Host-ID** details for GlobalProtect users despite having a quarantine Security policy rule. This occurred due to a missed local cache lookup.
PAN-205804	Fixed an issue on Panorama where a WildFire scheduled update for managed devices triggered multiple `UploadInstall` jobs per minute.
PAN-205729	(PA-3200 Series and PA-7000 Series firewalls only) Fixed an issue where the CPLD watchdog timeout caused the firewall to reboot unexpectedly.
PAN-205699	Fixed an issue where the cloud plugin configuration was automatically deleted from Panorama after a reboot or a *configd* process restart.
PAN-205698	Fixed an issue where GlobalProtect authentication did not work on Apple MacOS devices when the authentication method used was CIE with SAML Authentication.
PAN-205590	Fixed an issue where the fan tray fault LED light was on even though no alarm was reported in the system environment.
PAN-205453	Fixed an issue where running reports or queries under a user group caused the *reportd* process to stop responding.
PAN-205396	Fixed an issue where SD-WAN adaptive SaaS path monitoring did not work correctly during a next hop link down failure.
PAN-205260	Fixed an issue where there was an IP address conflict after a reboot due to a transaction ID collision.
PAN-205255	Fixed a rare issue that caused the dataplane to restart unexpectedly.

Issue ID	Description
PAN-205231	Fixed an issue where a commit operation remained at 55% for longer than expected if more than 7,500 Security policy rules were configured.
PAN-205211	Fixed an issue where the *reportd* process stopped responding while querying logs (**Monitor > Logs > <logtype>**).
PAN-205096	Fixed an issue where promoted sessions were not synced with all cluster members in an HA cluster.
PAN-204749	Fixed an issue where sudden, large bursts of traffic destined for an interface that was down caused packet buffers to fill, which stalled path monitor heartbeat packets.
PAN-204581	Fixed an issue where, when accessing a web application via the GlobalProtect Clientless VPN, the web application landing page continuously reloaded.
PAN-204575	(PA-7000 Series firewalls with Log Forwarding Cards (LFCs) only) Fixed an issue where the firewall did not forward logs to the log collector.
PAN-204572	Fixed an issue where python scripts were not working as expected.
PAN-204456	Fixed an issue related to the *logd* process that caused high memory consumption.
PAN-204335	Fixed an issue where Panorama became unresponsive, and when refreshed, the error **504 Gateway not Reachable** was displayed.
PAN-203964	(Firewalls in FIPS-CC mode only) Fixed an issue where the firewall went into maintenance mode due to downloading a corrupted software image, which resulted in the error message `FIPS-CC failure. Image File Authentication Error`.
PAN-203851	Fixed an issue with firewalls in HA configurations where host information profile (HIP) sync did not work between peer firewalls.
PAN-203681	(Panorama appliances in FIPS-CC mode only) Fixed an issue where a leaf certificate was unable to be imported into a template stack.
PAN-203663	Fixed an issue where administrators were unable to change the password of a local database for users configured as a local admin user via an authentication profile.

Issue ID	Description
PAN-203453	Fixed an issue on Panorama where the log query failed due to a high number of User-ID redistribution messages.
PAN-203430	Fixed an issue where, when the User-ID agent had `collector name/secret` configured, the configuration was mandatory on clients on PAN-OS 10.0 and later releases.
PAN-203339	Fixed an issue where services failed due to the RAID rebuild not being completed on time.
PAN-203147	(Firewalls in FIPS-CC mode only) Fixed an issue where the firewall unexpectedly rebooted when downloading a new PAN-OS software image.
PAN-203137	(PA-5450 firewalls only) Fixed an issue where HSCI ports did not come up when QSFP DAC cables were used.
PAN-202543	An enhancement was made to improve path monitor data collection by verifying the status of the control network.
PAN-202248	Fixed an issue where, due to a tunnel content inspection (TCI) policy match, IPSec traffic did not pass through the firewall when NAT was performed on the traffic.
PAN-201701	Fixed an issue where the firewall generated system log alerts if the raid for a system or log disk was corrupted.
PAN-201580	Fixed an issue where the *useridd* process stopped responding due to an invalid vsys_id request.
PAN-200845	(M-600 Appliances in Management-only mode only) Fixed an issue where XML API queries failed due to the configuration size being larger than expected.
PAN-200160	Fixed a memory leak issue on Panorama related to the *logd* process that caused an out-of-memory (OOM) condition.
PAN-200116	Fixed an issue where Elasticsearch displayed red due to frequent tunnel check failures between HA clusters.
PAN-199965	Fixed an issue where the *reportd* process stopped responding on log collectors during query and report operations due to a race condition between request handling threads.
PAN-199807	Fixed an issue where the dataplane frequently restarted due to high memory usage on wifclient.

Issue ID	Description
PAN-196597	Fixed an issue where the *dnsproxyd* process stopped responding due to corruption.
PAN-198306	Fixed an issue where the *useridd* process stopped responding when booting up the firewall.
PAN-198266	Fixed an issue where, when predicts for UDP packets were created, a configuration change occurred that triggered a new policy lookup, which caused the dataplane stopped responding when converting the predict. This resulted in a dataplane restart.
PAN-198038	A CLI command was added to address an issue where long-lived sessions were aging out even when there was ongoing traffic.
PAN-197872	Fixed an issue where the *useridd* process generated false positive critical errors.
PAN-197298	Fixed an issue where the audit comment archive for Security rule changes output had overlapping formats.
PAN-196410	Fixed an issue where you were unable to customize the risk value in **Risk-of-app**.
PAN-195756	Fixed an issue that caused an API request timeout when parsing requests using large header buffers.
PAN-194805	Fixed an issue where scheduled configuration backups to the SCP server failed with error message `No ECDSA host key is known`.
PAN-194068	(PA-5200 Series firewalls only) Fixed an issue where the firewall unexpectedly rebooted with the log message `Heartbeat failed previously`.
PAN-192513	Fixed an issue where log migration did not work when converting a Legacy mode Panorama appliance to Log Collector mode.
PAN-192282	(PA-415 and PA-445 firewalls only) Fixed an issue where, in 1G mode, the MGT and Ethernet 1/1 port LEDs incorrectly displayed as amber instead of green.
PAN-191222	Fixed an issue where Panorama became inaccessible when after a push to the collector group.
PAN-190502	Fixed an issue where the Policy filter and Policy optimizer filter were required to have the exact same syntax, including nested conditions

Issue ID	Description
	with rules that contained more than one tag when filtering via the `neq` operator.
PAN-189335	Fixed an issue where the *varrcvr* process restarted repeatedly, which caused the firewall to restart.
PAN-189200	Fixed an issue where sinkholes did not occur for AWS Gateway Load Balancer dig queries.
PAN-186412	Fixed an issue where invalid `packet-ptr` was seen in work entries.
PAN-186270	Fixed an issue where, when HA was enabled and a dynamic update schedule was configured, the *configd* process unexpectedly stopped responding during configuration commits.
PAN-183375	Fixed an issue where traffic arriving on a tunnel with a bad IP address header checksum was not dropped.
PAN-180948	Fixed an issue where an external dynamic list fetch failed with the error message `Unable to fetch external dynamic list. Couldn't resolve host name. Using old copy for refresh`.
PAN-179174	Fixed an issue where exported PDF report of the ACC was the incorrect color after upgrading from a PAN-OS 10.1 or later release.
PAN-178594	Fixed an issue where the descriptions of options under the `set syslogng ssl-conn-validation` CLI command were not accurate.
PAN-175142	Fixed an issue on Panorama where executing a debug command caused the *logrcvr* process to stop responding.
PAN-170414	Fixed an issue related to an OOM condition in the dataplane, which was caused by multiple `panio` commands using extra memory.

PAN-OS 11.0.0 Known and Addressed Issues

Review a list of known and addressed issues for PAN-OS 11.0.0.

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.

- PAN-OS 11.0.0 Known Issues
- PAN-OS 11.0.0-h4 Addressed Issues
- PAN-OS 11.0.0-h3 Addressed Issues
- PAN-OS 11.0.0-h2 Addressed Issues
- PAN-OS 11.0.0-h1 Addressed Issues
- PAN-OS 11.0.0 Addressed Issues

PAN-OS 11.0.0 Known Issues

The following list includes only outstanding known issues specific to PAN-OS® 11.0.0. This list includes issues specific to Panorama™, GlobalProtect™, VM-Series plugins, and WildFire®, as well as known issues that apply more generally or that are not identified by an issue ID.

Issue ID	Description
WF500-5632	The number of registered WildFire appliances reported in Panorama (**Panorama** > **Managed WildFire Appliances** > **Firewalls Connected** > **View**) does not accurately reflect the current status of connected WildFire appliances.
PAN-260851	From the NGFW or Panorama CLI, you can override the existing application tag even if Disable Override is enabled for the application (**Objects** > **Applications**) tag.
PAN-250062	Device telemetry might fail at configured intervals due to bundle generation issues.
PAN-234408	Enterprise DLP cannot detect and block non-file based traffic for ChatGPT from traffic forwarded to the DLP cloud service from an NGFW.
PAN-234015	The X-Forwarded-For (XFF) value is not displayed in traffic logs.
PAN-243951	On the Panorama management sever in an active/passive High Availability (HA) configuration, managed devices (**Panorama** > **Managed Devices** > **Summary**) display as `out-of-sync` on the passive HA peer when configuration changes are made to the SD-WAN (**Panorama** > **SD-WAN**) configuration on the active HA peer. **Workaround:** Manually synchronize the Panorama HA peers. **1.** Log in to the Panorama web interface on the active HA peer. **2.** Select **Commit** and **Commit to Panorama** the SD-WAN configuration changes on the active HA peer. On the passive HA peer, select **Panorama** > **Managed Devices** > **Summary** and observe that the managed devices are now `out-of-sync`. **3.** Log in to the primary HA peer Panorama CLI and trigger a manual synchronization between the active and secondary HA peers. *request high-availability sync-to-remote running-config*

Issue ID	Description
	4. Log back in to the active HA peer Panorama web interface and select **Commit** > **Push to Devices** and **Push**.
PAN-242910	On the Panorama management server, Panorama administrators (**Panorama** > **Administrators**) that are assigned a custom Panorama admin role (**Panorama** > **Admin Roles**) with **Push All Changes** enabled are unable to push configuration changes to managed firewalls when **Managed Devices** and **Push For Other Admins** are disabled.
PAN-241041	On the Panorama management server exporting template or template stack variables (**Panorama** > **Templates**) in CSV format results in an empty CSV file.
PAN-228515	The EleasticSearch SSH flaps on the M-600 appliance in Panorama or Log Collector mode. This causes logs to not display on the Panorama management server (**Monitor** > **Logs**) and the Log Collector health status (**Panorama** > **Managed Collectors** > **Status**) to display as degraded.
PAN-228273	On the Panorama management server in FIPS-CC mode, the ElasticSearch cluster fails to come up and the `show log-collector-es-cluster health` command displays the `status` is `red`. This results in log ingestion issues for Panorama in Panorama only or Log Collector mode.
PAN-227344	On the Panorama management server, PDF Summary Reports (**Monitor** > **PDF Reports** > **Manage PDF Summary**) display no data and are blank when predefined reports are included in the summary report.
PAN-225886	If you enable explicit proxy mode for the web proxy, intermittent errors and unexpected TCP reconnections may occur.
PAN-225337 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On the Panorama management server, the configuration push to a multi-vsys firewall fails if you: 1. Create a **Shared** and vsys-specific device group configuration object with an indentical name. For example, a **Shared** address object called `SharedA01` and a vsys-specific address object also called `SharedA01`. 2. Reference the **Shared** object in another **Shared** configuration. For example, reference the **Shared** address object (`SharedA01`) in a **Shared** address group called `SharedAG1`.

Issue ID	Description
	3. Use the **Shared** configuration object with the reference in a vsys-specific configuration. For example, reference the **Shared** address group (`SharedAG1`) in a vsys-specific policy rule. **Workaround:** Select **Panorama** > **Setup** > **Management** and edit the Panorama Settings to enable one of the following: - **Shared Unused Address and Service Objects with Devices**—This options pushes all **Shared** objects, along with device group specific objects, to managed firewalls. This is a global setting and applies to all managed firewalls, and may result in pushing too many configuration objects to your managed firewalls. - **Objects defined in ancestors will take higher precedence**—This option specifies that in the event of objects with the same name, ancestor object take precedence over descendent objects. In this case, the **Shared** objects take precedence over the vsys-specific object. This is a global setting and applies to all managed firewalls. In the example above, if the IP address for the **Shared** `SharedA01` object was `10.1.1.1` and the device group specific `SharedA01` was `10.2.2.2`, the `10.1.1.1` IP address takes precedence. Alternatively, you can remove the duplicate address objects from the device group configuration to allow only the **Shared** objects in your configuration.
PAN-223488 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Closed ElasticSearch shards are not deleted from the Panorama M-Series and virtual appliance. This causes the ElasticSearch shard purging to not work as expected, resulting in high disk usage.
PAN-223365 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	The Panorama management server is unable to query any logs if the ElasticSearch health status for any Log Collector (**Panorama** > **Managed Collector** is degraded. **Workaround:** Log in to the Log Collector CLI and restart ElasticSearch. `admin`**`debug elasticsearch es-restart all`**
PAN-222586	On PA-5410, PA-5420, PA-5430, and PA-5440 firewalls, the Filter dropdown menus, Forward Methods, and Built-In Actions for Correlation Log settings (**Device** > **Log Settings**) are not displayed and cannot be configured.

Issue ID	Description
PAN-222253 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	On the Panorama management server, policy rulebase reordering when you **View Rulebase by Groups** (**Policy** > **<policy-rulebase>**) does not persist if you reorder the policy rulebase by dragging and dropping individual policy rules and then moving the entire tag group.
PAN-221015 This issue is now resolved. See PAN-OS 11.0.4 Addressed Issues.	On M-600 appliances in Panorama or Log Collector mode, the `es-1` and `es-2` ElasticSearch processes fail to restart when the M-600 appliance is rebooted. The results in the Managed Collector ES health status (**Panorama** > **Managed Collectors** > **Health Status**) to be degraded. **Workaround:** Log in to the Panorama or Log Collector CLI experiencing degraded ElasticSearch health and restart all ElasticSearch processes. `admin>`**`debug elasticsearch es-restart optional all`**
PAN-220180 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Configured botnet reports (**Monitor** > **Botnet**) are not generated.
PAN-219644 This issue is now resolved. See PAN-OS 11.0.3 Addressed Issues.	Firewalls forwarding logs to a syslog server over TLS (**Objects** > **Log Forwarding**) use the default Palo Alto Networks certificate instead of the custom certificate configured on the firewall.
PAN-218521 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The ElasticSearch process on the M-600 appliance in Log Collector mode may enter a continuous reboot cycle. This results in the M-600 appliance becoming unresponsive, consuming logging disk space, and preventing new log ingestion.

PAN-217307	The following Security policy rule (**Policies** > **Security**) filters return no results:
	`log-start eq no`
	`log-end eq no`
	`log-end eq yes`

PAN-216214	For Panorama-managed firewalls in an Active/Active High Availability (HA) configuration where you configure the firewall HA settings (**Device** > **High Availability**) in a template or template stack (**Panorama** > **Templates**), performing a local

Issue ID	Description
	commit on one of the HA firewalls triggers an HA config sync on the peer firewall. This causes the HA peer configuration to go `Out of Sync`.
PAN-215778	On the M-600 appliance in Management Only mode, XML API Get requests for `/config` fail with the following error due to exceeding the total configuration size supported on the M-600 appliance. `504 Gateway timeout`
PAN-215082	M-300 and M-700 appliances may generate erroneous system logs (**Monitor** > **Logs** > **System**) to alert that the M-Series appliance memory usage limits are reached.
PAN-213746	On the Panorama management server, the **Hostkey** displayed as `undefined undefined` if you override an SSH Service Profile (**Device** > **Certificate Management** > **SSH Service Profile**) Hostkey configured in a Template from the Template Stack.
PAN-213119	PA-5410 and PA-5420 firewalls display the following error when you view the Block IP list (**Monitor** > **Block IP**): `show -> dis-block-table is unexpected`
PAN-212889	On the Panorama management server, different threat names are used when querying the same threat in the Threat Monitor (**Monitor** > **App Scope** > **Threat Monitor**) and **ACC**. This results in the ACC displaying `no data to display` when you are redirected to the ACC after clicking a threat name in the Threat Monitor and filtering the same threat name in the Global Filters.
PAN-212533	Modifying the **Administrator Type** for an existing administrator (**Device** > **Administrators** or **Panorama** > **Administrators**) from `Superuser` to a **Role-Based** custom admin, or vice versa, does not modify the access privileges of the administrator.
PAN-211531	On the Panorama management server, admins can still perform a selective push to managed firewalls when **Push All Changes** and **Push for Other Admins** are disabled in the admin role profile (**Panorama** > **Admin Roles**).
PAN-209937	Certificate-based authentication for administrator accounts may be unable to log into the Panorama or firewall web interface with the following error:

Issue ID	Description
This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	`Bad Request - Your browser sent a request that this server could not understand`
PAN-208325 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	The following NextGen firewalls and Panorama management server models are unable to automatically renew the device certificate (**Device** > **Setup** > **Management** or **Panorama** > **Setup** > **Management**). • M-300 and M-700 • PA-410 Firewall • PA-415 and PA-445 Firewalls • PA-440, PA-450, and PA-460 Firewalls • PA-1400 Series • PA-3400 Series • PA-5410, PA-5420, and PA-5430 Firewalls • PA-5440 Firewall • PA-5450 Firewall **Workaround:** Log in to the firewall CLI or Panorama CLI and fetch the device certificate. `admin>`**`request certificate fetch`**
PAN-208189 This issue is now resolved. See PAN-OS 11.0.1-h2 Addressed Issues.	Traffic fails to match and reach all destinations if a Security policy rule includes FQDN objects that resolve to two or more IP addresses.
PAN-207770	Data filtering logs (**Monitor** > **Logs** > **Data Filtering**) incorrectly display the traffic Direction as `server-to-client` instead of `client-to-server` for upload traffic that matches Enterprise data loss prevention (DLP) data patterns (**Objects** > **DLP** > **Data Filtering Patterns**) in an Enterprise DLP data filtering profile (**Objects** > **DLP** > **Data Filtering Profiles**).
PAN-207733	When a DHCPv6 client is configured on HA Active/Passive firewalls, if the DHCPv6 server goes down, after the lease time expires, the DHCPv6 client should enter SOLICIT state on both the Active and Passive firewalls. Instead, the client is stuck in BOUND state with an IPv6 address having lease time 0 on the Passive firewall.

Issue ID	Description
PAN-207629	On the Panorama management server, selective push fails to managed firewalls if the managed firewalls are enabled with multiple vsys and the Push Scope contains shared objects in device groups.
PAN-207616	On the Panorama management server, after selecting managed firewalls and creating a new **Tag** (**Panorama** > **Managed Devices** > **Summary**) the managed firewalls are automatically unselected and any new tag created is applied to the managed firewalls for which you initially created the new tag. **Workaround:** Select and then unselect the managed firewalls for which you created a new tag.
PAN-207611	When a DHCPv6 client is configured on HA Active/Passive firewalls, the Passive firewall sometimes crashes.
PAN-207040	If you disable Advanced Routing, remove logical routers, and downgrade from PAN-OS 11.0.0 to a PAN-OS 10.2.x or 10.1.x release, subsequent commits fail and SD-WAN devices on Panorama have no Virtual Router name.
PAN-206913	When a DHCPv6 client is configured on HA Active/Passive firewalls, releasing the IPv6 address from the client (using Release in the UI or using the `request dhcp client ipv6 release all` CLI command) releases the IPv6 address from the Active firewall, but not the Passive firewall.
PAN-206909	The Dedicated Log Collector is unable to reconnect to the Panorama management server if the `configd` process crashes. This results in the Dedicated Log Collector losing connectivity to Panorama despite the managed collector connection `Status` (**Panorama** > **Managed Collector**) displaying `connected` and the managed colletor `Health` status displaying as healthy. This results in the local Panorama config and system logs not being forwarded to the Dedicated Log Collector. Firewall log forwarding to the disconnected Dedicated Log Collector is not impacted. **Workaround:** Restart the `mgmtsrvr` process on the Dedicated Log Collector. **1.** Log in to the Dedicated Log Collector CLI.

Issue ID	Description

	2. Confirm the Dedicated Log Collector is disconnected from Panorama.
	`admin> show panorama-status`
	Verify the `Connected` status is no.
	3. Restart the `mgmtsrvr` process.
	`admin> debug software restart process management-server`

PAN-206416	On the Panorama management server, no data filtering log (**Monitor** > **Logs** > **Data Filtering**) is generated when the managed firewall loses connectivity to the following cloud services, and as a result fails to forward matched traffic for inspection. - DLP cloud service - Advanced Threat Protection inline cloud analysis service - Advanced URL Filtering cloud service
PAN-206315	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show session info` CLI command shows that the passive firewall has packet rate and throughput values. The packet rate and throughput of the passive firewall should be zero since it is not processing traffic.
PAN-206253 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	For PA-1400 and PA-3400 Series firewalls, the default log rate is set too low and the max configurable log rate is incorrectly capped resulting in the firewall not generating more than 6,826 logs per second.
PAN-206005 This issue is now resolved. See PAN-OS 11.0.1 Addressed Issues.	(PA-1400 Series, PA-3400 Series, and PA-5440 firewalls only) The l7_misc memory pool on these platforms is undersized and can cause a loss of connectivity when reaching the limit of the memory pool. Certain features, like using a decryption profile with Strip ALPN disabled, can lead to depleting the memory pool and causing a connection loss. **Workaround:** Disable HTTP2 by enabling Strip ALPN in the decryption profile or avoid usage of the l7_misc memory pool.
PAN-205255	There is a rare PAN-OS issue that causes the dataplane to restart unexpectedly.

Issue ID	Description
This issue is now resolved. See PAN-OS 11.0.1 Addressed Issues.	
PAN-205187	ElasticSearch may not start properly when a newly installed Panorama virtual appliance powers on for the first time, resulting in the Panorama virtual appliance being unable to query logs forwarded from the managed firewall to a Log Collector. **Workaround:** Log in to the Panorama CLI and start the PAN-OS software. `admin>`**`request restart software`**
PAN-205009	(PA-1420 firewall only) In an active/passive high availability (HA) configuration, the `show interface all`, `show-high availability interface ha2`, and `show high-availability all` CLI commands display the HSCI port state as unknown on both the active and passive firewalls.
PAN-204615 This issue is now resolved. See PAN-OS 11.0.0 Known Issues.	BGP sessions can flap even when an unrelated configuration is committed. This results in the BGP session going down and getting established again. As a result, BGP routes get exchanged again, which can lead to momentary traffic disruption if BGP routes were in use for establishing traffic.
PAN-201910	PAN-OS security profiles might consume a large amount of memory depending on the profile configuration and quantity. In some cases, this might reduce the number of supported security profiles below the stated maximum for a given platform.
PAN-201855	On the Panorama management server, cloning any template (**Panorama** > **Templates**) corrupts certificates (**Device** > **Certificate Management** > **Certificates**) with the **Block Private Key Export** setting enabled across all templates. This results in managed firewalls experiencing issues wherever the corrupted certificate is referenced. For example, you have template A, B, and C where templates A and B have certificates with the **Block Private Key Export** setting enabled. Cloning template C corrupts the certificates with **Block Private Key Export** setting enabled in templates A and B. **Workaround:** After cloning a template, delete and re-import the corrupted certificates.

Issue ID	Description
PAN-199557	On M-600 appliances in an Active/Passive high availability (HA) configuration, the `configd` process restarts due to a memory leak on the `Active` Panorama HA peer. This causes the Panorama web interface and CLI to become unresponsive. **Workaround:** Manually reboot the `Active` Panorama HA peer.
PAN-197588	The PAN-OS ACC (Application Command Center) does not display a widget detailing statistics and data associated with vulnerability exploits that have been detected using inline cloud analysis.
PAN-197419	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, the power over Ethernet (PoE) ports do not display a **Tag** value.
PAN-197097	Large Scale VPN (LSVPN) does not support IPv6 addresses on the satellite firewall.
PAN-196758	On the Panorama management server, pushing a configuration change to firewalls leveraging SD-WAN erroneously show the auto-provisioned BGP configurations for SD-WAN as being edited or deleted despite no edits or deletions being made when you **Preview Changes** (**Commit** > **Push to Devices** > **Edit Selections** or **Commit** > **Commit and Push** > **Edit Selections**).
PAN-196146 This issue is now resolved. See PAN-OS 11.0.5 Addressed Issues.	The VM-Series firewall on Azure does not boot up with a hostname (specified in an init-cgf.txt or user data) when bootstrapped.
PAN-195968	(PA-1400 Series firewalls only) When using the CLI to configure power over Ethernet (PoE) on a non-PoE port, the CLI prints an error depending on whether an interface type was selected on the non-PoE port or not. If an interface type, such as tap, Layer 2, or virtual wire, was selected before PoE was configured, the error message will not include the interface name (eg. ethernet1/4). If an interface type was not selected before PoE was configured, the error message will include the interface name.
PAN-195568	When PAN-OS 11.0 is installed on multiple data plane platforms, users are unable to connect to the GlobalProtect portal or gateway.

Issue ID	Description
PAN-195342	On the Panorama management server, Context Switch fails when you try to Context Switch from a managed firewall running PAN-OS 10.1.7 or earlier release back to Panorama and the following error is displayed: `Could not find start token '@start@'`
PAN-194978	(PA-1400 Series firewalls only) In **Network** > **Interface** > **Ethernet**, hovering the mouse over a power over Ethernet (PoE) **Link State** icon does not display link speed and link duplex details.
PAN-194424	(PA-5450 firewall only) Upgrading to PAN-OS 10.2.2 while having a log interface configured can cause both the log interface and the management interface to remain connected to the log collector. **Workaround:** Restart the log receiver service by running the following CLI command: `debug software restart process log-receiver`
PAN-192282 This issue is now resolved. See PAN-OS 11.0.1 Addressed Issues.	(PA-415 and PA-445 firewalls only) In 1G mode, the MGT and Ethernet 1/1 port LEDs glow amber instead of green.
PAN-187685	On the Panorama management server, the Template Status displays no synchronization status (**Panorama** > **Managed Devices** > **Summary**) after a bootstrapped firewall is successfully added to Panorama. **Workaround:** After the bootstrapped firewall is successfully added to Panorama, log in to the Panorama web interface and select **Commit** > **Push to Devices**.
PAN-187407	The configured Advanced Threat Prevention inline cloud analysis action for a given model might not be honored under the following condition: If the firewall is set to **Hold client request for category lookup** and the action set to **Reset-Both** and the URL cache has been cleared, the first request for inline cloud analysis will be bypassed.
PAN-186283	Templates appear out-of-sync on Panorama after successfully deploying the CFT stack using the Panorama plugin for AWS. **Workaround**: Use **Commit** > **Push to Devices** to synchronize the templates.

Issue ID	Description
PAN-184708	Scheduled report emails (**Monitor** > **PDF Reports** > **Email Scheduler**) are not emailed if: • A scheduled report email contains a Report Group (**Monitor** > **PDF Reports** > **Report Group**) which includes a SaaS Application Usage report. • A scheduled report contains only a SaaS Application Usage Report. **Workaround:** To receive a scheduled report email for all other PDF report types: 1. Select **Monitor** > **PDF Reports** > **Report Groups** and remove all SaaS Application Usage reports from all Report Groups. 2. Select **Monitor** > **PDF Reports** > **Email Scheduler** and edit the scheduled report email that contains only a SaaS Application Usage report. For the Recurrence, select **Disable** and click **OK**. Repeat this step for all scheduled report emails that contain only a SaaS Application Usage report. 3. **Commit**. (Panorama managed firewalls) Select **Commit** > **Commit and Push**
PAN-184406	Using the CLI to add a RAID disk pair to an M-700 appliance causes the dmdb process to crash. **Workaround:** Contact customer support to stop the dmdb process before adding a RAID disk pair to a M-700 appliance.
PAN-183404	Static IP addresses are not recognized when "and" operators are used with IP CIDR range.
PAN-182734 This issue is now resolved. See PAN-OS 11.0.2 Addressed Issues.	On an Advanced Routing Engine, if you change the IPSec tunnel configuration, BGP flaps.
PAN-181933	If you use multiple log forwarding cards (LFCs) on the PA-7000 series, all of the cards may not receive all of the updates and the mappings for the clients may become out of sync, which causes the firewall to not correctly populate the Source User column in the session logs.

Issue ID	Description
PAN-171938	No results are displayed when you **Show Application Filter** for a Security policy rule (**Policies** > **Security** > **Application** > **Value** > **Show Application Filter**).
PAN-164885	On the Panorama management server, pushes to managed firewalls (**Commit** > **Push to Devices** or **Commit and Push**) may fail when an EDL (**Objects** > **External Dynamic Lists**) is configured to **Check for updates** every 5 minutes due to the commit and EDL fetch processes overlapping. This is more likely to occur when multiple EDLs are configured to check for updates every 5 minutes.

PAN-OS 11.0.0-h4 Addressed Issues

Issue ID	Description
PAN-272809	A fix was made to address CVE-2024-0012 (PAN-SA-2024-0015) and CVE-2024-9474.

PAN-OS 11.0.0-h3 Addressed Issues

Issue ID	Description
PAN-252214	A fix was made to address CVE-2024-3400.

PAN-OS 11.0.0-h2 Addressed Issues

Issue ID	Description
PAN-238792	Fixed the following device certificate issues: • The firewall was unable to automatically renew the device certificate. • Fetching device certificates failed incorrectly with the error message `OTP is not valid`. • Firewalls disconnected from Cortex Data Lake after renewing the device certificate. • The device certificate was not correctly generated on the log forwarding card (LFC). • WildFire cloud logs did not log thermite certificate usage status.
PAN-237876	Extended the firewall Panorama root CA certificate which was previously set to expire on April 7th, 2024.
PAN-231771	Fixed an issue where the firewall issued /box/getserv/ requests with PAN-OS 7.1.0 and did not take device certificates.
PAN-227568	When a device certificate is installed, renewed, or removed, the firewall will reconnect to the WildFire cloud to use the newest certificate.
PAN-215576	Fixed an issue where the `userID-Agent` and `TS-Agent` certificates were set to expire on November 18, 2024. With this fix, the expiration date has been extended to January 2032.

PAN-OS 11.0.0-h1 Addressed Issues

Issue ID	Description
PAN-202450	Fixed an issue where the `device-client-cert` was set to expire on December 31, 2023. With this fix, the expiration date has been extended.
PAN-198372	Fixed an issue where the `root-cert` was set to expire on December 31, 2023. With this fix, the expiration date has been extended.

PAN-OS 11.0.0 Addressed Issues

Issue ID	Description
PAN-231823	A fix was made to address CVE-2024-5916.
PAN-207505	Fixed an issue where Email schedules (**Monitor** > **PDF Reports** > **Email Scheduler**) were not supported for SaaS Application Usage (**Monitor** > **PDF Reports** > **SaaS Application Usage**) reports.
PAN-204615	Fixed an issue where BGP sessions could flap even when an unrelated configuration was committed. This resulted in the BGP session going down and getting established again. As a result, BGP routes were exchanged again, which could lead to momentary traffic disruption if BGP routes were in use for establishing traffic.
PAN-202783	(PA-7000 Series firewalls with 100G NPC (Network Processing Cards) only) Fixed an issue where sudden, large bursts of traffic destined for an interface that was down caused packet buffers to fill, which stalled path monitor heartbeat packets.
PAN-202535	Fixed an issue where the Device Telemetry configuration for a region was unable to be set or edited via the web interface.
PAN-199726	Fixed an issue with firewalls in HA configurations where both firewalls responded with gARP messages after a switchover.
PAN-199654	Fixed an issue where ACC reports did not work for custom RBAC users when more than 12 access domains were associated with the username.
PAN-198733	(PA-5450 firewalls only) Fixed an issue where `tcpdump` was hardcoded to eth0 instead of bond0.
PAN-198332	(PA-5400 Series only) Fixed an issue where swapping Network Processing Cards (NPCs) caused high root partition use.
PAN-198244	Fixed an issue where using the `load config partial` CLI command to x-paths removed address object entries from address groups.
PAN-197383	Fixed an issue where, after upgrading to PAN-OS 10.2 release, the firewall ran a RAID rebuild for the log disk after ever every reboot.
PAN-197341	Fixed an issue on Panorama where, when you created multiple device group objects with the same name in the shared device group and any additional device groups (**Panorama** > **Device Groups**) under the

Issue ID	Description
	same device group hierarchy that were used in one or more policies, renaming the object with a shared name in any device group caused the object name to change in the policies that it was used in. This issue occurred with device group objects that were referenced in a Security policy rule.
PAN-196558	Fixed an issue where IP address tag policy updates were delayed.
PAN-196398	(PA-7000 Series SMC-B firewalls only) Fixed an issue where the firewall did not capture data when the active management interface was MGT-B.
PAN-194615	Fixed an issue where the packet broker session timeout value did not match the master sessions timeout value after the firewall received a TCP FIN or RST packet. The fix ensures that Broker session times out within 1 second after the master session timed out.
PAN-194152	(PA-5410, PA-5420, PA-5430, and PA-5440 firewalls in HA configurations only) Fixed an issue where HA1-A and HA1-B port information didn't match to front panel mappings.
PAN-189270	Fixed an issue that caused a memory leak on the *reportd* process.
PAN-188096	(VM-Series firewalls only) Fixed an issue where, on firewalls licensed with Software NGFW Credit (VM-FLEX-4 and higher), HA clustering was unable to be established.
PAN-171714	Fixed an issue where, when NetBIOS format (domain\user) was used for the IP address-to-username mapping and the firewall received the group mapping information from the Cloud Identity Engine, the firewall did not match the user to the correct group.

Related Documentation

Review the related documentation for PAN-OS 11.0.

To provide feedback on the documentation, write to us at: documentation@paloaltonetworks.com.

- Related Documentation for PAN-OS 11.0

Related Documentation for PAN-OS 11.0

Refer to the PAN-OS® 11.0 documentation on the Technical Documentation portal for general information on how to configure and use already-released features.

- PAN-OS 11.0 New Features Guide—Detailed information on configuring the features introduced in this release.
- PAN-OS 11.0 Upgrade Guide—Provides considerations and steps to upgrade PAN-OS.
- PAN-OS 11.0 Administrator's Guide—Provides the concepts and solutions to get the most out of your Palo Alto Networks next-generation firewalls. This includes taking you through the initial configuration and basic set up on your Palo Alto Networks firewalls.
- Panorama 11.0 Administrator's Guide—Provides the basic framework to quickly set up the Panorama™ virtual appliance or an M-Series appliance for centralized administration of the Palo Alto Networks firewalls.
- PAN-OS 11.0 Networking Administrator's Guide—Provides concepts and details around Palo Alto Networks firewall networking solution.
- Advanced WildFire Administration—Provides steps to set up a Palo Alto Networks firewall to forward samples for WildFire® Analysis, to deploy the WF-500 appliance to host a WildFire private or hybrid cloud, and to monitor WildFire activity.
- VM-Series 11.0 Deployment Guide—Provides details on deploying and licensing the VM-Series firewall on all supported hypervisors. It includes example of supported topologies on each hypervisor.
- GlobalProtect 10.1 (and later) Administrator's Guide—Describes how to set up and manage GlobalProtect™ features.
- PAN-OS 11.0 Web Interface Help—Detailed, context-sensitive help system integrated with the firewall and Panorama web interface.
- Palo Alto Networks Compatibility Matrix—Provides operating system and other compatibility information for Palo Alto Networks next-generation firewalls, appliances, and agents.