Palo Alto Networks Global Customer Services Support Resource Guide

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 www.paloaltonetworks.com/documentation.
- To search for a specific topic, go to our search page www.paloaltonetworks.com/documentation/document-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

Last Revised

May 2020

Dear Palo Alto Networks Customer,

Thank you! We greatly appreciate you entrusting Palo Alto Networks to secure and protect your business. Your organization counts on you—the cyber defender—to ensure the total protection and safety of your digital assets. Our intent is to be your cybersecurity partner of choice. Your protection is our priority.

Our commitment to your success is unwavering as we strive to deliver an exceptional customer experience for you. The Global Customer Services (GCS) organization and Authorized Support Centers are here to ensure maximum uptime and streamlined operations.

We offer a number of support services to optimize your Palo Alto Networks implementation and operation to ensure complete security. There are numerous enhancements to our support systems that make it easier for you to quickly and efficiently find the answers you are searching for, including:

- **LIVEcommunity**—a peer-to-peer online community of intelligent and collaborative network security and IT professionals working to address similar challenges together. Improvements to our search capabilities include the use of artificial intelligence to produce the most relevant results—enabling you to find answers fast.
- Improved resources, such as Knowledge Base, TechDocs, and the Customer Support Portal, to help answer your questions and solve your issues promptly.
- **Platinum Support**—a new support offering for your convenience. Platinum Support is a top-tier support offering that provides you with the expertise you need, exactly when you need it, to keep your business safe and secure. Platinum Support provides the fastest response times with a dedicated team of senior engineers to resolve any support issues.
- Finally, we've been recognized by TSIA and J.D. Power for the fifth consecutive year for providing "An Outstanding Customer Service Experience" with our Assisted Technical Support.

Please use this resource guide to help better acquaint yourself with the array of support services that are available to you. Remember, we are here to help you protect your business and to solve your cybersecurity challenges.

Sincerely,

Patty Hatter
SVP, Global Customer Services
Palo Alto Networks

Table of Contents

1. Overview of Support Resources

Palo Alto Networks Support provides timely access to the expertise needed to protect your business. Digital resources such as Knowledge Base, LIVEcommunity, Beacon, TechDocs, and other self-service tools are available 24/7, year-round.

The Global Customer Support teams, comprising Technical Support, Customer Service, and Hardware Services, provide around-the-clock web or phone support for customers with valid entitlements.

1.1 Self-Service Tools

We encourage you to use our self-service tools to help you quickly and efficiently find answers to your questions.

- **Knowledge Base**—knowledge-centered support to answer questions and resolve issues.
- **LIVEcommunity**—where authorized users can connect, share, and learn with other cybersecurity professionals through posts, blogs, and discussions.
- **Beacon**—one-stop education portal that gathers all Palo Alto Networks resources in one location.
- **TechDocs**—technical guides to all products, Best Practices, and resources, such as Release Notes and Compatibility Matrix.
- **Day 1 Configuration**—templates to build a baseline configuration based on best practices.
- **Applipedia**—application database used along with App-ID™ technology to identify applications traveling through your Palo Alto Networks Next-Generation Firewall.
- **Security Advisories**—lists all security vulnerabilities identified in currently supported Palo Alto Networks products.
- **Threat Vault**—enables authorized users to research the latest threats (vulnerabilities/exploits, viruses, and spyware) that Palo Alto Networks Next-Generation Firewalls can detect and prevent.
- **URL Filtering Categorization**—test URL filtering categories.
- **Updates**—software and dynamic (content) updates are available to authorized users in the Updates section of the Customer Support Portal (CSP).

1.2 Technical Support

Technical support for Palo Alto Networks products is available 24/7, year-round by web or phone for customers with Platinum and Premium Support. Standard Support is available during business hours. Customers with Premium Partner Support will open cases through their Authorized Support Center (ASC).

Technical Support handles:

- Technical break/fix and how-to issues
- Product software or feature problems (bugs)
- Defective returns (return merchandize authorization or RMAs)

To engage Technical Support, select Tech Support in the Type field when creating a web case or when prompted by the automated phone system.

1.3 Customer Service

Customer Service assists with non-technical administrative cases 24/7, year-round, including:

- Login Assistance for the Customer Support Portal
- Password resets and email address changes
- Product registration and license activation
- License management (expiration dates, grace period, bundles)
- Product and license transfers

Select **Admin** in the **Type** field when creating a web case or when prompted by the automated phone system. (Note: Select **Tech Support** for product login administration issues.)

1.4 Hardware Services

Technical Support determines if a product is defective and will assign a subcase to the Hardware Services team for the logistics follow up. Hardware Services will:

- Obtain the delivery address.
- Verify trade compliance for international deliveries.
- Submit an RMA to logistics provider.
- Provide delivery updates.

To report defective hardware, select Tech Support in the Type field when creating a web case or when prompted by the automated phone system.

2. Support Plan

With business-critical customer support options and 24/7 availability, as well as a global network of support centers and parts-replacement depots, Palo Alto Networks provides a range of support and maintenance options designed to meet all business needs:

- Standard Support
- Premium Support
- Platinum Support
- Focused Services
- On-Site Spares Hardware Program

2.1 Case Response SLA

		Required Support Tiers (Asset)		Optional Focused Services (Account)		
		Premium	Platinum	Focused	Focused PLUS	Focused ELITE
Technical Support	Telephone support	24/7	24/7			
	Response time (critical issue)	1 hour	15 minutes			
	Support specialist type	Support Engineer	Senior Engineer	Support Engineer	Designated Engineer	Designated Engineers
	RMA	NBD | 4 hours	NBD | 4 hours			
Security Assurance*	Assisted security investigations	•	•			
	Advanced log & IOC analysis	•	•			
	Recommended next steps	•	•			
Expert Assistance	Planned event support		•			•
	On-site assistance (critical issue)		•			•
	Failure analysis (HW)		•			•
Personalized Experience (Focused Services)	Designated SAM			•	•	•
	Case Management/Escalation			•	•	•
	Weekly Reviews (Cases, Planning)			•	•	•
	Root Cause Analysis (HW + SW)			•	•	•
	Best Practice Reviews			•	•	•
	FCS Services Webinars			•	•	•
	Proactive Threat Notifications			•	•	•
	Release Reviews			•	•	•
	Designated Engineers				•	24/7
	Tailored Release Strategy				•	•
	Access to engineering				•	•
	Proactive Performance Sweep				1	2
	SecOps Optimization Service				1	2
Customer Surround	Designated Service Delivery Leader				(Tier 3)	(Tier 2 and 3)
	Orchestrate all services delivered				•	•
	Coordinate all designated resources				•	•
	Report activities and milestone				•	•
	Continuous develop services strategy				•	•

Figure 1: Service-level agreements for case response

2.2 Target Follow-Up Times

- **Severity 1**—Critical: Every 4 hours until resolved or a workaround is in place.
- **Severity 2**—High: Every business day.
- **Severity 3**—Every 3 business days until resolved.
- **Severity 4**—Low: Once per business week until resolved.

2.3 Case Severity Guidelines

- **Severity 1**—Critical: Product or mission critical feature is down and critically affecting the customer production environment. No workaround is available.
- **Severity 2**—High: Product is impaired and customer production is up but impacted. No workaround yet available.
- **Severity 3**—Medium: A product function has failed and customer production is not affected. Support is aware of the issue and there is a workaround available.
- **Severity 4**—Low: Product function is not impaired and has no impact on customer business. Includes feature functionality and configuration questions, information, and documentation how-tos and enhancement requests.

Recommended for critical cases: Create a web case through the CSP and set the severity as critical. If you would like to speak with the case owner, call Support and enter the case number into the automated system. To see the service level agreement for each case severity, see table 1 in section 4.5.

3. Technical Case Workflow

When a case is opened, a Technical Support Engineer will review the issue and data presented. The engineer will update the case either via **Case Comments** or call the customer at the phone number provided when opening the case.

If a live troubleshooting call is required, the TAC engineer will coordinate with the customer at an appropriate time.

3.1 How to Open a Case

Web cases may be created by authorized users from the Customer Support Portal (CSP) or through LIVEcommunity for technical (Tech Support) and non-technical (Admin) issues. These options are available to customers with Platinum, Premium, or Standard Support. Customers with Premium Partner Support will contact their Authorized Support Center.

CSP: https://support.paloaltonetworks.com > Support Cases

LIVEcommunity: https://live.paloaltonetworks.com > Create a Support Case

Knowledge Base articles will be suggested throughout the case creation process based on subject and description.

Recommended for critical cases: Create a web case through the CSP. Set the severity as critical. If you would like to speak with the case owner, call Support and enter the case number into the automated system.

If unable to create a login or access the **Support Cases** section of the CSP, request **Login Assistance**. If unable to locate the product serial number, select the option to have Customer Service submit the technical case. Customer Service will then investigate and resolve the issue with the serial number.

New cases are not accepted via email, but once a case is created, email may be used to view and reply to case updates.

3.2 Case Owner Responsibilities

Once a support case is opened with Palo Alto Networks TAC, depending upon product technology and service entitlements, the case is routed to an appropriate engineer. The engineer is responsible for the following:

- Take ownership of the Palo Alto Networks Support Case.
- Provide an Initial Response within SLA and perform troubleshooting, diagnostics or undertake any remediation steps.
- TAC will document all activity in Case Comments and provide updates as per the committed follow-up times based on Case Severity.
- Engage additional resources as needed to address issues.
- Follow up and close the Support Case upon confirmation from Customer.

3.3 Requesting an Event

An event is a scheduled session with a support engineer where all parties will join a bridge at a predetermined time to conduct whatever troubleshooting or maintenance has been agreed upon.

An event may be requested for:

- Failed upgrade attempts
- Maintenance windows associated to a support case with an existing technical issue
- Troubleshooting session to resolve an ongoing technical issue

If requesting a Support Event, review the Support Event Guidelines: When to request a Support Event.

The Customer Support Program Summary explains which entitlements include Planned Event assistance.

3.4 Case Resolution Process

Palo Alto Networks Support engineers will take ownership of the support case and work toward providing a resolution. If a resolution cannot be provided, the Support engineer will make best effort to provide a workaround or share mitigation plan. Support engineer may perform any or all of the following steps:

- Review network topology, firewall configuration, and analyze logs to provide next steps or debug issue.
- Perform live troubleshooting on customer device or replicate issue in a Palo Alto Networks lab.
- If the issue is determined to be hardware failure, proceed with an RMA.
- If the issue is determined to be Software Defect, raise an issue report with Engineering.
- Guide customer to correct resource if issue falls outside scope of Support.

3.5 Customer Best Practices for Engaging Support

We understand your business needs to resolve Support issues in a timely manner. To help provide you quality support

experience and resolve your issues quickly, we encourage our customers to follow the best practices when engaging with Palo Alto Networks Support:

- Search for help online. See Section 1.1 for self-help tools.
- If you do choose to open a web case, check the articles offered as you enter the subject and description to see if they will resolve the issue.
- Submit one problem per case. Fill in all fields to the best of your knowledge. Provide a brief summary and detailed description of the issue with as much information as possible.
- Set the appropriate severity of the support case. Raise or lower the severity through the case online through the CSP if the situation changes.
- For faster resolution, upload all relevant support files and logs to the case when opening it.
- Note the case owner's working hours in the response email signature. If you need immediate attention outside your assigned engineer's working hours, call Support.
- Update a case via the email generated each time a comment is made, online through **Case Comments** or call Support for urgent issues. There is no option to email Support directly.
- If you are unable to log in or create a case, request **assistance**.
- During Case Creation we may ask you to provide additional information for certain product types. We strongly encourage you to spend a few more minutes and answer these questions as they help to speed up the resolution time.

3.6 Software Defect Case Resolution Process

During the course of investigation of a Support Issue, if we determine the issue is due to a software failure, the assigned Support case engineer will follow the process below:

- Open an issue report with Palo Alto Networks engineering team.
- Share Issue Report ID with the customer and provide updates on resolution status.
- Share with the customer any available workarounds or mitigation steps in the interim.
- Once a fix is identified and we have a targeted software release version, we will share the release info and estimated time for the fix.

4. Access Support Resources

4.1 Customer Support Portal Login

Create a Customer Support Portal (CSP) account and user login to securely access Support resources. Once the CSP account is created, you'll be able to register products and auth codes. Among other features offered on the portal, you'll be able to manage memberships, run the Day 1 Configuration tool, connect to knowledge resources, and log Support cases for products with valid Platinum, Premium, or Standard support.

4.2 Open a Non-Critical Case

Support cases may be created by authorized users from the CSP or through LIVEcommunity for technical (Tech Support) and non-technical (Admin) issues. These options are available to customers with Platinum, Premium, or Standard Support. Customers with Premium Partner Support will contact their Authorized Support Center (ASC).

Be sure case **Subject** and **Description** are complete and provide a clear explanation of the issue, including:

- Serial number of the product or auth code
- Cluster peer if HA
- Date and time of the issue (if possible)
- Explain changes made to the network or any new traffic introduced
- Products in question upgraded or downgraded
- Any logs, screenshots, or ACC output that can help further analyze the issue
- Upload relevant product support files

Knowledge articles which may resolve your issue will be suggested throughout the case creation process based on subject and description.

If unable to create a login or access **Support Cases**, request **Login Assistance**. If a serial number is not found when creating a case, select the option to have Customer Service create and route the technical case. The team will then investigate and resolve the issue with the missing serial number.

New cases are not accepted via email, but once a case is created, email may be used to view and reply to case updates.

4.3 Open a Critical Case

- Open a web case through the CSP as described above and set the severity as Critical. Confirm that the product is down and critically affecting a production environment with no workaround available.
- Call Support if more immediate attention is needed and enter the case number in the automated system.

We will work the issue around the clock until a resolution or workaround is available. If we are unable to contact you, the severity of the case will be lowered.

4.4 Update Case

Update an existing case by replying to the email generated when a new comment is entered or by logging in to the Support Portal, selecting **Support Cases,** and filtering by **My Cases, My Company's Cases**, or entering the case serial number. Enter the comment and click the **Post Comment** button.

Call Support for urgent updates. Enter the case number when prompted by the phone system, and your case will be routed to the assigned case owner or the next available engineer.

4.5 Increase Case Severity

The table below provides case response SLAs. More detailed information can be found in Section 2.

Table 1: Service-Level Agreements for Case Response

Severity	First Response (Standard/ Premium/ Focused Services)	Follow-Up Response	Platinum Support First Response SLAs
Critical	< 1 Hour	Every 4 hours	< 15 Minutes
High	< 2 Business Hours	1 Business Day	< 30 Minutes
Medium	< 4 Business Hours	3 Business Days	< 2 Hours
Low	< 8 Business Hours	Once per Business Week	< 4 Hours

Severity Definitions

- **Severity 1**—Critical: Product is down and critically affects customer production environment. No workaround yet available.
- **Severity 2**—High: Product is impaired and customer production is up but impacted. No workaround yet available.
- **Severity 3**—Medium: A product function has failed and customer production is not affected. Support is aware of the issue and there is a workaround available.
- **Severity 4**—Low: Product function is not impaired and has no impact on customer business. Includes feature, information, documentation, how-to, and enhancement requests from the customer.

If the impact of the issue has increased since initially reported, increase the severity online. The system will generate a notification to the case owner or available team member.

If the issue has become critical, update the case online and call Support if you want to speak to an engineer. Once the case number is entered in the system, the call will route to the assigned case owner or next available team member.

If you are not satisfied with the progress of a case, then call Support and ask to speak with a Duty Manager.

If still not satisfied with the results, contact your Palo Alto Networks Systems Engineer and request a case escalation.

4.6 Report a Software Defect (Bug)

Open a technical support case to confirm a software defect. Providing the additional details below will lead to a faster resolution:

- Detailed problem description
- If any upgrades/downgrades were performed, including release versions
- How the issue is observed (if under specific circumstances/ traffic patterns)
- Any logs, screenshots, or ACC output that can help further analyze the issue
- Tech Support Files

4.7 Request RMA

To report defective hardware, select Tech Support in the Type field when creating a web case or when prompted by the automated phone system. See Section 6 for more details.

4.8 Report a Beta Release Issue

Invitation-only beta releases are supported through the Beta Forum on LIVEcommunity. The forum is the place for authorized beta participants to engage in discussions, ask questions, report issues, and provide feedback about the product.

Contact **BetaSupport@paloaltonetworks.com** or your System Engineer for information about beta programs.

4.9 Request a Feature Enhancement

To submit a feature enhancement, reach out to your local sales team, to create a new request or add your vote to an existing one. For a new feature enhancement, it helps to have as many details as possible to support the request:

- Use cases
- Business needs
- Comparable features
- Existing examples

A business justification will help the product teams and engineers decide which features merit the most priority for the next or subsequent releases.

4.10 Reopen a Closed Case

A closed case less than 60 days old may be reopened if the same issue reoccurs. Search for the case in the **Closed** case filter or enter the case serial number. Click the **Request to Reopen Case** button and provide the reason to reopen the case. Call Support if the issue is urgent and the case will be routed to the next available engineer.

5. Return Materials Authorization (RMA) Workflow

5.1 Request an RMA

To request an RMA, the defective device must be registered in the CSP with an active support auth code, and a technical case must be submitted.

Select **Tech Support** in the **Type** field when creating a web case or when prompted by the automated phone system. The Technical Support Engineer will troubleshoot the device to diagnose the defect.

Upon making a determination that an RMA is necessary, the engineer will route the case to the Hardware Services team, which will act immediately to:

- Obtain delivery address
- Verify trade compliance for international deliveries
- Submit RMA to logistics provider
- Provide delivery updates

5.2 RMA Delivery Times

RMAs must be delivered to a physical address (not a P.O. box), and a recipient signature is required.

Customers with a **4-Hour Support** contract will receive the replacement within four hours of submission of the RMA to the logistics provider by the Hardware Services team. The replacement will be delivered by private courier, and no **RMA tracking** information will be available in the RMA Tracking section of the case. Contact your case owner for delivery updates. A specific delivery time may be requested if delivery within four hours is not convenient. Palo Alto Networks will pay for all shipping costs associated with the advance replacement and defective return.

Customers with **Platinum, Premium**, or **Premium Partner Support** will receive Next Business Day (NBD) delivery, if the order is received by the logistics provider by 3 p.m. at the depot from which it is being shipped. With the exception of some countries where local couriers are used, tracking information (generally from FedEx or DHL) will appear in the RMA Tracking section of the case. If there is no tracking information in your case, the case owner should be able to obtain an update for you. Palo Alto Networks will pay for all shipping costs associated with the advance replacement and defective return.

Customers with **Standard Support** must return the defective unit at their own expense to the address provided in the case by the Hardware Services team. A replacement unit will be shipped upon receipt. Replacement shipping costs will be paid by Palo Alto Networks. (Note: LAB and NFR units have **Standard Support**; however, RMAs will be processed with all NBD shipping rules.)

An Importer of Record (IOR) must be identified if shipping to a country that does not have a local depot. The IOR will facilitate customs clearance of the device. The device will remain in customs and eventually be returned to Palo Alto Networks or destroyed if no IOR is provided. Palo Alto Networks will reimburse any shipping and duty costs incurred if the device is under **Platinum, Premium**, or **Premium Partner Support**. Your Sales team will be able to provide information about depot locations. Shipping times will vary depending on the trade rules in these countries.

The RMA Process and Policy document provides additional detailed RMA information.

5.3 RMA License Transfers

The replacement device will be SKU'd as a "Spare" to permit the license transfer from defective to replacement.

Customers with an On-Site Spare (OSS) device will be able to transfer licenses from the defective device to the OSS using the steps in the above link. There are two replacement options with an OSS:

- Leave the OSS in the production network and use the RMA replacement as the new spare.
- Transfer the licenses from the OSS to the replacement spare and open an **Admin** Case to have the OSS returned to spares inventory.

Once the license transfer is complete, the spare device will have all of the attributes of the defective unit. The defective device will have valid licensing for 30 days from the date of the transfer to allow time to remove the unit from a production network.

Be sure to transfer licenses prior to returning the defective device. If the defective serial number is no longer visible in the CSP account, license recovery may still be possible using the **Can't Find Defective Serial Number** option. If still unable to find the serial number, create an Admin web case and Customer Service will assist.

5.4 Returning the Defective Platform/Part

A defective platform should be returned to Palo Alto Networks within 10 days of receipt of the replacement unit. Return instructions and a prepaid return airway bill will be provided with the replacement unit. Customers are asked to provide information for the Asset Recovery Contact in the RMA form. This is the person the Asset Recovery team will communicate with should the unit not be returned within 10 days.

Here are some additional RMA instructions and details:

- Click the **Missing Return Instructions** button in your RMA case if unable to locate your return instructions. The **Asset Recovery Contact** should receive new instructions within one business day.
- If the device will not be returned within 10 days, request an extension via case comments and provide an estimated return date. The Hardware Services team will notify Logistics.
- If returning the replacement or realize that the serial number reported defective is incorrect, update the **Case Comments** with the serial number being returned. The Hardware Services team will notify Logistics.
- Failure to return a defective device will result in the decommissioning of that serial number. Failure to notify Palo Alto Networks of a change to the returned serial number may also result in the decommissioning of the original serial number reported.
- Many defective parts do not need to be returned. The Hardware Service team will advise via **Case Comments** if the defective part can be recycled. No prepaid airway bill will be provided with the replacement for parts that do not need to be returned.

5.5 Failure Analysis Reports

A detailed failure analysis report may only be requested for devices entitled with Platinum Support. When submitting the case for such serial numbers, indicate in the **Case Comments** that a failure analysis report is needed. The Hardware Services team will include the request when submitting the RMA to Logistics. Failure analysis may be requested after the RMA has been submitted up until the returned unit has been scrubbed of all customer data. The Hardware Services team will be able to advise the status of the defective serial number.

Failure Analysis for devices with Premium Support will be provided on an exception basis only with a Technical Support Manager's approval. Failure Analysis is not available for devices with Standard Support.

6. Security Vulnerability Workflow

6.1 Definition of a Security Vulnerability

Palo Alto Networks defines a Security Vulnerability as a weakness or flaw in a product or service that could allow an attacker to compromise the integrity, availability, or confidentiality of the product or service.

NOTE: This specifically excludes network security-related functionality of the product or service (e.g., intrusion prevention, application or file identification, antivirus, malware analysis) which pertain to the function and efficacy of the product or service. Issues pertaining to security-related functionality of a product or service will be handled via Palo Alto Networks Customer Support.

6.2 How to Report a Security Vulnerability

Contact the Palo Alto Networks Product Security Incident Response Team (PSIRT) by completing the Palo Alto Networks Product Vulnerability – Report a Security Vulnerability form or submitting an email to **psirt@paloaltonetworks.com**. We encourage the submission of vulnerabilities via encrypted email. Our PGP public key is available here.

Please include details on the software and hardware configuration, reproduction steps, potential impact, and a proof of concept (if possible). This will enable us to duplicate the issue and respond to your report more quickly. **In order to avoid reporting a known issue that has already been resolved, we recommend all testing be performed on the most recent software version available from https://support.paloaltonetworks.com.**

6.3 Acknowledgement and Analysis of a Vulnerability Report

PSIRT will acknowledge the receipt of the report within two (2) business days. A tracking number will be provided in the acknowledgment email. Please include this tracking number in the subject of all further email communications relating to the submission. Upon receiving all relevant information, we will endeavor to provide a response with our analysis within five (5) business days. Some issues may be more complex and require more time to investigate.

6.4 Fix or Corrective Action

Palo Alto Networks will provide a fix for a security vulnerability that affects our products or services that are not end of life. Our end-of-life policy can be viewed at End-of-Life Summary.

The fix may take one or more of the following forms:

- For customer-delivered software (such as PAN-OS and Panorama), a software fix included in a subsequent major or minor release of the affected product
- For cloud-based services (such as Aperture and AutoFocus), a software fix applied to the cloud-delivered service
- A corrective procedure or workaround to mitigate the impact of the vulnerability

6.5 Notification of Product Security Information and Software Updates

Information relating to addressed vulnerabilities are published in Security Advisories on our website at Palo Alto Networks Product Vulnerability – Security Advisories.

6.6 Publication of Security Advisories

Security Advisories are published under the following situations:

- A security issue that is specific to our software or that affects open source software which can reasonably be assumed to affect our software is publicly reported and widely available, AND a fix is available in one or more supported software versions.
- A security issue that affects our software is privately reported to Palo Alto Networks, AND a fix is available in all currently supported software versions.

Security Advisories will contain a Description, Common Vulnerability Enumerator (CVE), Impact, Severity, Affected Products, Available Updates, and Acknowledgement of the reporter (if applicable).

We may publish follow-up blog posts or Knowledge Base articles for issues that drive high volumes of support requests or generate media attention, or in cases where additional information is useful to support our customers after the release of a Security Advisory.

Customers can sign up for email notification of new or updated Security Advisories on our support website at https://support.paloaltonetworks.com.

6.7 Security Assurance

If you detect suspicious activity in your network, Security Assurance provides extra help from Palo Alto Networks when you need it the most. Security Assurance provides:

- Access to Palo Alto Networks security experts and their specialized threat intelligence tools and threat hunting practices.
- Advanced log and indicators of compromise (IOC) analysis.
- Configuration assessment that includes customized product security recommendations.
- Next step recommendations to expedite the transition to your incident response (IR) vendor to help manage and resolve the incident.

To take advantage of Security Assurance, you must subscribe to the Premium Support Contract (on or after November 1, 2019) or to the Platinum Support Contract. The first step toward Security Assurance is to run the Best Practice Assessment (BPA) to measure your adoption of seven key security capabilities.

If you experience suspicious activity, when you engage Security Assurance, you must provide a specific set of data about the suspected incident so Palo Alto Networks' experts can investigate the activity. After you collect data about the suspicious activity to ensure the timely analysis of the relevant information, you're ready to engage Security Assistance. You can engage Security Assistance in two ways:

Log in to the Customer Support Portal. Click **Create a Case** to open a support case. When you fill out the form, select **Threat**.

Your sales engineer (SE) can open a support case on your behalf.

For further information on Security Assurance, please visit this best practices document.

7. End of Life Announcements

Products eventually reach their natural end of life for various reasons, including new and better technologies becoming available, marketplace changes, or source parts and technologies are unavailable. This is part of any technology product's lifecycle. It is a goal of Palo Alto Networks to make this process as seamless as possible for you and our partners as well as to provide as much visibility into what you can expect during the process.

- End-of-Life (EOL) Policy
- End-of-Sale Announcement
- Software End-of-Life Dates
- Hardware End-of-Life Dates

8. Appendix A: Quick Reference to Support Resources

8.1 Overview

Palo Alto Networks offers a variety of online resources to answer product questions, resolve issues and provide configuration help.

Support is available for product issues 24/7, year-round with current Platinum or Premium entitlements. Premium Partner Support will be provided by the contracted Authorized Service Center.

8.2 Online Self-Help

- **Day 1 Configuration**—templates to build a baseline configuration based on best practices.
- **Knowledge Base**—knowledge-centered support to answer questions and resolve issues.
- **LIVEcommunity**—where authorized users can connect, share and learn with other cybersecurity professionals, through posts, blogs, and discussions.
- **TechDocs**—technical guides to all products, Best Practices and resources such as Release Notes, and Compatibility Matrix.
- **Beacon**—a one-stop education portal that gathers all Palo Alto Networks resources in one location.
- **Applipedia**—application database used along with App-ID to identify applications traveling through your Palo Alto Networks Next-Generation Firewall.
- **Security Advisories**—listing of all security vulnerabilities identified in currently supported Palo Alto Networks products.
- **Threat Vault**—enables authorized users to research the latest threats (e.g., vulnerabilities/exploits, viruses, spyware) that Palo Alto Networks Next-Generation Firewalls can detect and prevent.
- **URL Filtering Categorization**—test URL filtering categories.
- **Updates**—software and dynamic (content) updates are available to authorized users in the Updates section of the Customer Support Portal (CSP).

8.3 How to Open a Case

Web cases may be created by authorized users from the Customer Support Portal (CSP) or through LIVEcommunity for technical (Tech Support) and non-technical (Admin) issues. These options are available to customers with Platinum, Premium, or Standard Support. Customers with Premium Partner Support will contact their Authorized Support Center.

CSP: https://support.paloaltonetworks.com > Support Cases

LIVEcommunity: https://live.paloaltonetworks.com > Create a Support Case Now

Knowledge Base articles will be suggested throughout the case creation process based on subject and description.

Recommended for critical cases: Create a web case through the CSP. Set the severity as critical. If you like to speak with the case owner, call Support and enter the case number in the automated system.

If unable to create a login or access the **Support Cases** section of the CSP, request **Login Assistance**. If unable to locate the product serial number, select the option to have Customer Service submit the technical case. Customer Service will then investigate and resolve the issue with the serial number.

New cases are not accepted via email, but once a case is created, email may be used to view and reply to case updates.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com