Contact Information

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

About this Guide

This guide describes the Palo Alto Networks next-generation firewall and Panorama web interfaces. It provides reference information on how to populate fields within these web interface. For additional information, refer to the following resources:

- For information on the additional capabilities and for instructions on configuring the features on the firewall, refer to https://docs.paloaltonetworks.com.
- For access to the knowledge base, discussion forums, and videos, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/services/solution-assurance.
- For the most current PAN-OS and Panorama release notes, see https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes.html.

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

▲ Firewall Overview
▲ Features and Benefits
▲ Management Interfaces
▲ Last Login Time and Failed Login Attempts
▲ Message of the Day
▲ Task Manager
▲ Language
▲ Alarms
▲ Commit Changes
▲ Lock Configurations
▲ Save Candidate Configurations
Palo Alto Networks® offers a full line of next-generation security appliances that range from the PA-200 firewall, designed for enterprise remote offices, to a PA-7000 Series firewall, which is a modular chassis designed for high-speed data centers. The firewall allows you to specify security policies based on accurate identification of each application that will traverse your network. Unlike traditional firewalls that identify applications only by protocol and port number, the Palo Alto Networks next-generation firewall uses packet inspection and a library of application signatures to distinguish between applications that have the same protocol and port and to identify potentially malicious applications that use nonstandard ports.

To safely enable the use of applications, maintain complete visibility and control, and protect the organization from the latest cyber threat, you can define security policies for specific applications or application groups rather than use a single policy for all port 80 connections. For each identified application, you can specify a security policy to block or allow traffic based on the source and destination zones and addresses (IPv4 and IPv6). Each security policy can also specify security profiles to protect against viruses, spyware, and other threats.
Features and Benefits

The Palo Alto Networks next-generation firewalls provide granular control over the traffic allowed to access your network. The primary features and benefits include:

- **Application-based policy enforcement (App-ID)**—Access control according to application type is far more effective when application identification is based on more than just protocol and port number. The App-ID™ service can block high risk applications, as well as high risk behavior, such as file-sharing, and traffic encrypted with the Secure Sockets Layer (SSL) protocol can be decrypted and inspected.

- **User identification (User-ID)**—The User-ID™ feature allows administrators to configure and enforce firewall policies based on users and user groups instead of or in addition to network zones and addresses. The firewall can communicate with many directory servers, such as Microsoft Active Directory, eDirectory, SunOne, OpenLDAP, and most other LDAP-based directory servers to provide user and group information to the firewall. You can then use this information for secure application enablement that can be defined per user or group. For example, the administrator could allow one organization to use a web-based application but not allow any other organizations in the company to use that same application. You can also configure granular control of certain components of an application based on users and groups (see User Identification).

- **Threat prevention**—Threat prevention services that protect the network from viruses, worms, spyware, and other malicious traffic can be varied by application and traffic source (see Objects > Security Profiles).

- **URL filtering**—Outbound connections can be filtered to prevent access to inappropriate web sites (see Objects > Security Profiles > URL Filtering).

- **Traffic visibility**—Extensive reports, logs, and notification mechanisms provide detailed visibility into network application traffic and security events. The Application Command Center (ACC) in the web interface identifies the applications with the most traffic and the highest security risk (see Monitor).

- **Networking versatility and speed**—The Palo Alto Networks firewall can augment or replace your existing firewall and can be installed transparently in any network or configured to support a switched or routed environment. Multigigabit speeds and a single-pass architecture provide these services to you with little or no impact on network latency.

- **GlobalProtect**—The GlobalProtect™ software provides security for client systems, such as laptops that are used in the field, by allowing easy and secure login from anywhere in the world.

- **Fail-safe operation**—High availability (HA) support provides automatic failover in the event of any hardware or software disruption (see Device > Virtual Systems).

- **Malware analysis and reporting**—The WildFire™ security service provides detailed analysis and reporting on malware that passes through the firewall.

- **VM-Series firewall**—A VM-Series firewall provides a virtual instance of PAN-OS® positioned for use in a virtualized data center environment and is ideal for your private, public, and hybrid cloud computing environments.

- **Management and Panorama**—You can manage each firewall through an intuitive web interface or through a command-line interface (CLI) or you can centrally manage all firewalls through the Panorama™ centralized management system, which has a web interface very similar to the web interface on Palo Alto Networks firewalls.
Management Interfaces

Palo Alto Networks next-generation firewalls support the following management interfaces.

- **Web interface**—Configuration and monitoring over HTTP or HTTPS from a web browser. For detailed step-by-step instructions on how to configure and manage the firewall, refer to the PAN-OS Administrator’s Guide.

- **CLI**—Text-based configuration and monitoring over Telnet, Secure Shell (SSH), or the console port. For information on how to use the CLI, including on information on how to find a command and get help on command syntax, refer to the CLI Quick Start.

- **Panorama**—Palo Alto Networks product that provides web-based management, reporting, and logging for multiple firewalls. The Panorama web interface is similar to the firewall web interface but with additional management functions (for details, see to the Panorama Administrator’s Guide).

- **XML API**—Provides a Representational State Transfer (REST)-based interface to access firewall configuration, operational status, reports, and packet captures from the firewall. There is an API browser available on the firewall at https://<firewall>/api, where <firewall> is the host name or IP address of the firewall. This link provides help on the parameters required for each type of API call. For details, refer to the PAN-OS and Panorama XML API Usage Guide.
Last Login Time and Failed Login Attempts

To detect misuse and prevent exploitation of a privileged account, such as an administrative account on a Palo Alto Networks firewall or Panorama, the web interface and the command line interface (CLI) displays your last login time and any failed login attempts for your username when you log in. This information allows you to easily identify whether someone is using your administrative credentials to launch an attack.

After you log in to the web interface, the last login time information appears at the bottom left of the window. If one or more failed logins occurred since the last successful login, a caution icon appears to the right of the last login information. Hover over the caution symbol to view the number of failed login attempts or click to view the Failed Login Attempts Summary window, which lists the administrator’s account name, the source IP address, and the reason for the login failure.

If you see multiple failed login attempts that you do not recognize as your own, you should work with your network administrator to locate the system that is performing the brute-force attack and then investigate the user and host computer to identify and eradicate any malicious activity. If you see that the last login date and time indicates an account compromise, you should immediately change your password and then perform a configuration audit to determine if suspicious configuration changes were committed. Revert the configuration to a known good configuration if you see that logs were cleared or if you have difficulty determining if improper changes were made using your account.
Message of the Day

If you or another administrator configured a message of the day, or Palo Alto Networks embedded one as part of a software or content release, a Message of the Day dialog displays automatically upon login to the web interface. This ensures that you see information, such as an impending system restart, that might affect the tasks you intend to perform.

The dialog displays one message per page. If the dialog includes the option to select Do not show again, you can select it for each message that you don't want the dialog to display after subsequent logins.

Anytime the Message of the Day changes, the message appears in your next session even if you selected Do not show again during a previous login. You must then reselect this option to avoid seeing the modified message in subsequent sessions.

To navigate the dialog pages, click the right ( ) and left ( ) arrows along the sides of the dialog or click a page selector ( ) along the bottom of the dialog. After you Close the dialog, you can manually reopen it by clicking messages ( ) at the bottom of the web interface.

To configure a message of the day, select Device > Setup > Management and edit the Banners and Messages settings.
Task Manager

Click **Tasks** at the bottom of the web interface to display the operations that you, other administrators, or PAN-OS initiated since the last firewall reboot (for example, manual commits or automatic FQDN refreshes). For each task, the Task Manager provides the following information and actions.

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>The type of operation, such as log request, license refresh, or commit. You can click certain types to see more details about the operation, such as warning messages.</td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>Indicates whether the operation is pending (such as commits with Queued status), in progress (such as log requests with Active status), completed, or failed. For commits in progress, the Status indicates the percentage of completion.</td>
</tr>
<tr>
<td><strong>Start Time</strong></td>
<td>The date and time when the operation started. For commit operations, the Start Time indicates when a commit was added to the commit queue.</td>
</tr>
<tr>
<td><strong>Messages</strong></td>
<td>Displays details about the operation. If the entry indicates that there are too many messages, you can click the operation Type to see the messages. For commit operations, the Messages include the dequeued time to indicate when PAN-OS started performing the commit. To see the description an administrator entered for a commit, click <strong>Commit Description</strong>. For details, see <strong>Commit Changes</strong>.</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td>Click x to cancel a pending commit.</td>
</tr>
<tr>
<td><strong>Show</strong></td>
<td>Display <strong>All</strong> tasks (default) or only <strong>Running</strong> tasks (in progress), and optionally filter the list by task type (<strong>Jobs, Reports</strong>, or <strong>Log Requests</strong>).</td>
</tr>
<tr>
<td><strong>Clear Commit Queue</strong></td>
<td>Cancel all pending commits (available only to predefined administrative roles).</td>
</tr>
</tbody>
</table>
Language

By default, the locale (such as Spanish) of the computer from which you log in to the firewall determines the language that the web interface displays. To change the Language (bottom of the web interface), select a Language from the drop-down and click OK. The web interface then refreshes using the new language.
Alarms

An alarm is a firewall-generated message indicating that the number of events of a particular type (for example, encryption and decryption failures) has exceeded the threshold configured for that event type (see Define Alarm Settings). When generating an alarm, the firewall creates an Alarm log and opens the System Alarms dialog to display the alarm. After closing the dialog, you can reopen it anytime by clicking Alarms ( ) at the bottom of the web interface. To prevent the firewall from automatically opening the dialog for a particular alarm, select Unacknowledged Alarms and click Acknowledge to move the alarms to the Acknowledged Alarms list.
Commit Changes

Click **Commit** at the top right of the web interface to commit, validate, or preview your changes to the firewall configuration. Committing applies the candidate configuration to the running configuration, which activates all configuration changes since the last commit. To save, revert, import, export, or load configurations, select **Device > Setup > Operations**.

The firewall queues commit requests so that you can initiate a new commit while a previous commit is in progress. The firewall performs the commits in the order they are initiated but prioritizes commits that the firewall initiates automatically, such as FQDN refreshes. If the queue already has the maximum number of administrator-initiated commits (which varies by platform), you must wait for the firewall to finish processing a pending commit before initiating a new commit. Use the **Task Manager** to cancel commits or see details about commits that are pending, in progress, completed, or failed.

In the Commit dialog, click **Advanced** to display the following options.

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Device and Network configuration</td>
<td>Select this option to commit changes to settings in the <strong>Device</strong> and <strong>Network</strong> tabs (enabled by default).</td>
</tr>
<tr>
<td>Include Shared Object configuration</td>
<td>Select this option to commit changes to shared objects (enabled by default). This option is available only on firewalls with multiple virtual systems.</td>
</tr>
<tr>
<td>Include Policy and Object configuration</td>
<td>Select this option to commit changes to settings in the <strong>Policy</strong> and <strong>Objects</strong> tabs (enabled by default). This option is available only on firewalls for which the multiple virtual systems capability is disabled.</td>
</tr>
<tr>
<td>Include Virtual System configuration</td>
<td>Select this option to commit changes to policies and objects in <strong>All virtual systems</strong> (default) or <strong>Select one or more virtual systems</strong> in the list (enabled by default). This option is available only on firewalls with multiple virtual systems.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description (up to 512 characters) for the commit. A brief summary of what changed in the configuration is useful to other administrators who might want to know this without performing a configuration audit (comparison). The System log for a commit event will truncate the description value if it exceeds 512 characters.</td>
</tr>
<tr>
<td>Preview Changes</td>
<td>Click <strong>Preview Changes</strong> to compare the candidate configuration to the running configuration. Use the <strong>Lines of Context</strong> drop-down to specify the number of lines—from the compared configuration files—to display before and after each highlighted difference. If you select All, the results include the entire configuration files. Changes are color-coded based on configurable settings: added (green), modified (yellow), and deleted (red). The <strong>Device &gt; Config Audit</strong> feature performs the same function (see <strong>Device &gt; Config Audit</strong>). Because the preview results display in a new window, your browser must allow pop-up windows. If the preview window does not open, refer to your browser documentation for the steps to unblock pop-up windows.</td>
</tr>
</tbody>
</table>
### Validate Changes
Select this option to perform a syntactic validation (whether configuration syntax is correct) and semantic validation (whether the configuration is complete and makes sense) of the firewall configuration before committing the changes. The response will include all of the errors and warnings that a full commit or virtual system commit would, including rule shadowing and application dependency warnings; however, no changes are made to the running configuration. This validation helps you know if a change can be successfully committed before actually committing it, significantly reducing failures at commit time. To control who can validate configurations, you can enable or disable the **Validate** option in Admin Role profiles.

### Commit
Select this option to start the commit or, if other commits are pending, to add it to the commit queue.
Lock Configurations

To help you coordinate configuration tasks with other firewall administrators during concurrent login sessions, the web interface enables you to apply a configuration or commit lock so that other administrators cannot change the configuration or commit changes until the lock is removed.

At the top right of the web interface, a locked padlock (🔒) indicates that one or more locks are set (with the number of locks in parentheses); an unlocked padlock (_unlocked padlock) indicates that no locks are set. Clicking either padlock opens the Locks dialog, which provides the following options and fields.

<table>
<thead>
<tr>
<th>Field/Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin</td>
<td>The username of the administrator who set the lock.</td>
</tr>
<tr>
<td>Location</td>
<td>On a firewall with more than one virtual system (vsys), the scope of the lock can a specific vsys or the Shared location.</td>
</tr>
</tbody>
</table>
| Type | The lock type can be:  
- **Config Lock**—Blocks other administrators from changing the candidate configuration. Only a superuser or the administrator who set the lock can remove it.  
- **Commit Lock**—Blocks other administrators from committing changes made to the candidate configuration. The commit queue does not accept new commits until all locks are released. This lock prevents collisions that can occur when multiple administrators make changes during concurrent login sessions and one administrator finishes and initiates a commit before the other administrators have finished. The firewall automatically removes the lock after completing the commit for which the administrator set the lock. A superuser or the administrator who set the lock can also manually remove it. |
| Comment | Enter up to 256 characters of text. This is useful for other administrators who want to know the reason for the lock. |
| Created At | The date and time when an administrator set the lock. |
| Logged In | Indicates whether the administrator who set the lock is currently logged in. |
| Take a Lock | To set a lock, **Take a Lock**, select the **Type**, select the **Location** (multiple virtual system firewalls only), enter optional **Comments**, click **OK**, and then **Close**. |
| Remove Lock | To release a lock, select it, **Remove Lock**, click **OK**, and then **Close**. |

To configure the firewall to automatically set a commit lock whenever an administrator changes the candidate configuration, select **Device > Setup > Management**, edit the General Settings, enable **Automatically Acquire Commit Lock**, and then click **OK** and **Commit**.
Save Candidate Configurations

Click Save at the top right of the web interface to create a snapshot file (.snapshot.xml) of the candidate configuration or to overwrite the existing snapshot with your latest changes. If the firewall reboots before you commit your changes, you can then revert the candidate configuration to the current snapshot to restore changes you made between the last commit and the last snapshot. To revert to the snapshot, select Device > Setup > Operations and click Revert to last saved configuration. If you don’t revert to the snapshot after a reboot, the candidate configuration will be the same as the last committed configuration (the running configuration).

Saving your changes to the candidate configuration does not activate those changes. You must Commit Changes to activate them.

If you want to save configuration changes without overwriting the default snapshot file (.snapshot.xml), select Device > Setup > Operations, click Save named configuration snapshot, and specify a different Name for the snapshot file.