

PAN-OS[®] *New Features Guide*

Version 9.0

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 12, 2019

Table of Contents

Upgrade to PAN-OS 9.0.....	7
Upgrade/Downgrade Considerations.....	9
Upgrade the Firewall to PAN-OS 9.0.....	13
Determine the Upgrade Path to PAN-OS 9.0.....	13
Upgrade Firewalls Using Panorama.....	15
Upgrade a Standalone Firewall to PAN-OS 9.0.....	20
Upgrade an HA Firewall Pair to PAN-OS 9.0.....	23
Downgrade from PAN-OS 9.0.....	27
Downgrade a Firewall to a Previous Feature Release.....	27
Downgrade a Firewall to a Previous Maintenance Release.....	28
Downgrade a Windows Agent from PAN-OS 9.0.....	28
 App-ID Features.....	 31
Policy Optimizer.....	33
HTTP/2 Inspection.....	34
Strict Default Ports for Decrypted Applications.....	36
 Virtualization Features.....	 37
VM-Series Firewall on AWS—Support for C5 and M5 Instance Types with ENA.....	39
VM-Series Plugin.....	40
VM-Series Plugin on the VM-Series Firewall.....	40
VM-Series Plugin on Panorama.....	41
Plugin Upgrades.....	42
Support for HA for VM-Series on Azure.....	43
Higher Performance for VM-Series on Azure using Azure Accelerated Networking (SR-IOV).....	49
 Panorama Features.....	 51
Master Key Deployment from Panorama.....	53
Device Management Capacity Enhancement.....	54
Upgrade Panorama for Increased Device Management Capacity.....	55
Install a New Panorama for Increased Device Management Capacity.....	55
Granular Configuration Management of Device Groups and Templates.....	57
Streamlined Device Onboarding.....	58
 Content Inspection Features.....	 61
DNS Security.....	63
New Security-Focused URL Categories.....	64
Multi-Category URL Filtering.....	66
Built-In External Dynamic List for Bulletproof Hosts.....	68
EDL Capacity Increases.....	70
Support for New Predefined Data Filtering Patterns.....	73
Cellular IoT Security.....	75
GTP Event Packet Capture.....	80

GlobalProtect Features.....	83
Endpoint Tunnel Configurations Based on Source Region or IP Address.....	85
Portal Configuration Assignment and HIP-Based Access Control Using New Endpoint Attributes.....	88
Agent Configurations Based on the Endpoint's Machine Certificate.....	88
Agent Configurations Based on the Endpoint Serial Number.....	90
Agent Configurations Based on Software and App Settings.....	91
HIP-Based Policy Enforcement Based on the Endpoint Status.....	93
HIP Report Redistribution.....	100
DNS Configuration Assignment Based on Users or User Groups.....	102
Tunnel Restoration and Authentication Cookie Usage Restrictions.....	105
Mixed Authentication Method Support for Certificates or User Credentials.....	108
Pre-Logon Followed by Two-Factor Authentication.....	111
Pre-Logon Followed by SAML Authentication.....	112
GlobalProtect Gateway and Portal Location Configuration.....	113
User Location Visibility on GlobalProtect Gateways and Portals.....	114
Concurrent Support for IPv4 and IPv6 DNS Servers.....	117
Support for IPv6-Only GlobalProtect Deployments.....	118
 Management Features.....	 121
Enforcement of Rule Description, Tag, and Audit Comment.....	123
Rule Changes Archive.....	125
Tag Based Rule Groups.....	127
Policy Match and Connectivity Tests from the Web Interface.....	128
Rule Usage Filtering.....	129
Objects Capacity Improvements on the PA-5220 and PA-3200 Series Firewalls.....	130
API Key Lifetime.....	132
PAN-OS REST API for a Simplified Integration Experience.....	133
Universally Unique Identifiers for Policy Rules.....	134
Temporary Master Key Expiration Extension.....	138
Real-Time Enforcement and Expanded Capacities for Dynamic Address Groups.....	139
IP-Tag Log.....	139
IP-Tag Timeout.....	140
 Networking Features.....	 143
Security Group Tag (SGT) Ethertype Support.....	145
FQDN Refresh Enhancement.....	146
GRE Tunneling Support.....	148
Wildcard Address Support in Security Policy Rules.....	150
Hostname Option Support for DHCP Clients.....	154
FQDN Support for Static Route Next Hop, PBF Next Hop, and BGP Peer.....	155
Dynamic DNS Support for Firewall Interfaces.....	156
HA1 SSH Key Refresh.....	158
Advanced Session Distribution Algorithms for Destination NAT.....	159
VXLAN Tunnel Content Inspection.....	161
 User-ID Features.....	 165
WinRM Support for Server Monitoring.....	167
Shared User-ID Mappings Across Virtual Systems.....	170
User-ID Support for Large Numbers of Terminal Servers.....	173

WildFire Features..... 175

 Increased WildFire File Forwarding Capacity.....177

 WildFire Appliance Archive Support..... 179

Upgrade to PAN-OS 9.0

- > Upgrade/Downgrade Considerations
- > Upgrade the Firewall to PAN-OS 9.0
- > Downgrade from PAN-OS 9.0

Upgrade/Downgrade Considerations



The following table lists the new features that have upgrade or downgrade impact. Make sure you understand all upgrade/downgrade considerations before you upgrade to or downgrade from a PAN-OS 9.0 release. For additional information about PAN-OS 9.0 releases, refer to the [PAN-OS 9.0 Release Notes](#).



Review the following when upgrading Panorama to PAN-OS 9.0:

- For M-100 appliances, Palo Alto Networks requires upgrading the memory to 32GB or more for management and log collection tasks. See [M-100 Memory Upgrade Guide](#) for more information.
- [Upgrading Panorama with Local Log Collector or Dedicated Log Collectors](#).

Table 1: PAN-OS 9.0 Upgrade/Downgrade Considerations

Feature	Upgrade Considerations	Downgrade Considerations
VM-Series Plugin The VM-Series plugin manages integration with public and private clouds, allowing Palo Alto Networks to release bug fixes, new features, or new cloud integrations, independent of a PAN-OS release.	 <i>Save your PAN-OS 8.1 configuration before upgrading to PAN-OS 9.0.</i> The plugin is installed automatically when you install or upgrade the VM-Series firewall to PAN-OS 9.0. The plugin can be upgraded or downgraded, but it cannot be removed from PAN-OS.  <i>The plugin supports all clouds, so upgrades might not apply to you. Before upgrading the plugin, consult the release notes.</i> Each plugin version provides PAN-OS compatibility information. You can upgrade the plugin version from the VM-Series firewall with Device > Plugins > Check Now or from a bootstrap file.	If you have upgraded the VM-Series plugin independent of PAN-OS, downgrading to a previous release works the same as for other plugins. Downgrading from PAN-OS version 9.0 to 8.1 generates many error messages or disallows the downgrade. Instead of downgrading, restore your 8.1 configuration on a new firewall. <ol style="list-style-type: none">1. Deactivate any licenses for the VM-Series firewall, and delete the VM.2. Deploy a new VM-Series firewall and load your previously saved configuration.
Use Panorama to manage VM-Series plugin integrations with your managed firewalls.	If you have one or more cloud integrations configured in 8.1 when you upgrade to 9.0 (Google Stackdriver, Azure Application Insights, or AWS CloudWatch), the VM-Series plugin is automatically installed and any existing configuration is migrated to the VM-Series plugin. If you have not configured cloud integrations in 8.1, the VM-Series plugin	If you have upgraded the VM-Series plugin independent of Panorama, downgrading to a previous release works the same as for other plugins.

Feature	Upgrade Considerations	Downgrade Considerations
	<p>is supplied when you upgrade Panorama to 9.0, but it is not installed.</p> <p>In 9.0, if you want to manage cloud integrations from Panorama, go to Panorama > Plugins and use Check Now to view the VM-Series plugin. Load the VM-Series plugin, and install. Once installed the plugin can be upgraded and downgraded.</p>	
User-ID Support for Large Numbers of Terminal Servers	None.	To downgrade, remove any Alternative IP Addresses that contain an FQDN. If you have configured more than 1000 Terminal Services agents across all virtual systems on the firewall, remove agents until there are no more than 1000 before downgrading.
Shared User-ID Mapping Across Virtual Systems	None.	If you have consolidated the User-ID sources on the hub, you need to reconfigure the User-ID sources on each virtual system.
WinRM Support for Server Monitoring	None.	During a downgrade, any server profiles using WinRM-HTTP or WinRM-HTTPS are migrated to WMI.
Universally Unique Identifiers for Policy Rules	<p>When you upgrade, upgrade Panorama first, push the rulebases to the firewalls Panorama manages, and then upgrade the firewalls. If you do not push the policy configuration to the firewalls from Panorama before upgrading the managed firewalls, the upgrade will not be successful.</p> <p>In addition, if you are upgrading an HA pair (either managed by Panorama or standalone firewalls), upon upgrade to PAN-OS 9.0, each peer independently assigns UUIDs for each policy rule. Because of this, the peers will show as out of sync until you either sync the configuration or perform a commit on the active peer.</p> <p>In the ACC, the Rule field is now Rule Name to distinguish it from the new Rule UUID field.</p> <p>If you push a log forwarding profile that uses UUIDs from an upgraded Panorama to a firewall that has not been upgraded,</p>	<p>All UUIDs are retained as attributes so they can be reapplied to the rulebase in case you re-upgrade.</p> <p>If you are using UUIDs in log forwarding profiles or custom reports, the downgrade and any autocommits will be successful, but any subsequent commits will not be successful.</p> <p>If you downgrade Panorama, the Shared Policy column (Panorama > Managed Devices > Summary) for all devices displays as Out of sync, due to the missing UUIDs. After you commit and push the configuration to the devices, they will display as In sync.</p>

Feature	Upgrade Considerations	Downgrade Considerations
	the commit on the firewall will not be successful.	
Upgrading Panorama with Local Log Collectors or Dedicated Log Collectors	PAN-OS 9.0 introduces a new log data format, and as a result, the upgrade procedure may take up to six hours to complete in order for Panorama or the Log Collector to automatically reformat existing log data. During this time, log data is not visible in the ACC and Monitor tabs. Additionally, new log data is not forwarded to the appliance until the upgrade is complete.	Existing log data must be reformatted to the log format introduced in PAN-OS 8.0 upon downgrade using a log migration script provided by Palo Alto Networks. During the reformatting, log data is not visible in the ACC and Monitor tabs. Additionally, new log data is not forwarded to Log Collectors until the reformatting is complete.
	<p>All Log Collectors in a collector group must be upgraded at the same time to avoid any log data loss. If the majority of Log Collectors in a collector group are upgraded, the log data for the minority, non-upgraded Log Collectors are not visible in the ACC and Monitor tabs.</p> <p>For example, if you have three Log Collectors in a collector group, and you upgrade two of the Log Collectors, logs are not forwarded to the third non-upgraded Log Collector. Additionally, the existing log data for the third Log Collector is not displayed in the ACC or Monitor tabs.</p>	
Built-In External Dynamic List for BulletProof Hosts	None.	<p>Downgrade from PAN-OS 9.0 to earlier release versions is not supported for firewalls with security policy rules that use the predefined external dynamic lists for bulletproof hosts. Additionally, if Panorama pushes the list to a device group that includes pre-9.0 firewalls, the commit will fail.</p> <p>Workaround: In either of these cases, remove the bulletproof hosts list from any security policy rules that reference it.</p>
Multi-Category URL Filtering	Release versions earlier than PAN-OS 9.0 allowed you to configure URL Filtering block and allow lists as URL Filtering Overrides (Objects > Security Profiles > URL Filtering > Overrides). In PAN-OS 9.0, the Overrides tab no longer exists.	

Feature	Upgrade Considerations	Downgrade Considerations
	<p>Now, the option to configure URL Filtering block and allow lists is available when you create or modify a URL Filtering custom object (Objects > Custom Objects > URL Category).</p> <p>Contents of URL Filtering block and allow lists (including lists that you configured before upgrading to PAN-OS 9.0) are now displayed in the URL Filtering profile Categories tab, the Custom URL Categories dropdown (Objects > Security Profiles > URL Filtering > Categories). For details, see Multi-Category URL Filtering.</p> <p>In some cases, when the block and allow lists from previous release versions are merged with new Custom URL Categories list, the URL Filtering profile might reach its limit for custom URL categories, causing the PAN-OS 9.0 upgrade to fail.</p> <p>Workaround: Use this command to reset the ID manager process: <code>debug device-server reset id-manager type vsys-custom-url-category shared-custom-url-category</code>. If that doesn't work, you might need to remove some custom URL categories.</p>	

Upgrade the Firewall to PAN-OS 9.0

How you upgrade to PAN-OS 9.0 depends on whether you have standalone firewalls or firewalls in a high availability (HA) configuration and, for either scenario, whether you use Panorama to manage your firewalls. Review the [PAN-OS 9.0 Release Notes](#) and then follow the procedure specific to your deployment:

- [Determine the Upgrade Path to PAN-OS 9.0](#)
- [Upgrade Firewalls Using Panorama](#)
- [Upgrade a Standalone Firewall to PAN-OS 9.0](#)
- [Upgrade an HA Firewall Pair to PAN-OS 9.0](#)
- [Downgrade from PAN-OS 9.0](#)



When upgrading firewalls that you manage with Panorama or firewalls that are configured to forward content to a WildFire appliance, you must first [upgrade Panorama](#) and its [Log Collectors](#) and then [upgrade the WildFire appliance](#) before you upgrade the firewalls.

Determine the Upgrade Path to PAN-OS 9.0

When you upgrade from one PAN-OS feature release version to a later feature release, you cannot skip the installation of any feature release versions in the path to your target release. In addition, the recommended upgrade path includes installing the latest maintenance release in each release version before you install the base image for the next feature release version. To minimize downtime for your users, perform upgrades during non-business hours.

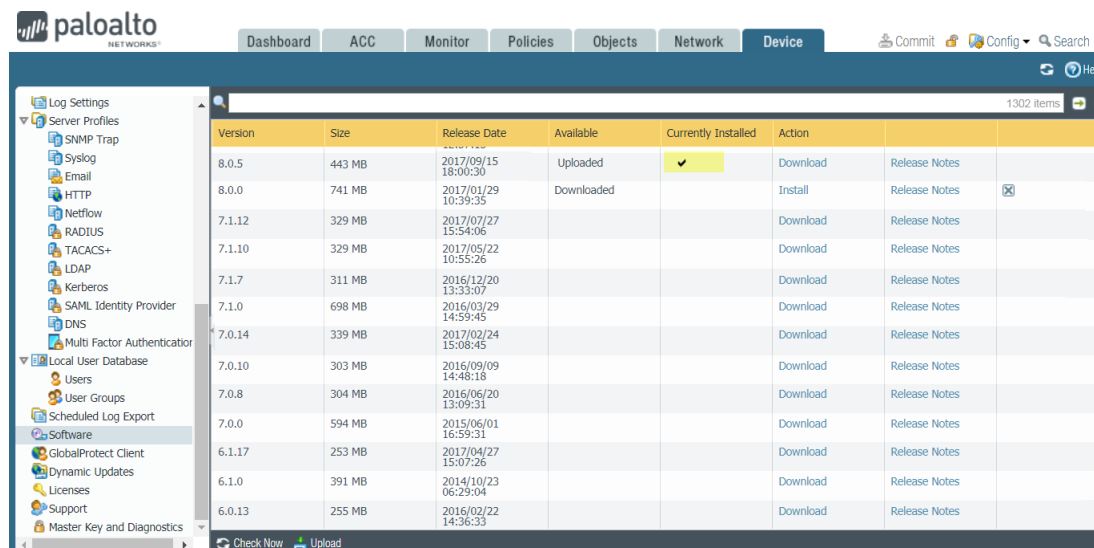


For manual upgrades, you must install the base image for a feature release before you upload and install a maintenance release image.

Determine the upgrade path as follows:

STEP 1 | Identify which version is currently installed.

- From Panorama, select **Panorama > Managed Devices** and check the Software Version on the firewalls you plan to upgrade.
- From the firewall, select **Device > Software** and check which version has a check mark in the Currently Installed column.



Version	Size	Release Date	Available	Currently Installed	Action		
8.0.5	443 MB	2017/09/15 18:00:30	Uploaded	✓	Download	Release Notes	
8.0.0	741 MB	2017/01/29 10:39:35	Downloaded		Install	Release Notes	✕
7.1.12	329 MB	2017/07/27 15:54:06			Download	Release Notes	
7.1.10	329 MB	2017/05/22 10:55:26			Download	Release Notes	
7.1.7	311 MB	2016/12/20 13:33:07			Download	Release Notes	
7.1.0	698 MB	2016/03/29 14:59:45			Download	Release Notes	
7.0.14	339 MB	2017/02/24 15:08:45			Download	Release Notes	
7.0.10	303 MB	2016/09/09 14:48:18			Download	Release Notes	
7.0.8	304 MB	2016/06/20 13:09:31			Download	Release Notes	
7.0.0	594 MB	2015/06/01 16:59:31			Download	Release Notes	
6.1.17	253 MB	2017/04/27 15:07:26			Download	Release Notes	
6.1.0	391 MB	2014/10/23 06:29:04			Download	Release Notes	
6.0.13	255 MB	2016/02/22 14:36:33			Download	Release Notes	

STEP 2 | Identify the upgrade path:



Review the known issues and changes to default behavior in the [Release Notes](#) and upgrade/downgrade considerations in the [New Features Guide](#) for each release through which you pass as part of your upgrade path.

Installed PAN-OS Version	Recommended Upgrade Path to PAN-OS 9.0
8.1.x	If you are already running a PAN-OS 8.1 release, download and install the latest PAN-OS 8.1 maintenance release and reboot. You can then proceed to Upgrade the Firewall to PAN-OS 9.0 .
8.0.x	<ul style="list-style-type: none">❑ Download and install the latest PAN-OS 8.0 maintenance release and reboot.❑ Download and install PAN-OS 8.1.0 and, as a best practice, reboot.❑ Download and install the latest PAN-OS 8.1 maintenance release and reboot.❑ Proceed to Upgrade the Firewall to PAN-OS 9.0.
7.1.x	<ul style="list-style-type: none">❑ Download and install the latest PAN-OS 7.1 maintenance release and reboot.❑ Download and install PAN-OS 8.0.0 and, as a best practice, reboot.❑ Download and install the latest PAN-OS 8.0 maintenance release and reboot.❑ Download and install PAN-OS 8.1.0 and, as a best practice, reboot.❑ Download and install the latest PAN-OS 8.1 maintenance release and reboot. <p>Proceed to Upgrade the Firewall to PAN-OS 9.0.</p>
7.0.x	<ul style="list-style-type: none">❑ Download and install the latest PAN-OS 7.0 maintenance release and reboot.❑ Download and install PAN-OS 7.1.0.❑ Download and install the latest PAN-OS 7.1 maintenance release and reboot.❑ Download and install PAN-OS 8.0.0 and, as a best practice, reboot.❑ Download and install the latest PAN-OS 8.0 maintenance release and reboot.❑ Download and install PAN-OS 8.1.0 and, as a best practice, reboot.❑ Download and install the latest PAN-OS 8.1 maintenance release and reboot. <p>Proceed to Upgrade the Firewall to PAN-OS 9.0.</p>
6.1.x	<ul style="list-style-type: none">❑ Download and install the latest 6.1 maintenance release and reboot.

Installed PAN-OS Version	Recommended Upgrade Path to PAN-OS 9.0
	<ul style="list-style-type: none"> ❑ Download and install PAN-OS 7.0.1 (7.0.1 is the base image for the 7.0 release, not 7.0.0). ❑ Download and install the latest PAN-OS 7.0 maintenance release and reboot. ❑ Download and install PAN-OS 7.1.0. ❑ Download and install the latest PAN-OS 7.1 maintenance release and reboot. ❑ Download and install PAN-OS 8.0.0 and, as a best practice, reboot. ❑ Download and install the latest PAN-OS 8.0 maintenance release and reboot. ❑ Download and install PAN-OS 8.1.0 and, as a best practice, reboot. ❑ Download and install the latest PAN-OS 8.1 maintenance release and reboot. <p>Proceed to Upgrade the Firewall to PAN-OS 9.0.</p>

Upgrade Firewalls Using Panorama

Review the [PAN-OS 9.0 Release Notes](#) and then use the following procedure to upgrade firewalls that you manage with Panorama. This procedure applies to standalone firewalls and firewalls deployed in a high availability (HA) configuration.



If Panorama is unable to connect directly to the update server, follow the procedure for [deploying updates to firewalls when Panorama is not internet-connected](#) so that you can manually download images to Panorama and then distribute the images to firewalls.

Before you can upgrade firewalls from Panorama, you must:

- ❑ Make sure Panorama is running the same or a later PAN-OS version than you are upgrading to. You must [upgrade Panorama](#) and its [Log Collectors](#) to 9.0 before upgrading the managed firewalls to this version. In addition, when upgrading Log Collectors to 9.0, you must upgrade all Log Collectors at the same time due to changes in the logging infrastructure.
- ❑ Plan for an extended maintenance window of up to six hours when upgrading Panorama to 9.0. This release includes significant infrastructure changes, which means that the Panorama upgrade will take longer than in previous releases.
- ❑ Ensure that firewalls are connected to a reliable power source. A loss of power during an upgrade can make a firewall unusable.

STEP 1 | After [upgrading Panorama](#), [commit and push](#) the configuration to the firewalls you are planning to upgrade.

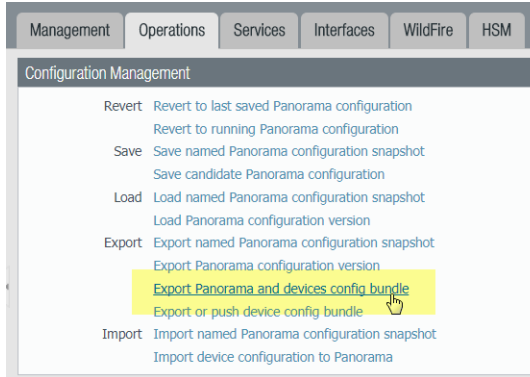
The PAN-OS 9.0 release introduces universally unique identifiers (UUIDs) for policy rules. If you manage firewall policy from Panorama, these UUIDs are generated on Panorama and therefore must be pushed from Panorama. If you do not push the configuration from Panorama prior to upgrading the firewalls, the firewall upgrade will not succeed because it will not have the UUIDs.

STEP 2 | Save a backup of the current configuration file on each managed firewall you plan to upgrade.



Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.

1. From the Panorama web interface, select **Panorama > Setup > Operations** and click **Export Panorama and devices config bundle** to generate and export the latest configuration backup of Panorama and of each managed appliance.



2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

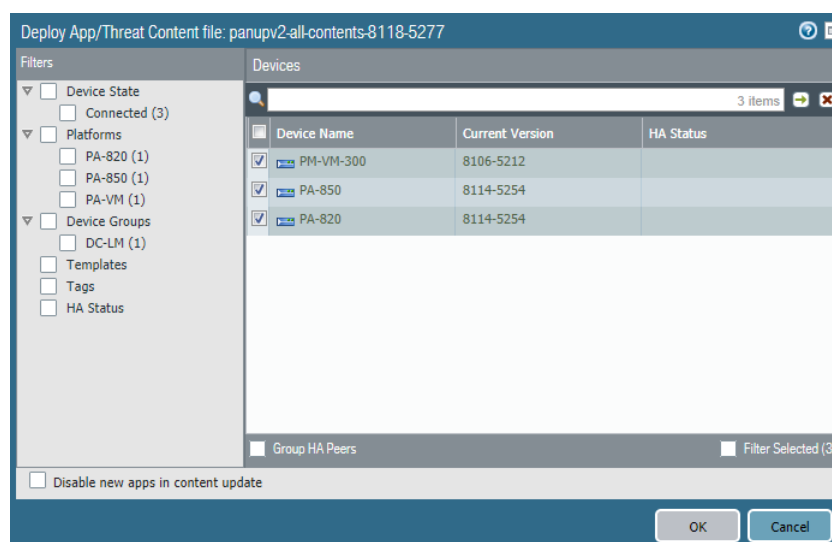
STEP 3 | Update the content release version on the firewalls you plan to upgrade.

Refer to the [Release Notes](#) for the minimum content release version required for PAN-OS 9.0. Make sure to follow the [Best Practices for Application and Threat Updates](#) when deploying content updates to Panorama and managed firewalls.

1. Select **Panorama > Device Deployment > Dynamic Updates** and **Check Now** for the latest updates. If an update is available, the Action column displays a **Download** link.

▼ Applications and Threats			Last checked: 2019/01/29 09:23:19 PST				
8118-5277	panupv2-all-contents-8118-5277	Contents	Full	44 MB	2019/01/28 18:16:51 PST	Download	Release Notes
8118-5277	panupv2-all-apps-8118-5277	Apps	Full	37 MB	2019/01/28 18:16:39 PST	Download	Release Notes
8118-5276	panupv2-all-apps-8118-5276	Apps	Full	37 MB	2019/01/28 13:41:15 PST	Download	Release Notes
8118-5276	panupv2-all-contents-8118-5276	Contents	Full	44 MB	2019/01/28 13:41:09 PST	Download	Release Notes
8118-5275	panupv2-all-apps-8118-5275	Apps	Full	37 MB	2019/01/27 04:21:20 PST	Download	Release Notes
8118-5275	panupv2-all-contents-8118-5275	Contents	Full	44 MB	2019/01/27 04:21:12 PST	Download	Release Notes
8118-5274	panupv2-all-apps-8118-5274	Apps	Full	37 MB	2019/01/25 20:31:16 PST	Download	Release Notes
8118-5274	panupv2-all-contents-8118-5274	Contents	Full	44 MB	2019/01/25 20:31:10 PST	Download	Release Notes
8117-5272	panupv2-all-contents-8117-5272	Contents	Full	44 MB	2019/01/25 09:56:36 PST	Download	Release Notes
8117-5272	panupv2-all-apps-8117-5272	Apps	Full	37 MB	2019/01/25 09:56:30 PST	Download	Release Notes

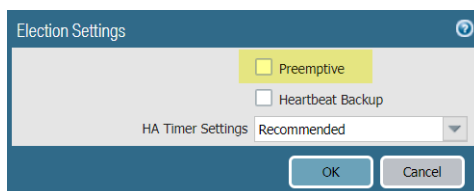
2. If not already installed, **Download** the latest content release version.
3. Click **Install**, select the firewalls on which you want to install the update, and click **OK**. If you are upgrading HA firewalls, you must update content on both peers.



By default, you can upload a maximum of two software or content updates of each type to a Panorama appliance and if you download a third update of the same type, Panorama will delete the update for the earliest version of that type. If you need to upload more than two software updates or content updates of a single type, use the `setmax-num-images count <number>` CLI command to increase the maximum.

STEP 4 | (HA firewall upgrades only) If you will be upgrading firewalls that are part of an HA pair, disable preemption. You need only disable this setting on one firewall in each HA pair.

1. Select **Device > High Availability** and edit the **Election Settings**.
2. If enabled, disable (clear) the **Preemptive** setting and click **OK**.



3. **Commit** your change. Make sure the commit is successful before you proceed with the upgrade.

STEP 5 | Determine the Upgrade Path to PAN-OS 9.0

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 9.0.0. Review the known issues and changes to default behavior in the [Release Notes](#) and upgrade/downgrade considerations in the [New Features Guide](#) for each release through which you pass as part of your upgrade path.



If upgrading more than one firewall, streamline the process by determining upgrade paths for all firewalls before you start downloading images.

STEP 6 | Download the target PAN-OS 9.0 release image.

1. Select **Panorama > Device Deployment > Software** and **Check Now** for the latest release versions.
2. **Download** the firewall-specific file (or files) for the release version to which you are upgrading. You must download a separate installation file for each firewall model (or firewall series) that you intend to upgrade.

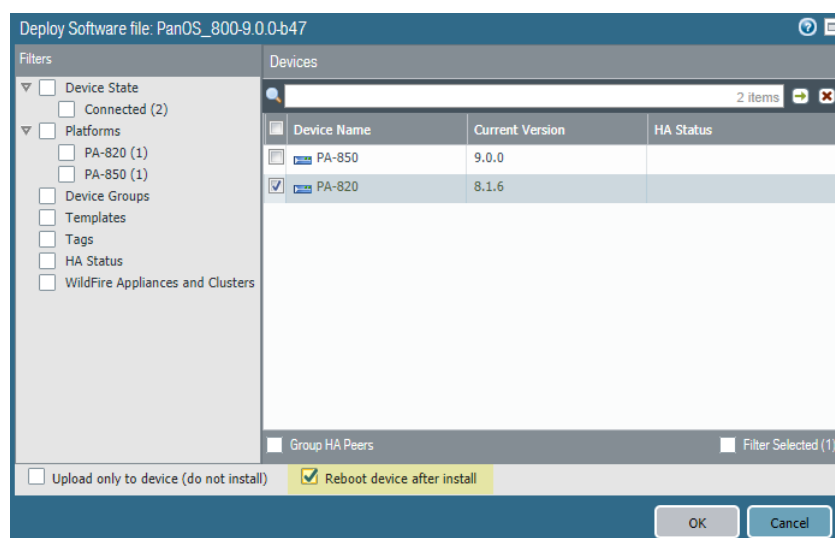
Version	File Name	Platform	Size	Release Date	Available	Action	
9.0.0	PanOS_7000-9.0.0	7000	2556 MB	2019/01/28 16:57:54		Download	Release Notes
9.0.0	PanOS_7000-9.0.0	7000	1840 MB	2019/01/28 16:55:01		Download	Release Notes
9.0.0	WildFire_m-9.0.0	m	1517 MB	2019/01/28 16:54:18		Download	Release Notes
9.0.0	PanOS_5200-9.0.0	5200	1375 MB	2019/01/28 16:51:31		Download	Release Notes
9.0.0	PanOS_3200-9.0.0	3200	1287 MB	2019/01/28 16:49:19		Download	Release Notes
9.0.0	Panorama_m-9.0.0	m	936 MB	2019/01/28 16:47:35		Download	Release Notes
9.0.0	PanOS_3000-9.0.0	3000	941 MB	2019/01/28 16:47:18		Download	Release Notes
9.0.0	Panorama_pc-9.0.0	pc	874 MB	2019/01/28 16:46:46		Download	Release Notes
9.0.0	PanOS_vm-9.0.0	vm	759 MB	2019/01/28 16:44:56		Download	Release Notes
9.0.0	PanOS_220-9.0.0	220	472 MB	2019/01/28 16:42:56		Download	Release Notes
9.0.0	PanOS_800-9.0.0	800	479 MB	2019/01/28 16:42:43		Download	Release Notes

For example, to upgrade your PA-220, PA-820, and VM-300 firewalls to PAN-OS 9.0.0, download the PanOS_220-9.0.0, PanOS_vm-9.0.0, and PanOS_800-9.0.0 images. After you successfully download an image, the Action column changes to **Install** for that image.

Version	File Name	Platform	Size	Release Date	Available	Action	
9.0.0	PanOS_7000-9.0.0	7000	2556 MB	2019/01/28 16:57:54		Download	Release Notes
9.0.0	PanOS_7000-9.0.0	7000	1840 MB	2019/01/28 16:55:01		Download	Release Notes
9.0.0	WildFire_m-9.0.0	m	1517 MB	2019/01/28 16:54:18		Download	Release Notes
9.0.0	PanOS_5200-9.0.0	5200	1375 MB	2019/01/28 16:51:31		Download	Release Notes
9.0.0	PanOS_3200-9.0.0	3200	1287 MB	2019/01/28 16:49:19		Download	Release Notes
9.0.0	Panorama_m-9.0.0	m	936 MB	2019/01/28 16:47:35		Download	Release Notes
9.0.0	PanOS_3000-9.0.0	3000	941 MB	2019/01/28 16:47:18		Download	Release Notes
9.0.0	Panorama_pc-9.0.0	pc	874 MB	2019/01/28 16:46:46		Download	Release Notes
9.0.0	PanOS_vm-9.0.0	vm	759 MB	2019/01/28 16:44:56	Downloaded	Install	Release Notes
9.0.0	PanOS_220-9.0.0	220	472 MB	2019/01/28 16:42:56	Downloaded	Install	Release Notes
9.0.0	PanOS_800-9.0.0	800	479 MB	2019/01/28 16:42:43	Downloaded	Install	Release Notes

STEP 7 | Install the PAN-OS 9.0 software update on the firewalls.

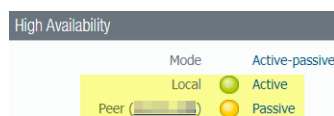
1. Click **Install** in the Action column that corresponds to the firewall models you want to upgrade. For example, if you want to upgrade your PA-820 firewalls, click **Install** in the row that corresponds to PanOS_800-9.0.0.
2. In the Deploy Software file dialog, select all firewalls that you want to upgrade. To reduce downtime, select only one peer in each HA pair. For active/passive pairs, select the passive peer; for active/active pairs, select the active-secondary peer.
3. (HA firewall upgrades only) Make sure **Group HA Peers** is not selected.
4. Select **Reboot device after install**.
5. To begin the upgrade, click **OK**.



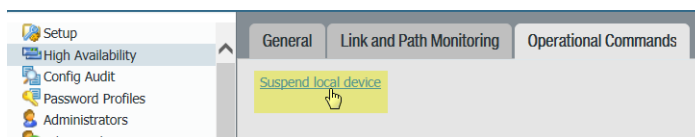
6. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, select **Device > Setup > Operations** and **Reboot Device**.
7. After the firewalls finish rebooting, select **Panorama > Managed Devices** and verify the Software Version is 9.0.0 for the firewalls you upgraded. Also verify that the HA status of any passive firewalls you upgraded is still passive.

STEP 8 | (HA firewall upgrades only) Upgrade the second HA peer in each HA pair.

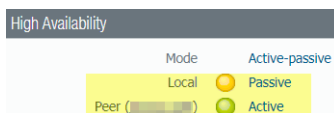
1. (Active/passive upgrades only) Suspend the active device in each active/passive pair you are upgrading.
 1. Switch context to the active firewall.
 2. In the High Availability widget on the **Dashboard**, verify that **Local** firewall state is **Active** and the **Peer** is **Passive**.



3. Select **Device > High Availability > Operational Commands > Suspend local device**.



4. Go back to the High Availability widget on the **Dashboard** and verify that **Local** changed to **Passive** and **Peer** changed to **Active**.



2. Go back to the Panorama context and select **Panorama > Device Deployment > Software**.
3. Click **Install** in the Action column that corresponds to the firewall models of the HA pairs you are upgrading.
4. In the Deploy Software file dialog, select all firewalls that you want to upgrade. This time, select only the peers of the HA firewalls you just upgraded.
5. Make sure **Group HA Peers** is not selected.

6. Select **Reboot device after install**.
7. To begin the upgrade, click **OK**.
8. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, select **Device > Setup > Operations and Reboot Device**.
9. (Active/passive upgrades only) From the CLI of the peer you just upgraded, run the following command to make the firewall functional again:


```
request high-availability state functional
```








STEP 9 | Verify the software and content release version running on each managed firewall.

1. On Panorama, select **Panorama > Managed Devices**.
2. Locate the firewalls and review the content and software versions in the table.

For HA firewalls, you can also verify that the HA Status of each peer is as expected.



If your HA firewalls have local policy rules configured, upon upgrade to PAN-OS 9.0, each peer independently assigns UUIDs for each rule. Because of this, the peers will show as out of sync until you either sync the configuration or perform a commit on the active peer.

	Device Name	Model	Operational Mode	IP Address	Status			Software Version	Apps and Threat
<input type="checkbox"/>					Device State	HA Status	Certificate		
▼ Alviso_Corp (5/5 Devices Connected): Shared > test-parent > Alviso_Corp									
<input type="checkbox"/>	vmPAN-Branch3	PA-VM	normal		Connected	 Active	pre-defined	9.0.0	8118-5277
<input type="checkbox"/>	vmPAN-Branch1	PA-VM	normal		Connected		pre-defined	8.1.0	8116-5267
<input type="checkbox"/>	vmPAN-Branch5	PA-VM	normal		Connected		pre-defined	8.0.7	8116-5258
<input type="checkbox"/>	vmPAN-Branch2	PA-VM	normal		Connected	 Passive	pre-defined	9.0.0	8118-5277
<input type="checkbox"/>	vmPAN-Branch4	PA-VM	normal		Connected		pre-defined	8.0.4	8116-5258

STEP 10 | (HA firewall upgrades only) If you disabled preemption on one of your HA firewalls before you upgraded, then edit the **Election Settings (Device > High Availability)** and re-enable the **Preemptive** setting for that firewall and then **Commit** the change.

Upgrade a Standalone Firewall to PAN-OS 9.0

Review the [PAN-OS 9.0 Release Notes](#) and then use the following procedure to upgrade a firewall that is not in an HA configuration to PAN-OS 9.0.



If your firewalls are configured to forward samples to a WildFire appliance for analysis, you must [upgrade the WildFire appliance](#) before upgrading the forwarding firewalls.



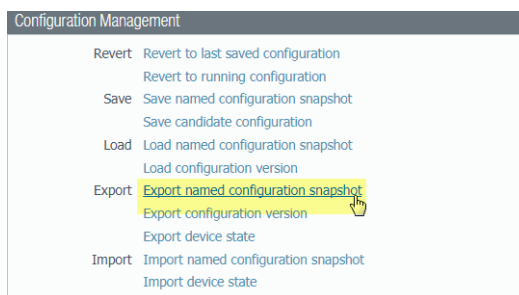
To avoid impacting traffic, plan to upgrade within the outage window. Ensure the firewall is connected to a reliable power source. A loss of power during an upgrade can make the firewall unusable.

STEP 1 | Save a backup of the current configuration file.

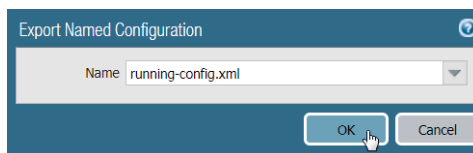


Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.

1. Select **Device > Setup > Operations** and click **Export named configuration snapshot**.



2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.



3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

STEP 2 | If you have enabled User-ID, after you upgrade, the firewall clears the current IP address-to-username and group mappings so that they can be repopulated with the attributes from the User-ID sources. To estimate the time required for your environment to repopulate the mappings, run the following CLI commands on the firewall.

- For IP address-to-username mappings:
 - **showuser user-id-agent state all**
 - **show user server-monitor state all**
- For group mappings: **show user group-mapping statistics**

STEP 3 | Ensure that the firewall is running the latest content release version.

Refer to the [Release Notes](#) for the minimum content release version you must install for a PAN-OS 9.0 release. Make sure to follow the [Best Practices for Application and Threat Updates](#).

1. Select **Device > Dynamic Updates** and see which **Applications** or **Applications and Threats** content release version is Currently Installed.

Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Documentation
▼ Applications and Threats Last checked: 2019/01/29 11:51:59 PST Schedule: Every hour at 5 minutes past the hour (Download and Install)									
8110-5233	panupv2-all-contents-8110-5233	Apps, Threats	Full	44 MB	2019/01/03 13:19:25 PST			Download	Release Notes
8111-5239	panupv2-all-contents-8111-5239	Apps, Threats	Full	44 MB	2019/01/08 09:45:01 PST			Download	Release Notes
8112-5247	panupv2-all-contents-8112-5247	Apps, Threats	Full	44 MB	2019/01/11 14:10:28 PST			Download	Release Notes
8113-5252	panupv2-all-contents-8113-5252	Apps, Threats	Full	44 MB	2019/01/15 16:20:35 PST			Download	Release Notes
8114-5254	panupv2-all-contents-8114-5254	Apps, Threats	Full	44 MB	2019/01/16 15:14:11 PST			Download	Release Notes
8115-5256	panupv2-all-contents-8115-5256	Apps, Threats	Full	44 MB	2019/01/17 17:16:41 PST			Download	Release Notes
8116-5267	panupv2-all-contents-8116-5267	Apps, Threats	Full	44 MB	2019/01/23 16:09:25 PST	✓ previously		Revert	Release Notes
8117-5272	panupv2-all-contents-8117-5272	Apps, Threats	Full	44 MB	2019/01/25 18:59:18 PST	✓	✓	Review Policies Review Apps	Release Notes

2. If the firewall is not running the minimum required content release version or a later version required for PAN-OS 9.0, **Check Now** to retrieve a list of available updates.
3. Locate and **Download** the desired content release version.
After you successfully download a content update file, the link in the Action column changes from **Download** to **Install** for that content release version.
4. **Install** the update.

STEP 4 | [Determine the Upgrade Path to PAN-OS 9.0](#)

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 9.0.0.



Review the known issues and changes to default behavior in the [Release Notes](#) and upgrade/downgrade considerations in the [New Features Guide](#) for each release through which you pass as part of your upgrade path.

STEP 5 | Upgrade to PAN-OS 9.0.



If your firewall does not have internet access from the management port, you can download the software image from the [Palo Alto Networks Customer Support Portal](#) and then manually Upload it to your firewall.

1. Select **Device > Software** and click **Check Now** to display the latest PAN-OS updates.
2. Locate and **Download PAN-OS 9.0.0**.
3. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.

Version	Size	Release Date	Available	Currently Installed	Action		
9.0.0	485 MB	2018/02/23 20:35:29	Uploaded		Install		
8.1.4	348 MB	2017/11/13 22:21:00	Uploaded	✓	Reinstall	Release Notes	
8.1.3	348 MB	2017/12/12 23:52:41			Download	Release Notes	
8.1.2	329 MB	2017/09/20 23:11:19			Download	Release Notes	
8.1.1	295 MB	2017/07/26 14:29:57			Download	Release Notes	
8.1.0	298 MB	2017/04/18 14:56:08			Download	Release Notes	

4. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, select **Device > Setup > Operations** and click **Reboot Device**.



At this point, the firewall clears the User-ID mappings, then connects to the User-ID sources to repopulate the mappings.

5. If you have enabled User-ID, use the following CLI commands to verify that the firewall has repopulated the IP address-to-username and group mappings before allowing traffic.
 - **show user ip-user-mapping all**
 - **show user group list**

STEP 6 | Verify that the firewall is passing traffic.

Select **Monitor > Session Browser** and verify that you are seeing new sessions.

	Start Time	From Zone	To Zone	Source	Destinati...	From Port	To Port	Proto...	Applicati...	Rule	Ingress I/F	Egress I/F	Bytes
+	02/02 12:04:27	T-Zone	T-Zone			4527	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	123216
+	02/05 15:06:39	T-Zone	T-Zone			18222	40822	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	1128202
+	02/05 15:27:01	T-Zone	T-Zone			61150	10495	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	145
+	01/31 20:10:22	T-Zone	T-Zone			49591	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	344421
+	02/05 15:24:11	T-Zone	T-Zone			31732	40356	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	148
+	02/05 10:09:58	T-Zone	T-Zone			62544	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	13761
+	02/05 15:12:53	T-Zone	T-Zone			56383	16937	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	145
+	01/30 11:27:10	T-Zone	T-Zone			4096	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	31846467
+	02/04 14:06:08	T-Zone	T-Zone			61253	80	6	web-browsing	Required Infrastructure	ethernet...	ethernet...	5042982
+	02/03 22:09:27	T-Zone	T-Zone			2385	80	6	facebook-base	Allowed Personal Apps	ethernet...	ethernet...	4949041
+	02/05 15:20:19	T-Zone	T-Zone			53111	26640	17	bittorrent	Allowed Personal Apps	ethernet...	ethernet...	109

Upgrade an HA Firewall Pair to PAN-OS 9.0

Review the [PAN-OS 9.0 Release Notes](#) and then use the following procedure to upgrade a pair of firewalls in a high availability (HA) configuration. This procedure applies to both active/passive and active/active configurations.

To avoid downtime when upgrading firewalls that are in a high availability (HA) configuration, update one HA peer at a time: For active/active firewalls, it doesn't matter which peer you upgrade first (though for simplicity, this procedure shows you how to upgrade the active-secondary peer first). For active/passive firewalls, you must upgrade the passive peer first, suspend the active peer (fail over), update the active peer, and then return that peer to a functional state (fail back). To prevent failover during the upgrade of the HA peers, you must make sure preemption is disabled before proceeding with the upgrade. You only need to disable preemption on one peer in the pair.



To avoid impacting traffic, plan to upgrade within the outage window. Ensure the firewalls are connected to a reliable power source. A loss of power during an upgrade can make firewalls unusable.

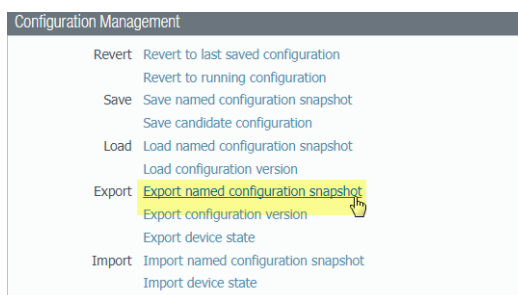
STEP 1 | Save a backup of the current configuration file.



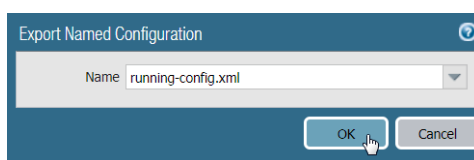
Although the firewall automatically creates a backup of the configuration, it is a best practice to create and externally store a backup before you upgrade.

Perform these steps on each firewall in the pair:

1. Select **Device > Setup > Operations** and click **Export named configuration snapshot**.



2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.



3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

STEP 2 | If you have enabled User-ID, after you upgrade, the firewall clears the current IP address-to-username and group mappings so that they can be repopulated with the attributes from the User-ID sources. To estimate the time required for your environment to repopulate the mappings, run the following CLI commands on the firewall.

- For IP address-to-username mappings:
 - `showuser user-id-agent state all`
 - `show user server-monitor state all`
- For group mappings: `show user group-mapping statistics`

STEP 3 | Ensure that each firewall in the HA pair is running the latest content release version.

Refer to the [release notes](#) for the minimum content release version you must install for a PAN-OS 9.0 release. Make sure to follow the [Best Practices for Application and Threat Updates](#).

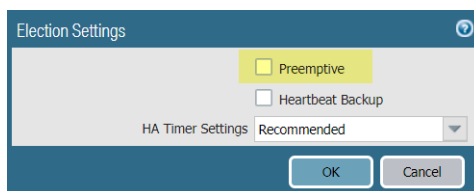
1. Select **Device > Dynamic Updates** and check which **Applications** or **Applications and Threats** to determine which update is Currently Installed.

Version ▲	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Documentation	
▼ Applications and Threats Last checked: 2019/01/29 11:51:59 PST Schedule: Every hour at 5 minutes past the hour (Download and Install)										
8110-5233	panupv2-all-contents-8110-5233	Apps, Threats	Full	44 MB	2019/01/03 13:19:25 PST			Download	Release Notes	
8111-5239	panupv2-all-contents-8111-5239	Apps, Threats	Full	44 MB	2019/01/08 09:45:01 PST			Download	Release Notes	
8112-5247	panupv2-all-contents-8112-5247	Apps, Threats	Full	44 MB	2019/01/11 14:10:28 PST			Download	Release Notes	
8113-5252	panupv2-all-contents-8113-5252	Apps, Threats	Full	44 MB	2019/01/15 16:20:35 PST			Download	Release Notes	
8114-5254	panupv2-all-contents-8114-5254	Apps, Threats	Full	44 MB	2019/01/16 15:14:11 PST			Download	Release Notes	
8115-5256	panupv2-all-contents-8115-5256	Apps, Threats	Full	44 MB	2019/01/17 17:16:41 PST			Download	Release Notes	
8116-5267	panupv2-all-contents-8116-5267	Apps, Threats	Full	44 MB	2019/01/23 16:09:25 PST	✓ previously		Revert	Release Notes	ⓧ
8117-5272	panupv2-all-contents-8117-5272	Apps, Threats	Full	44 MB	2019/01/25 18:59:18 PST	✓	✓	Review Policies Review Apps	Release Notes	ⓧ

2. If the firewalls are not running the minimum required content release version or a later version required for PAN-OS 9.0, **Check Now** to retrieve a list of available updates.
3. Locate and **Download** the desired content release version.
After you successfully download a content update file, the link in the Action column changes from **Download** to **Install** for that content release version.
4. **Install** the update. You must install the update on both peers.

STEP 4 | Disable preemption on the first peer in each pair. You only need to disable this setting on one firewall in the HA pair but ensure that the commit is successful before you proceed with the upgrade.

1. Select **Device > High Availability** and edit the **Election Settings**.
2. If enabled, disable (clear) the **Preemptive** setting and click **OK**.



3. **Commit** the change.

STEP 5 | Determine the Upgrade Path to PAN-OS 9.0

You cannot skip installation of any feature release versions in the path from the currently running PAN-OS version to PAN-OS 9.0.0.



Review the known issues and changes to default behavior in the [Release Notes](#) and upgrade/downgrade considerations in the [New Features Guide](#) for each release through which you pass as part of your upgrade path.

STEP 6 | Install PAN-OS 9.0 on the first peer.

To minimize downtime in an active/passive configuration, upgrade the passive peer first. For an active/active configuration, upgrade the secondary peer first. As a best practice, if you are using an active/active configuration, we recommend upgrading both peers during the same maintenance window.



If you want to test that HA is functioning properly before the upgrade, consider upgrading the active peer in an active/passive configuration first to ensure that failover occurs without incident.

1. On the first peer, select **Device > Software** and click **Check Now** for the latest updates.
2. Locate and **Download** PAN-OS 9.0.0.

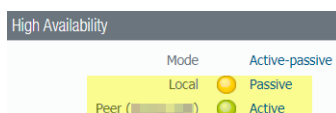


If your firewall does not have internet access from the management port, you can download the software image from the [Palo Alto Networks Support Portal](#) and then manually Upload it to your firewall.

3. After you download the image (or, for a manual upgrade, after you upload the image), **Install** the image.

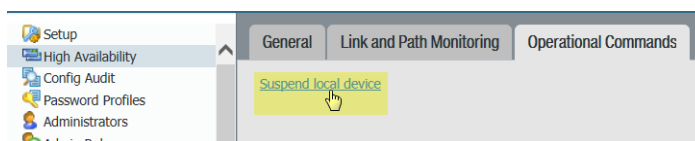
Version	Size	Release Date	Available	Currently Installed	Action		
9.0.0	485 MB	2018/02/23 20:35:29	Uploaded		Install		
8.1.4	348 MB	2017/11/13 22:21:00	Uploaded	✓	Reinstall	Release Notes	
8.1.3	348 MB	2017/12/12 23:52:41			Download	Release Notes	
8.1.2	329 MB	2017/09/20 23:11:19			Download	Release Notes	
8.1.1	295 MB	2017/07/26 14:29:57			Download	Release Notes	
8.1.0	298 MB	2017/04/18 14:56:08			Download	Release Notes	

4. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, select **Device > Setup > Operations** and **Reboot Device**.
5. After the device finishes rebooting, view the High Availability widget on the **Dashboard** and verify that the device you just upgraded is still the passive or active-secondary peer in the HA configuration.



STEP 7 | Install PAN-OS 9.0 on the second peer.

1. (Active/passive configurations only) Suspend the active peer so that HA fails over to the peer you just upgraded.
 1. On the active peer, select **Device > High Availability > Operational Commands** and click **Suspend local device**.



2. View the High Availability widget on the **Dashboard** and verify that the state changes to **Passive**.
3. On the other peer, verify that it is active and is passing traffic (**Monitor** > **Session Browser**).
2. On the second peer, select **Device** > **Software** and click **Check Now** for the latest updates.
3. Locate and **Download** PAN-OS 9.0.0.
4. After you download the image, **Install** it.
5. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, select **Device** > **Setup** > **Operations** and **Reboot Device**.
6. (Active/passive configurations only) From the CLI of the peer you just upgraded, run the following command to make the firewall functional again:


```
request high-availability state functional
```



If your HA firewalls have local policy rules configured, upon upgrade to PAN-OS 9.0, each peer independently assigns UUIDs for each rule. Because of this, the peers will show as out of sync until you either sync the configuration or perform a commit on the active peer.

STEP 8 | Verify that both peers are passing traffic as expected.

In an active/passive configuration, only the active peer should be passing traffic; both peers should be passing traffic in an active/active configuration.

Run the following CLI commands to confirm that the upgrade succeeded:

- (Active peers only) To verify that active peers are passing traffic, run the `show session all` command.
- To verify session synchronization, run the `show high-availability interface ha2` command and make sure that the Hardware Interface counters on the CPU table are increasing as follows:
 - In an active/passive configuration, only the active peer shows packets transmitted; the passive peer will show only packets received.



If you enabled HA2 keep-alive, the hardware interface counters on the passive peer will show both transmit and receive packets. This occurs because HA2 keep-alive is bi-directional, which means that both peers transmit HA2 keep-alive packets.

- In an active/active configuration, you will see packets received and packets transmitted on both peers.

STEP 9 | If you disabled preemption prior to the upgrade, re-enable it now.

1. Select **Device** > **High Availability** and edit the **Election Settings**.
2. Select **Preemptive** and click **OK**.
3. **Commit** the change.

Downgrade from PAN-OS 9.0

The way you downgrade a firewall from PAN-OS 9.0 depends on whether you are downgrading to a previous feature release (where the first or second digit in the PAN-OS version changes, for example, from 8.1.2 to 8.0.13 or from 8.0.6 to 7.1.9) or downgrading to a maintenance release version within the same feature release (where the third digit in the release version changes, for example, from 8.1.2 to 8.1.0). When you downgrade from one feature release to an earlier feature release, you can migrate the configuration from the later release to accommodate new features. To migrate the PAN-OS 9.0 configuration to an earlier PAN-OS release, first restore the configuration for the feature release to which you are downgrading. You do not need to restore the configuration when you downgrade from one maintenance release to another within the same feature release.

- [Downgrade a Firewall to a Previous Maintenance Release](#)
- [Downgrade a Firewall to a Previous Feature Release](#)
- [Downgrade a Windows Agent from PAN-OS 9.0](#)



Always downgrade into a configuration that matches the software version. Unmatched software versions and configurations can result in failed downgrades or force the system into maintenance mode. This only applies to a downgrade from one feature release to another (for example 9.0.0 to 8.1.3), not to downgrades to maintenance releases within the same feature release version (for example, 8.1.3 to 8.1.1).

If you have a problem with a downgrade, you may need to enter maintenance mode and reset the device to factory default and then restore the configuration from the original config file that was exported prior to the upgrade.

Downgrade a Firewall to a Previous Feature Release

Use the following workflow to restore the configuration that was running before you upgraded to a different feature release. Any changes made since the upgrade are lost. Therefore, it is important to back up your current configuration so you can restore those changes when you return to the newer feature release.

Use the following procedure to downgrade to a previous feature release.

STEP 1 | Save a backup of the current configuration file.



Although the firewall automatically creates a backup of the configuration, it is a best practice to create a backup before you upgrade and store it externally.

1. **Export named configuration snapshot (Device > Setup > Operations).**
2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.
3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the downgrade.

STEP 2 | Install the previous feature release image.



Autosave versions are created when you upgrade to a new release.

1. **Check Now (Device > Software)** for available images.
2. Locate the image to which you want to downgrade. If the image is not already downloaded, then **Download** it.

3. After the download completes, **Install** the image.
4. **Select a Config File for Downgrading**, which the firewall will load after you reboot the device. In most cases, you should select the configuration that was saved automatically when you upgraded from the release to which you are now downgrading. For example, if you are running PAN-OS 9.0 and are downgrading to PAN-OS 8.1.3, select `autosave-8.1.3`.
5. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**.

Downgrade a Firewall to a Previous Maintenance Release

Because maintenance releases do not introduce new features, you can downgrade to a previous maintenance release in the same feature release without having to restore the previous configuration. A maintenance release is a release in which the third digit in the release version changes, for example a downgrade from 8.1.6 to 8.1.4 is considered a maintenance release downgrade because only the third digit in the release version is different.

Use the following procedure to downgrade to a previous maintenance release within the same feature release.

STEP 1 | Save a backup of the current configuration file.



Although the firewall automatically creates a backup of the configuration, it is a best practice to create a backup before you downgrade and store it externally.

1. **Export named configuration snapshot (Device > Setup > Operations)**.
2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.
3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the downgrade.

STEP 2 | Install the previous maintenance release image.



If your firewall does not have internet access from the management port, you can download the software update from the [Palo Alto Networks Support Portal](#). You can then manually Upload it to your firewall.

1. **Check Now (Device > Software)** for available images.
2. Locate the version to which you want to downgrade. If the image is not already downloaded, then **Download** it.
3. After the download completes, **Install** the image.
4. After the installation completes successfully, reboot using one of the following methods:
 - If you are prompted to reboot, click **Yes**.
 - If you are not prompted to reboot, go to Device Operations (**Device > Setup > Operations**) and **Reboot Device**.

Downgrade a Windows Agent from PAN-OS 9.0

After you uninstall the PAN-OS 9.0 Windows-based User-ID agent, perform the following steps before you install an earlier agent release.

STEP 1 | Open the Windows Start menu and select **Administrative Tools**.

STEP 2 | Select **Computer Management > Services and Applications > Services** and double-click **User-ID Agent**.

STEP 3 | Select **Log On**, select **This account**, and specify the username for the User-ID agent account.

STEP 4 | Enter the **Password** and **Confirm Password**.

STEP 5 | Click **OK** to save your changes.

App-ID Features

- > Policy Optimizer
- > HTTP/2 Inspection
- > Strict Default Ports for Decrypted Applications

Policy Optimizer

You now have a simple way to gain visibility into, control usage of, and safely enable applications in Security policy rules: [Policy Optimizer](#). This new feature identifies port-based rules so you can convert them to application-based whitelist rules without compromising application availability. It also identifies rules configured with unused applications. **Policy Optimizer** information helps you analyze rule characteristics and prioritize which rules to migrate or clean up first.

Converting port-based rules to application-based rules enables you to whitelist the applications you want to allow and deny access to all other applications, which improves your security posture. Restricting application traffic to its default ports prevents evasive applications from running on non-standard ports. Removing unused applications from rules is a best practice that reduces the attack surface and keeps the rulebase clean.

You can use this new feature on:

- Firewalls that run PAN-OS version 9.0 and have App-ID enabled.
- Panorama running PAN-OS version 9.0. You don't have to upgrade firewalls that Panorama manages to use the **Policy Optimizer** capabilities. However, to use the **Rule Usage** capabilities, managed firewalls must run PAN-OS 8.1 or later. If managed firewalls connect to Log Collectors, those Log Collectors must also run PAN-OS version 9.0.

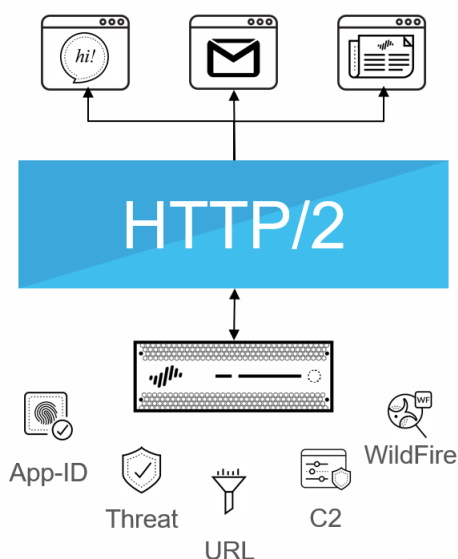


Due to resource constraints, VM-50 Lite virtual firewalls don't support the Policy Optimizer.

- [Policy Optimizer Concepts](#)
- [Migrate Port-Based to App-ID Based Security Policy Rules](#)
- [Identify Security Policy Rules with Unused Applications](#)

HTTP/2 Inspection

You can now safely enable applications running over HTTP/2, without any additional configuration on the firewall. As more websites continue to adopt HTTP/2, the firewall can enforce security policy and all threat detection and prevention capabilities on a stream-by-stream basis. This visibility into HTTP/2 traffic enables you to secure web servers that provide services over HTTP/2, and allow your users to benefit from the speed and resource efficiency gains that HTTP/2 provides.



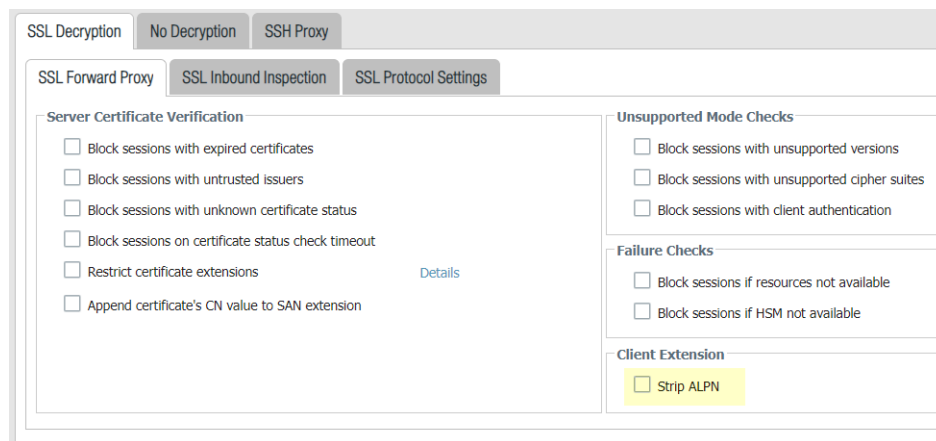
The firewall processes and inspects HTTP/2 traffic by default when [SSL decryption](#) is enabled. All firewall platforms support HTTP/2 inspection. Except for PA-3000 Series firewalls, HTTP/2 inspection includes support for the HTTP/2 server push feature, where a server can send multiple resources in response to a single client request, instead of requiring the client to explicitly request each resource.

For HTTP/2 inspection to work correctly, the firewall must be enabled to use ECDHE (elliptic curve Diffie-Hellman) as a key exchange algorithm for SSL sessions. ECDHE is enabled by default, but you can check to confirm that it's enabled by selecting **Objects > Decryption > Decryption Profile > SSL Decryption > SSL Protocol Settings**.

You can disable HTTP/2 inspection for targeted traffic, or globally:

- Disable HTTP/2 inspection for targeted traffic.

You'll need to specify for the firewall to remove any value contained in the Application-Layer Protocol Negotiation (ALPN) TLS extension. ALPN is used to secure HTTP/2 connections—when there is no value specified for this TLS extension, the firewall either downgrades HTTP/2 traffic to HTTP/1.1 or classifies it as unknown TCP traffic.



1. Select **Objects > Decryption > Decryption Profile > SSL Decryption > SSL Forward Proxy** and then select **Strip ALPN**.
2. Attach the decryption profile to a decryption policy (**Policies > Decryption**) to turn off HTTP/2 inspection for traffic that matches the policy.
3. **Commit** your changes.

- Disable HTTP/2 inspection globally.

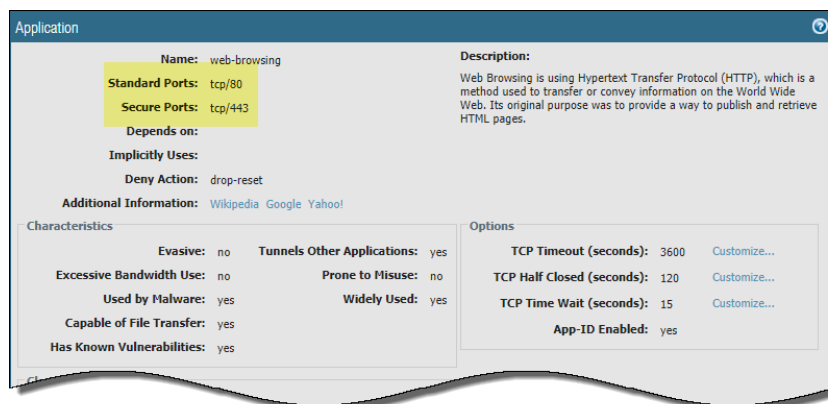
Use the CLI command: `set deviceconfig setting http2 enable no` and **Commit** your changes. The firewall will classify HTTP/2 traffic as unknown TCP traffic.

Strict Default Ports for Decrypted Applications

[Application-default](#) gives you a way to safely enable applications on their most commonly-used ports. It allows you to write simple, application-based policy rules based on your business needs, while preventing attacks that attempt to bypass traditional port-based policies.

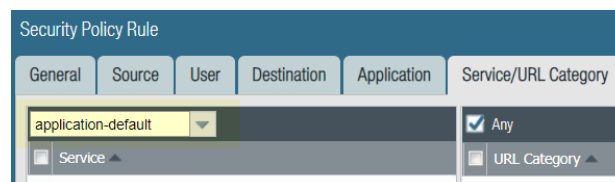
Now, because certain applications use a different default port when they are encrypted, application-default differentiates between cleartext and encrypted application traffic when SSL decryption is turned on. For the applications that require it, like web-browsing, application-default enforces the application on both the standard port—the port the cleartext application uses—and the secure port—the port the encrypted application uses.

In the case of web-browsing, for example, this means that application-default now strictly enforces cleartext web-browsing traffic only on port 80 and SSL-tunneled web-browsing traffic only on port 443. Application-default for encrypted applications works by default and is supported for web-browsing, SMTP, FTP, LDAP, POP3 and IMAP traffic. For these applications, you can visit [Applopedia](#) or select **Objects > Applications** to view applications details, which include the secure port it uses when encrypted.



Application-default is a best practice for application-based security policies and SSL decryption:

- ❑ If you're [decrypting SSL traffic](#), use application-default in your security policy rules. As the firewall decrypts SSL traffic, and identifies the tunneled applications as web-browsing, SMTP, FTP, POP3, LDAP, or IMAP, application-default specifies for it to enforce those applications on the secure port.
- ❑ We recommend that you update [security policy rules](#) that control web-browsing. Security policy rules that are currently configured to enforce web-browsing traffic on service-http and service-https should be updated to instead allow web-browsing only on the **application-default** ports (**Policies > Security > Service/URL Category**).



Virtualization Features

- > VM-Series Firewall on AWS—Support for C5 and M5 Instance Types with ENA
- > VM-Series Plugin
- > Support for HA for VM-Series on Azure
- > Higher Performance for VM-Series on Azure using Azure Accelerated Networking (SR-IOV)

VM-Series Firewall on AWS—Support for C5 and M5 Instance Types with ENA

You can now [deploy](#) the VM-Series firewall on [C5/M5](#) instance types with the [Enhanced Network Adapter](#) (ENA) and the Nitro hypervisor. The C5 and M5 instance types are supported in SR-IOV mode; DPDK is not supported.

VM-Series Plugin

The VM-Series firewall now supports the VM-Series plugin, a built-in plugin architecture for integration with public clouds or private cloud hypervisors. You can upgrade the VM-Series plugin independently of PAN-OS, enabling accelerated releases of new features, fixes, or new integrations with public clouds or private hypervisors.

The VM-Series plugin manages cloud-specific interactions between the VM-Series firewalls and public clouds such as [Google Cloud Platform](#), [Azure](#), [AWS](#), and private cloud hypervisors such as KVM, ESXi, and others. Some of the capabilities that the plugin enables include bootstrapping, configuring user credential provisioning information from public cloud environments, seamless updates for cloud libraries or agents on PAN-OS, and publishing custom metrics to cloud monitoring services such as AWS CloudWatch.

The VM-Series plugin is part of PAN-OS, which means that you can upgrade or downgrade the plugin but you cannot remove it. You configure the VM-Series plugin locally on the virtual firewall.

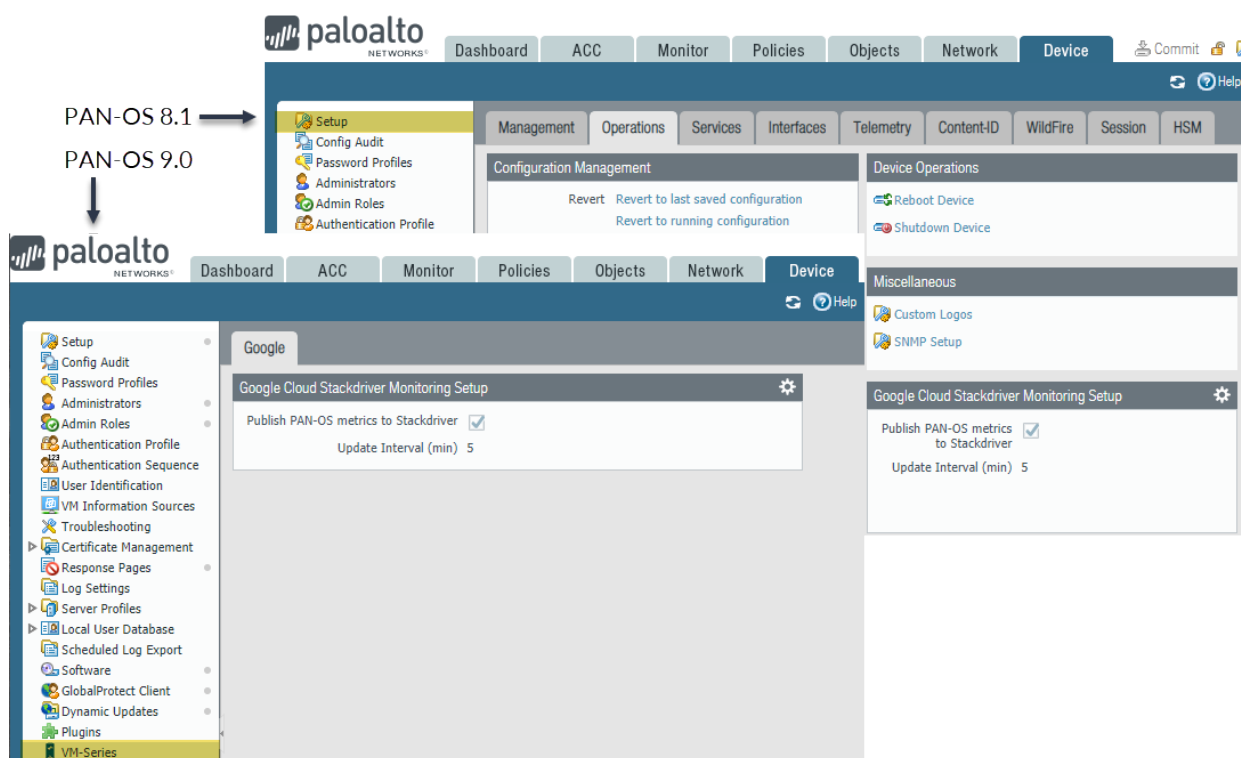
You can also manage the plugin configuration centrally from Panorama. The VM-Series plugin is optional on Panorama, but you can install it manually if you want to centrally configure plugins.

- [VM-Series Plugin on the VM-Series Firewall](#)
- [VM-Series Plugin on Panorama](#)
- [Plugin Upgrades](#)

VM-Series Plugin on the VM-Series Firewall

On the VM-Series firewall, the VM-Series plugin is automatically installed during a new VM-Series 9.0 installation or an upgrade from PAN-OS 8.1 to PAN-OS 9.0. You can view the VM-Series plugin version on the Dashboard, or from **Device > Plugins**.

In previous releases, you configured integrations for AWS CloudWatch or Google Stackdriver Monitoring from **Device > Setup > Operations**. Starting in version 9.0, you configure the integration from the **Device > VM-Series** node, as shown in the VM-Series firewall comparison below.



In the version 9.0 screenshot the VM-Series node is selected, and a tab displays the public cloud hosting the VM-Series firewall (Google), and the configuration settings for the plugin (Stackdriver Monitoring).

VM-Series Plugin on Panorama

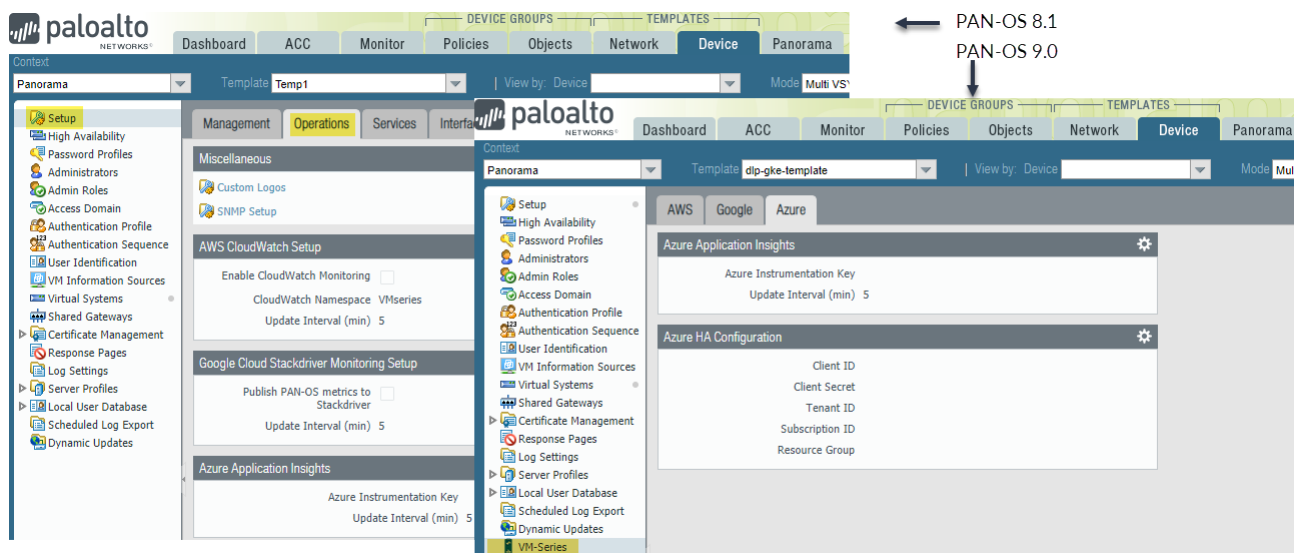
If you want Panorama to manage the VM-Series plugin on your managed firewalls, you can install the VM-Series plugin manually.

- If your Panorama 8.1 installation does not have any integrations configured when you upgrade to 9.0, the VM-Series plugin is not installed. You can manually install the plugin from **Panorama > Plugins**.
- If you have an existing plugin configuration, the VM-Series plugin is automatically installed. For example, if you configured AWS CloudWatch in 8.1.3, the 9.0 upgrade migrates your legacy integration to the VM-Series plugin.

You can view the versions for all plugins on the Panorama **Dashboard**.

In previous releases, you configured cloud integrations in Panorama from **Device > Setup > Operations**. If the VM-Series plugin is installed you can view all the cloud platform integrations from **Device > VM-Series**.

The following screenshot contrasts Panorama 8.1 and 9.0. In version 8.1 the **Operations** tab shows AWS, Google, and Azure configuration panes. In the version 9.0 upgrade, **Device > VM-Series** displays each cloud configuration on a separate tab.



Plugin Upgrades

Whenever a new VM-Series plugin releases, you must manually upgrade the VM-Series plugin independently of a PAN-OS or Panorama update.

Because the VM-Series plugin manages multiple cloud integrations, a new plugin version might not apply to public cloud integrations you are using. For example, if a VM-Series plugin update release contains fixes for AWS only, upgrade your VM-Series firewalls on AWS, but do not update the plugin on VM-Series firewalls in other clouds.



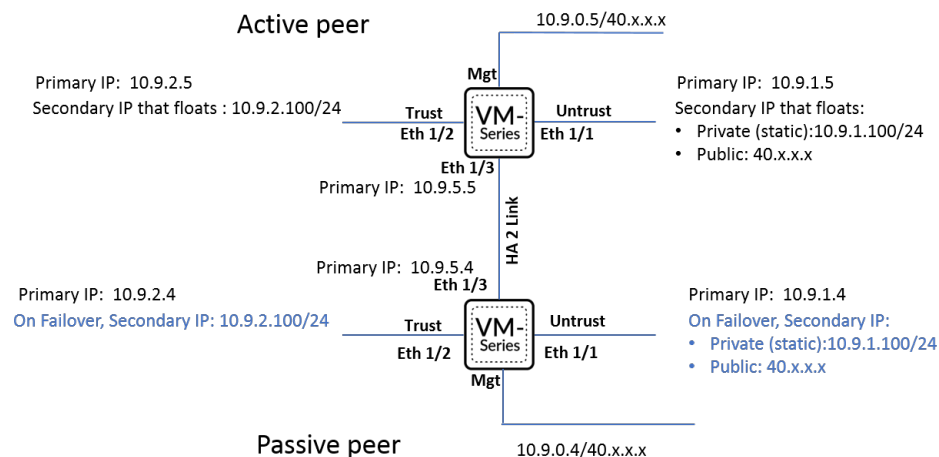
Refer to the release notes, and only install upgrades that are pertinent to your configuration.

For more about the VM-Series plugin, see [VM-Series Plugin](#) in the [VM-Series Deployment Guide](#).

Support for HA for VM-Series on Azure

With the [VM-Series Plugin](#), you can now configure the VM-Series firewalls on Azure in an [active/passive high availability \(HA\) configuration](#). For an HA configuration, both HA peers must belong to the same Azure Resource Group. You can deploy the first instance of the firewall from the Azure Marketplace, and then use your custom ARM template or the Palo Alto Networks [sample GitHub](#) template for deploying the second instance of the firewall into the existing Resource Group. The reason you need a custom template or the Palo Alto Networks sample template is because Azure does not support the ability to deploy the firewall in to an Resource Group that is not empty.

To ensure uptime in an HA setup on Azure, you need floating IP addresses that can quickly move from the active firewall to the passive firewall so that the passive firewall can seamlessly secure traffic as soon as it becomes the active peer and [HA links](#)—a control link (HA1) and a data link (HA2)—to synchronize data and maintain state information between the HA peers.



To support HA, you need to configure the interfaces on the VM-Series firewalls on Azure as follows:

Interface	Active firewall peer	Passive firewall peer	Description
Trust	Secondary IP address	—	<p>The trust interface of the active peer requires a secondary IP configuration that can float to the other peer on failover. This secondary IP configuration on the trust interface must be a private IP address with the netmask of the servers that it secures.</p> <p>On failover, the VM-Series plugin calls the Azure API to detach this secondary private IP address from the active peer and attach it to the passive peer. Attaching this IP address to the now active peer ensures that the firewall can receive traffic on the floating IP on the untrust interface and send it through to the floating IP on the trust interface and on to the workloads.</p>

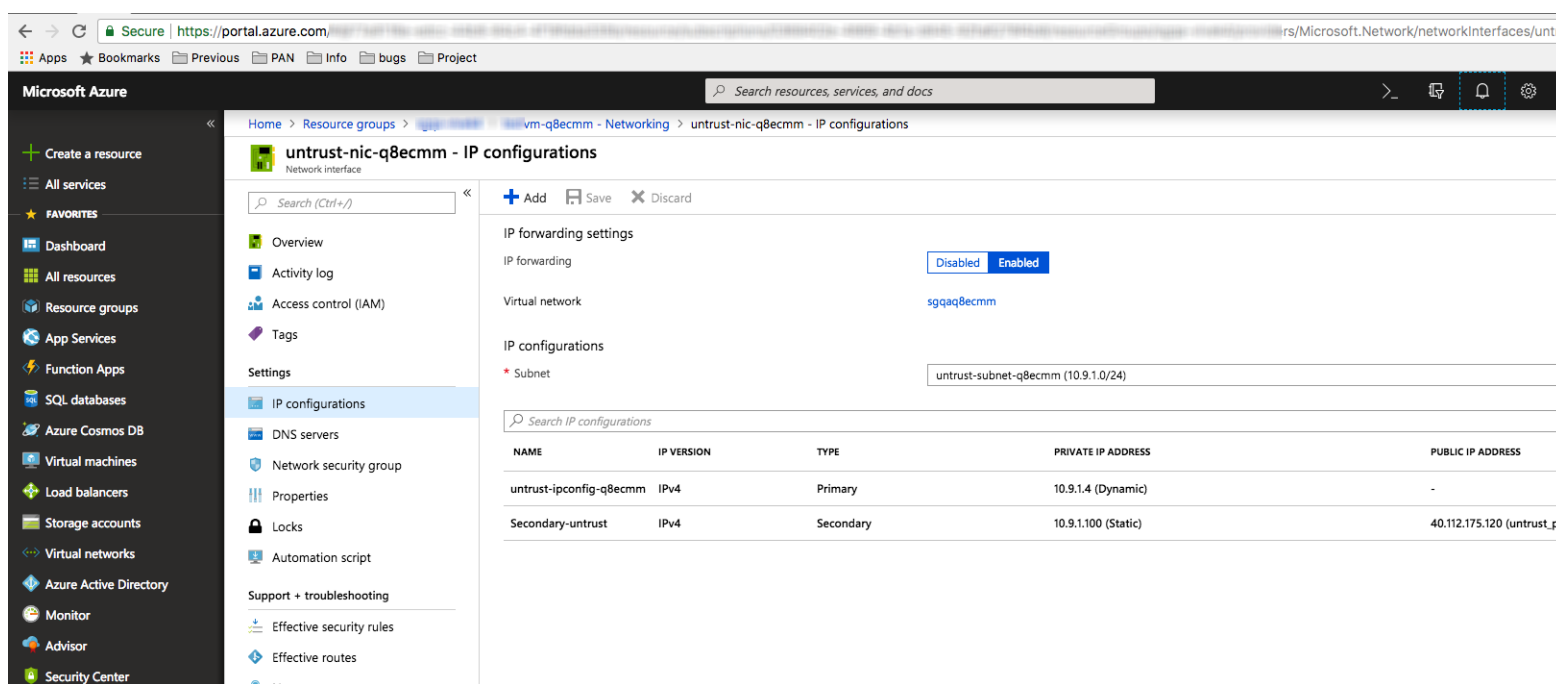
Interface	Active firewall peer	Passive firewall peer	Description
Untrust	Secondary IP address	—	<p>The untrust interface of the firewall requires a secondary IP configuration that includes a static private IP address with a netmask for the untrust subnet, and a public IP address for accessing the internet. Without this public IP address, you can access internal Azure resources through the untrust interface, but will be unable to access anything over the internet.</p> <p>On failover, the VM-Series plugin calls the Azure API to detach the secondary IP configuration from the active peer and attach it to the passive peer before it transitions to the active state. This process of floating the secondary IP configuration, enables the now active firewall to continue processing inbound traffic that is destined to the workloads.</p>
HA2	Add a NIC to the firewall from the Azure management console.	Add a NIC to the firewall from the Azure management console.	<p>On the active and passive peers, add a dedicated HA2 link to enable session synchronization.</p> <p>The default interface for HA1 is the management interface, and you can opt to use the management interface instead of adding an additional interface to the firewall. For enabling data flow over the HA2 link, you need to add an additional network interface on the Azure portal and configure the interface for HA2 on the firewall.</p>

STEP 1 | Deploy a VM-Series firewall.

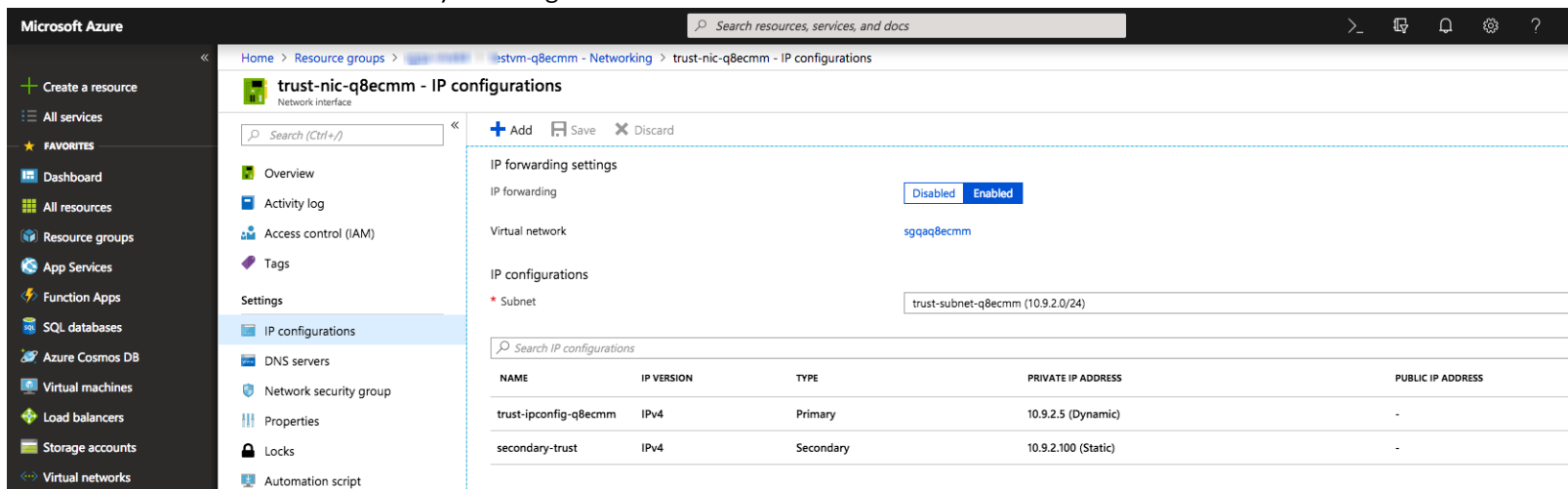
You can use the PAN-OS 9.0 Solution template on the Azure Marketplace to deploy the first instance of the firewall or upgrade an existing VM-Series firewall instance to PAN -OS 9.0. To complete the inputs for deploying the second instance of the firewall, you must note the following details about the first instance of the firewall—Azure subscription, name of the Resource Group, location of the Resource Group, name of the existing VNet, VNet CIDR, Subnet names associated with each interface on the first instance of the firewall, Subnet CIDRs, and start the IP address for the management, trust and untrust subnets.

STEP 2 | Set up the network interfaces for HA.

1. Add a secondary IP configuration to the untrust interface of the firewall.



2. Add a secondary IP configuration to the trust interface of the firewall.



The secondary IP configuration for the trust interface requires a static private IP address only. This IP address moves from the active firewall to the passive firewall on failover so that traffic flows through from the untrust to the trust interface and to the destination subnets that the firewall secures.

3. Attach a network interface for the HA2 communication between the firewall HA peers.

STEP 3 | Configure the interfaces on the firewall.

Complete these steps on the active HA peer, before you deploy and set up the passive HA peer.

1. Log in to the firewall web interface.
2. Configure ethernet 1/1 as the untrust interface and ethernet 1/2 as the untrust interface.

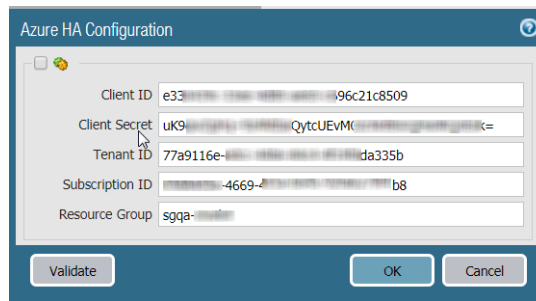
Select **Network > Interfaces** and configure as follows:

3. Configure ethernet 1/3 as the HA interface.

To set up the HA2 link, select the interface and set **Interface Type** to **HA**. Set link speed and duplex to auto.

STEP 4 | Configure the VM-Series plugin to authenticate to the Azure resource group in which you have deployed the firewall.

Select **Device > VM-Series** to enable programmatic access between the firewall plugin and the Azure resources.



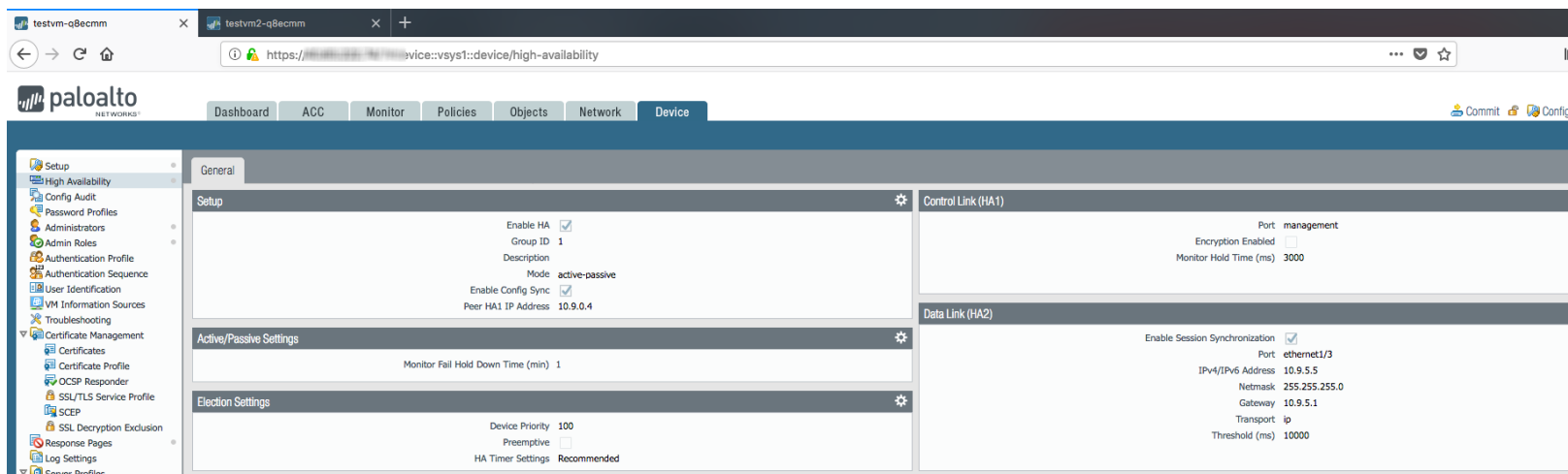
Azure HA Configuration dialog box with the following fields:

- Client ID: e33...96c21c8509
- Client Secret: uk9...QytcUEvM...
- Tenant ID: 77a9116e-...da335b
- Subscription ID: ...4669-...b8
- Resource Group: sgqa-...

Buttons: Validate, OK, Cancel

STEP 5 | Enable HA.

Select **Device** > **Setup** > **HA**.



Palo Alto Networks VM-Series Firewall HA Configuration interface. The left sidebar shows the navigation menu with 'Setup' > 'High Availability' selected. The main panel shows the 'General' tab with the following settings:

- Setup:**
 - Enable HA: ☒
 - Group ID: 1
 - Description:
 - Mode: active-passive
 - Enable Config Sync: ☒
 - Peer HA1 IP Address: 10.9.0.4
- Active/Passive Settings:**
 - Monitor Fail Hold Down Time (min): 1
- Election Settings:**
 - Device Priority: 100
 - Preemptive: ☐
 - HA Timer Settings: Recommended
- Control Link (HA1):**
 - Port: management
 - Encryption Enabled: ☐
 - Monitor Hold Time (ms): 3000
- Data Link (HA2):**
 - Enable Session Synchronization: ☒
 - Port: ethernet1/3
 - IPv4/IPv6 Address: 10.9.5.5
 - Netmask: 255.255.255.0
 - Gateway: 10.9.5.1
 - Transport: ip
 - Threshold (ms): 10000

1. Enter **Peer HA1 IP address** as the private IP address of the passive peer.
2. Edit the Data Link (HA2) to use **Port** ethernet 1/3 and add the IP address of this peer and the **Gateway** IP address for the subnet.

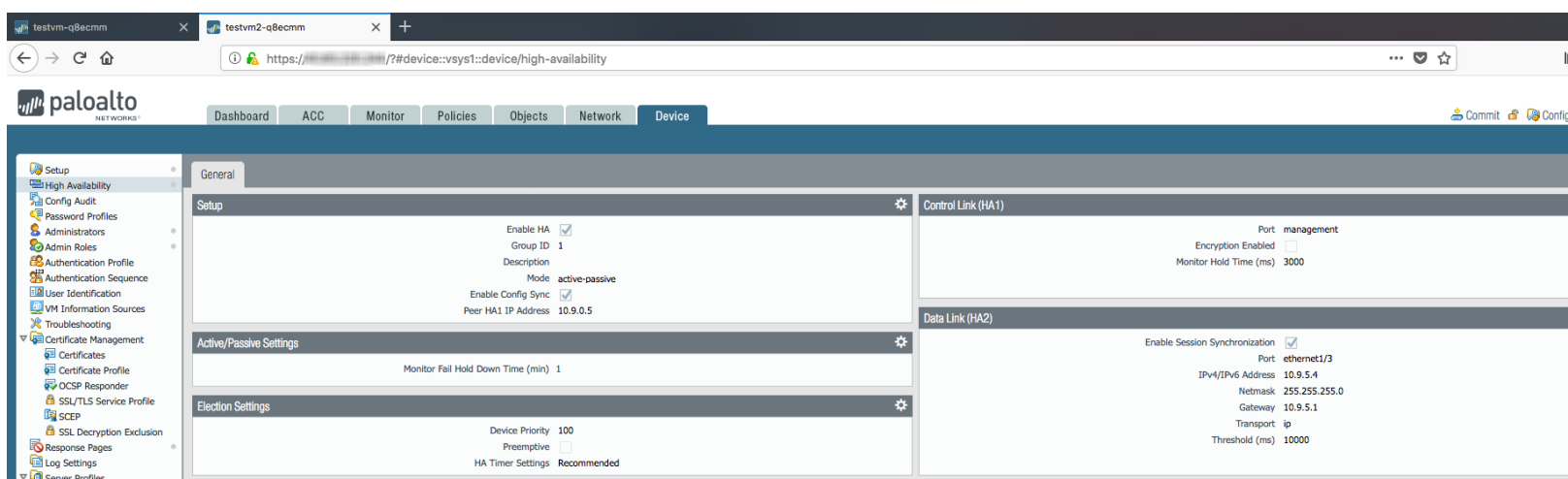
STEP 6 | Commit the changes.

STEP 7 | Deploy the VM-Series firewall HA peer.

For the HA peer, you can either use a custom template or the [sample GitHub](#) template that allows you to deploy the second instance of the firewall within the same Azure Resource Group. Make sure to deploy this HA peer within the subscription, Resource Group, VNet and the same subnet configurations as that of the first firewall instance you've deployed.

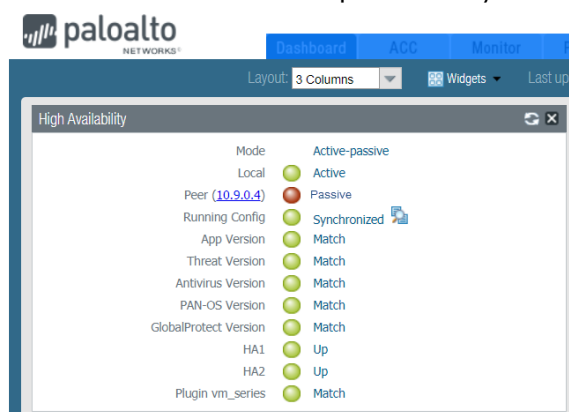
STEP 8 | Set up the network interfaces for the passive peer and enable HA.

Modify the IP addresses as appropriate for this passive HA peer. You do not have to configure the VM-Series plugin to authenticate to the Azure resource group, because that configuration is synchronized across the HA peers after you enable HA.



STEP 9 | After you finish configuring both firewalls, verify that the firewalls are paired in active/passive HA.

1. Access the **Dashboard** on both firewalls, and view the High Availability widget.
2. On the active firewall, click the **Sync to peer** link.
3. Confirm that the firewalls are paired and synced.



4. On the passive peer, verify that the VM-Series plugin configuration is now synced.

Select **Device > VM-Series** and validate that you can view the Azure HA configuration that you had omitted configuring on the passive peer.

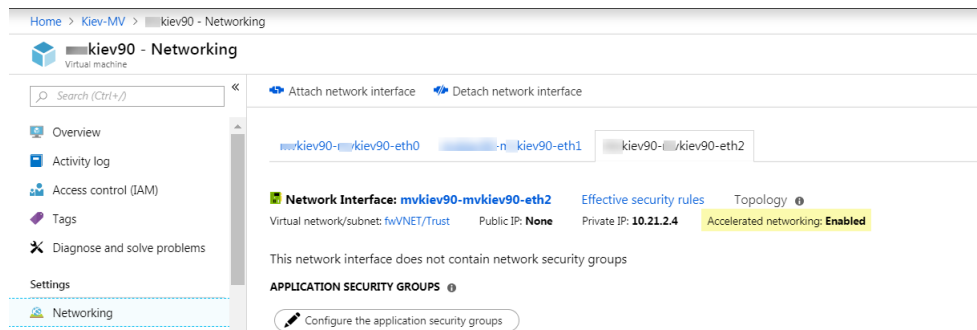
Higher Performance for VM-Series on Azure using Azure Accelerated Networking (SR-IOV)

[VM-Series firewalls](#) deployed on D/DSv2 and D/DSv3 class of Azure VMs include support for Accelerated Networking (SR-IOV). Refer to the Azure documentation for instruction on [supported VMs](#) and for instructions on [enabling accelerated networking](#).

You can enable accelerated networking for an existing firewall after upgrading it to PAN-OS 9.0 or deploy new instances of the firewall using the PAN-OS 9.0 solution template.

- When you select the DSv2 and DSv3 class of Azure VMs to deploy a new instance of the VM-Series firewall using the latest image (from the Azure portal), accelerated networking is automatically enabled on the dataplane interfaces of the firewall.

To verify that your firewall is enabled for accelerated networking, select the firewall, and on **Settings > Networking** and check that **Accelerated Networking** is **Enabled**.



- When you upgrade an existing VM-Series firewall to PAN-OS 9.0, to enable accelerated networking, you must stop the firewall and [use the Azure CLI](#) to enable it. If your firewalls belong to an availability set, you must stop/deallocate all instances within the availability set before enabling Accelerated Networking on any of the NICs. On a VM-Series firewall that is not part of an availability set or VMSS, you must stop/deallocate the individual instance only.

Panorama Features

- > Master Key Deployment from Panorama
- > Device Management Capacity Enhancement
- > Granular Configuration Management of Device Groups and Templates
- > Streamlined Device Onboarding

Master Key Deployment from Panorama

Panorama™, firewalls, Log Collectors, and WF-500 appliances use a master key to encrypt sensitive elements in a configuration. As part of a standard security practice, you must renew the key on each individual firewall, Log Collector, WildFire appliance, and Panorama when your master key expires. Starting with PAN-OS 9.0, you can now deploy a new master key to multiple firewalls, Log Collectors, and WF-500 appliances directly from Panorama to ensure a uniform key deployment. See [Configure the Master Key](#) for more information.

STEP 1 | [Log in to the Panorama web interface.](#)

STEP 2 | Select **Commit** > **Commit to Panorama** and **Commit** any pending changes.

Panorama must re-encrypt data using the new master key. To deploy the master key to managed devices and encrypt the data, you must commit all pending changes before you can successfully deploy the key. The new master key deployment fails if there are any pending changes on the Panorama management server.

STEP 3 | Deploy the master key to managed firewalls.

1. Select **Panorama** > **Managed Devices** > **Summary** and **Deploy Master Key**.
2. Select all devices and **Change** the master key.
3. Configure the master key and click **OK**.
4. Verify that the master key was deployed successfully to all selected devices.

A System log generates when you deploy a new master key from Panorama.

STEP 4 | Deploy the master key to Log Collectors.

1. Select **Panorama** > **Managed Collectors** and **Deploy Master Key**.
2. Select all devices and **Change** the master key.
3. Configure the master key and click **OK**.
4. Verify that the master key was deployed successfully to all selected devices.

A System log generates when you deploy a new master key from Panorama.

STEP 5 | Deploy the master key to managed WildFire appliances.

1. Select **Panorama** > **Managed WildFire Appliances** and **Deploy Master Key**.
2. Select all devices and **Change** the master key.
3. Configure the master key and click **OK**.
4. Verify that the master key was deployed successfully to all selected devices.

A System log generates when you deploy a new master key from Panorama.

Device Management Capacity Enhancement

PAN-OS 9.0 allows you to manage up to 5,000 firewalls using a single or M-600 appliance in a high availability (HA) configuration, or a similarly resourced Panorama™ virtual appliance. Managing your entire deployment from a single or Panorama management server in HA configuration alleviates the operational complexity of management, and reduces the security and compliance risk of managing multiple Panorama management servers. For log collection, a single Panorama management server is ideal because it provides a centralized location to view and analyze log data from managed devices, rather than requiring you to access each individual Panorama management server. To provide redundancy in the event of system or network failure, Palo Alto Networks recommends deploying two Panorama management servers in a HA configuration.

To manage up to 5,000 firewalls, the Panorama management server must meet the following minimum requirements:

Requirement	M-Series Appliance	Panorama Virtual Appliance
Model	M-600	All supported Panorama hypervisors. For more information, see Panorama Models .
Panorama Mode	Management Only	Management Only
System Disk	240GB SSD Used to store the operating system files and system logs.	81GB Used to store the operating system files and system logs.
Cores	28 (hyperthreaded)	56
Memory	256GB	256GB
Log Collection	Local log collection is not supported. See Deploy Panorama with Dedicated Log Collectors to set up log collection.	Local log collection is not supported. See Deploy Panorama with Dedicated Log Collectors to set up log collection.
Logging and Reporting	Enable the Use Panorama Data for Pre-Defined Reports setting (Panorama > Setup > Management > Logging and Reporting Settings > Log Export and Reporting)	Enable the Use Panorama Data for Pre-Defined Reports setting (Panorama > Setup > Management > Logging and Reporting Settings > Log Export and Reporting)

To manage up to 5,000 firewalls, determine your deployment scenario and follow the procedure:

- [Upgrade Panorama for Increased Device Management Capacity](#)
- [Install a New Panorama for Increased Device Management Capacity](#)

Upgrade Panorama for Increased Device Management Capacity

Upgrade an existing M-600 appliance, or similarly provisioned Panorama™ virtual appliance, to PAN-OS 9.0 to manage up to 5,000 firewalls using your existing device management license.

STEP 1 | [Log in to the Panorama CLI.](#)

STEP 2 | Change the Panorama management server to Management Only if Panorama is not already in this mode.

STEP 3 | [Log in to the Panorama web interface.](#)

STEP 4 | Upgrade the Panorama management server.

STEP 5 | Select **Panorama > Licenses** and verify that the device management license has been successfully activated.



If you activated your device management license and then upgraded to PAN-OS 9.0, you can manage up to 5,000 firewalls but the Description displays Device management license to manage up to 1000 devices.

If you are activating a new device management license on a Panorama, the Description displays Device management license to manage up to 1000 devices or more.

Install a New Panorama for Increased Device Management Capacity

To manage up to 5,000 firewalls from a single Panorama™ management server, set up the M-600 appliance, or deploy a similarly provisioned Panorama virtual appliance.

STEP 1 | Contact your Palo Alto Networks sales representative to obtain the Panorama device management license that enables you to manage up to 5,000 firewalls.

- If you are deploying an M-600 appliance, obtain the PAN-M-600-P-1K device management license.
- If you are deploying a Panorama virtual appliance, obtain the PAN-PRA-1000 device management license.

STEP 2 | Set up the Panorama management server.

STEP 3 | Change the Panorama management server to Management Only if Panorama is not already in this mode.

STEP 4 | Register your Panorama management server and install licenses.

1. [Register Panorama.](#)
2. [Activate a Panorama Support License.](#)
3. Activate the device management license on the Panorama management server.
 - [Activate/Retrieve a Firewall Management License on the M-Series Appliance](#)
 - [Activate/Retrieve a Firewall Management License when the Panorama Virtual Appliance is not Internet-connected](#)
 - [Activate/Retrieve a Firewall Management License when the Panorama Virtual Appliance is Internet-connected](#)

STEP 5 | Select **Panorama > Licenses** and verify that the device management license has been successfully activated.



If you activated your device management license and then upgraded to PAN-OS 9.0, you can manage up to 5,000 firewalls but the Description displays Device management license to manage up to 1000 devices.

If you are activating a new device management license on a Panorama, the Description displays Device management license to manage up to 1000 devices or more.

Granular Configuration Management of Device Groups and Templates

To support you with more granular control in managing device group and template configurations, PAN-OS 9.0 adds support for Granular Configuration Management of Device Groups and Templates, allowing administrators granular control when [saving and exporting](#), [reverting](#), or [loading](#) configurations. Administrators can now select specific device groups, templates, or template stacks in their assigned access domain, allowing for only the partial configuration to be reverted, saved, loaded or exported without affecting any other device group or template on the Panorama management server.

In this procedure, you revert the configuration of device groups and templates assigned to the administrator access domain to the last saved Panorama configuration.

STEP 1 | [Log in to the Panorama web interface](#).

STEP 2 | Select **Panorama > Setup > Operations** and **Revert to last saved Panorama configuration**.

STEP 3 | Select the **Select Device Group & Templates** check box when prompted.

STEP 4 | Select the device groups and templates to revert, and click **OK**.

STEP 5 | After the revert operation completes, click **Close**.

STEP 6 | Select **Commit > Commit and Push** and **Commit and Push** the reverted configuration to your managed devices.

Streamlined Device Onboarding

When [adding new firewalls](#) to be managed from a Panorama™ management server, you must assign firewalls to a device group and template stack in order to push the firewall configuration, as well as a Collector Group and a Log Collector to collect logs. PAN-OS 9.0 introduces the ability to associate new firewalls with a device group, template stack, Collector Group, and Log Collector during the initial firewall deployment. Additionally, you can enable the Panorama management server to automatically push the firewall configuration to the firewalls when they first connect to the Panorama. Automatically pushing the firewall configuration on the first connection to Panorama is supported only on firewalls not previously managed by a Panorama management server.

Streamlined Device Onboarding is supported on single vsys firewalls, and helps you to streamline and automate the device deployment procedure by allowing you to assign the new firewalls to their various configuration components as they are being added. By enabling Panorama to automatically push the firewall configuration as soon as the firewall has connected to Panorama, you ensure that the firewall is configured correctly and promptly. This helps reduce firewall deployment downtime and gets your networks secured quickly.

STEP 1 | Configure the firewall to connect to the Panorama management server.

Repeat this step for all firewalls you want to manage using the Panorama management server.

1. [Log in to the firewall web interface](#).
2. Select **Device > Setup > Management** and edit the **Panorama Settings**.
3. Enter the IP address of the Panorama management server and click **OK**.
4. Click **Commit** and **Commit** your changes.

STEP 2 | [Log in to the Panorama web interface](#).

STEP 3 | Add your managed devices.

- Add one or more managed devices
 1. Select **Panorama > Managed Devices > Summary** and **Add** a new managed device.
 2. Enter the firewall **Serial** number. If you are adding multiple firewalls, enter each serial number on a separate line.
 3. Select the **Associate Devices** check box and click **OK**.
 4. Assign the **Device Group**, **Template Stack**, **Collector Group**, or **Log Collector** from the drop-down of each column.
 5. Select the **Auto Push on 1st connect** check box to automatically push the device group and template stack configuration to the new devices when the devices successfully connect to Panorama.



The Auto Push on 1st Connect option is only supported on firewalls running PAN-OS 8.1 or later release. The `commit all` job executes from Panorama to managed devices running PAN-OS 8.1 and later releases.

6. Click **OK** to add the devices.
- Bulk import multiple devices using a CSV
 1. Select **Panorama > Managed Devices > Summary** and **Add** a new managed device.
 2. Click **Import**.
 3. Click **Download Sample CSV** and edit the downloaded CSV file with the firewalls you are adding. Save the CSV after you have finished editing it.
 4. Click **Browse...** and select the CSV file you edited in the previous step.

-
5. If not already assigned in the CSV, assign the firewalls a **Device Group**, **Template Stack**, **Collector Group**, or **Log Collector** from the drop-down of each column.
 6. If not already enabled in the CSV, select the **Auto Push on 1st connect** check box to automatically push the device group and template stack configuration to the new devices when the devices successfully connect to Panorama.
 7. Click **OK** to add the devices.

STEP 4 | Click **Commit** > **Commit to Panorama** and **Commit** your changes.

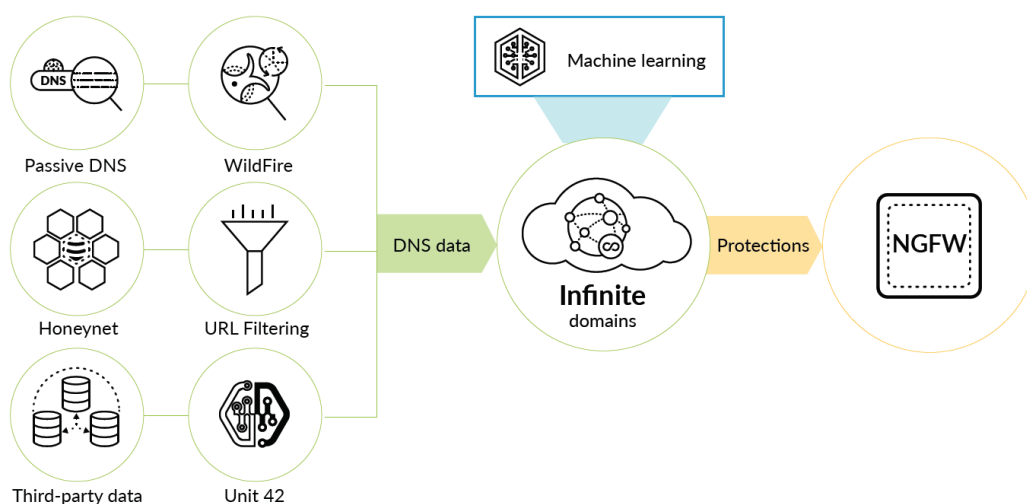
STEP 5 | Select **Panorama** > **Managed Devices** > **Summary** and verify that the new managed devices have successfully **connected** to the Panorama management server.

Content Inspection Features

- > DNS Security
- > New Security-Focused URL Categories
- > Multi-Category URL Filtering
- > Built-In External Dynamic List for Bulletproof Hosts
- > EDL Capacity Increases
- > Support for New Predefined Data Filtering Patterns
- > Cellular IoT Security
- > GTP Event Packet Capture

DNS Security

DNS Security is an on-demand cloud subscription service designed to protect your organization from advanced threats using DNS. By applying advanced machine learning and predictive analytics to a diverse range of threat intelligence sources, DNS Security generates an enhanced DNS signature set and provides real-time analysis of DNS requests to effectively defend your network against newly generated malicious domains. Because the DNS signatures and protections generated through this service are distributed by the cloud without the hardcoded limitations of the downloadable DNS signature sets, you can access newly added content without downloading and installing updates. To access the DNS security service, you must have a valid Threat Prevention and DNS Security license.



For information about using and configuring DNS Security for your deployment, see [DNS Security](#)

New Security-Focused URL Categories

New security-focused URL categories enable you to implement simple security and decryption policies based on website safety, without requiring you to research and individually assess the sites that are likely to expose you to web-based threats.

The new categories can help you to reduce your attack surface by providing targeted decryption and enforcement for sites that pose varying levels of risk, but are not confirmed malicious. Websites are classified with a security-related category only so long as they meet the criteria for that category; as site content changes, policy enforcement dynamically adapts.

Because [Multi-Category URL Filtering](#) allows for URLs to be classified with multiple categories, all URLs—except those that are confirmed malware, C2, or phishing sites—now include one of the risk categories, to indicate the level of suspicious activity the site displays. Unlike URL categories that identify page content and function, risk categories are always assigned at the domain-level (the risk category for an individual URL is inherited from the domain).

The following table below describes each of the new security-focused URL categories, and their default policy actions. If you choose not to block newly-registered domains, high-risk, and medium-risk categories, we recommend the following best practices to very strictly control user access and interaction with these types of sites:

- ❑ [Target decryption](#) to high-risk, medium-risk, and newly-registered domains.
- ❑ Enable the strict predefined Anti-Spyware, Vulnerability Protection, File Blocking profiles, and implement the [best practices](#) for each profile. To view the strict predefined security profiles, select **Objects > Security Profiles > Anti-Spyware/Vulnerability Protect/File Blocking**. You can't edit a predefined profile, but you can clone a predefined profile to use it as template for a new profile.
- ❑ Build a URL Filtering profile that [blocks all recommended categories](#). You can clone the default URL Filtering profile to get started, but you'll need to update the action for newly-registered domains to block.
- ❑ [Prevent phishing attacks](#) by blocking users from submitting their corporate credentials to high-risk, medium-risk, and newly-registered domains.
- ❑ [Display a response page](#) to users when they visit high- and medium-risk sites. Alert them that the site they are attempting to access is potentially malicious, and advise them on how to take precautions if they decide to continue to the site.



Change requests are not supported for risk categories or newly-registered-domains.


Security-Focused URL Categories

High-Risk

High-risk sites include:

- Sites previously confirmed to be malware, phishing, or C2 sites that have displayed only benign activity for at least 30 days.
- Unknown domains are classified as high-risk until PAN-DB completes site analysis and categorization.
- Sites that are associated with confirmed malicious activity. For example, a page might be high-risk if there are malicious hosts on the same domain, even if the page itself does not contain malicious content.

Security-Focused URL Categories

	<ul style="list-style-type: none">• Bulletproof ISP-hosted sites.• Sites hosted on IPs from ASNs that are known to allow malicious content. <p>Default and Recommended Policy Action: Alert</p>
Medium-Risk	<p>Medium-risk sites include:</p> <ul style="list-style-type: none">• All cloud storage sites (with the URL category online-storage-and-backup).• Sites previously confirmed to be malware, phishing, or C2 sites that have displayed only benign activity for at least 60 days.• Unknown IP addresses are categorized as medium-risk until PAN-DB completes site analysis and categorization. <p>Default and Recommended Policy Action: Alert</p>
Low-Risk	<p>All web content that is not medium or high-risk, is considered low-risk. This includes sites previously found to be malicious that have displayed only benign activity for at least 90 days.</p> <p>Default and Recommended Policy Action: Allow</p>
Newly-Registered Domains	<p>Identifies sites that have been registered within the last 32 days. New domains are frequently used as tools in malicious campaigns.</p> <p>Default Policy Action: Alert</p> <p>Recommended Policy Action: Block</p> <p> <i>Newly-registered domains are often generated purposefully or by domain generation algorithms and used for malicious activity. It is a best practice to block this URL category.</i></p>

Multi-Category URL Filtering

PAN-DB, the Palo Alto Networks URL database, now assigns multiple categories to URLs that classify a site's content, purpose, and safety. Every URL now has up to four categories, including a [risk category](#) that indicates how likely it is that the site will expose you to threats. More granular URL categorizations means that you can move beyond a basic "block-or-allow" approach to web access. Instead, you can control how your users interact with online content that, while necessary for business, is more likely to be used as part of a cyberattack.

For instance, you might consider certain URL categories risky to your organization, but are hesitant to block them outright as they also provide valuable resources or services (like cloud storage services or blogs). Now, you can allow users to visit sites that fall into these types of URL categories, while also protecting your network by decrypting and inspecting traffic and enforcing read-only access to the content.

With multi-category URL Filtering, PAN-DB might classify a developer blog that your engineers use for research as:

- personal-sites-and-blogs
- computer-and-internet-info
- high-risk

The blog might be high-risk because a malware-infected blog is hosted on the same domain. You'd like your users to be able to access the blog, but want to protect against potential threats. Now, you could design your security policy to allow personal-sites-and-blogs and computer-and-internet-info, and then very strictly limit the options available to users when accessing high-risk content (for example, block obfuscated Javascript, enable credential theft prevention, and restrict dangerous file downloads).

If you're already enforcing security policy based on URL categories, you will automatically start to benefit from multi-category URL Filtering after upgrading to PAN-OS 9.0.

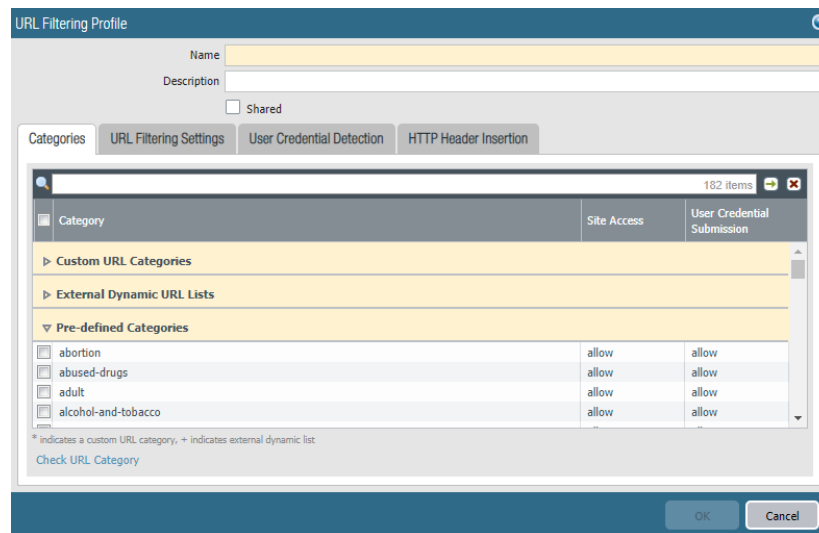
Here's what's most important to know about multi-category URL Filtering, with some tips to get started:

- ❑ Multi-category URL Filtering requires a [PAN-DB URL Filtering subscription](#). To confirm that the PAN-DB URL Filtering subscription license is active on the firewall, select **Device > Licenses**).

With an active license, the firewall connects to PAN-DB by default.

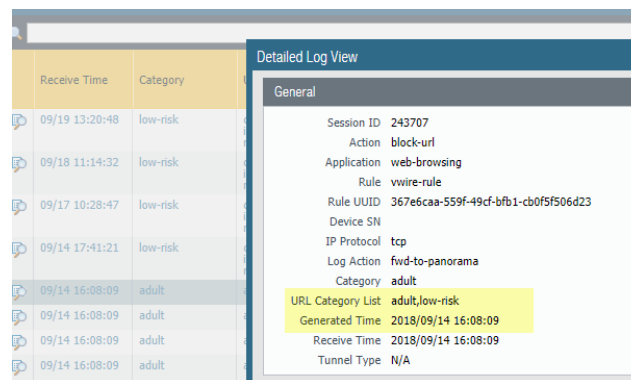
- ❑ You can [Test A Site](#) to see the categories that PAN-DB applies to URLs, and to learn about all the available URL categories.
- ❑ URL Filtering profiles now display your **Custom URL Categories**, **External Dynamic URL Lists**, and **Pre-defined Categories** (the PAN-DB categories) together, so that you can choose from these categories when defining policy for website access and usage.

The **Custom URL Categories** list now contains contents of the Allow and Block Lists that you would have previously set up on the **URL Filtering Profile Overrides** tab, which is now also removed.



- ❑ You can define a custom URL category based on multiple PAN-DB URL categories. A new type of custom URL Category, **Category Match**, means that you can target enforcement for a website or page that matches a set of categories. The website or page must match *all* of the categories that you list. Here's how to [create custom URL categories](#).
- ❑ For websites or pages that hold more than one URL category, URL Filtering logs display the URL category with which the firewall based policy enforcement (the **Category**). URL Filtering logs also display all the URL categories for the site (the **URL Category List**).

To view URL Filtering logs, select **Monitor > Logs > URL Filtering** and select any entry to learn more about the activity that triggered the log record.

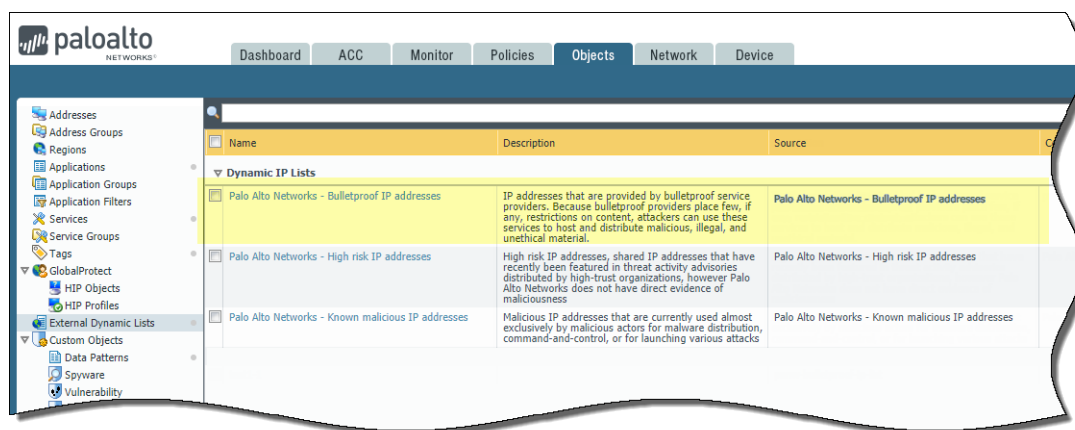


- ❑ To get started:
 - Visit <https://docs.paloaltonetworks.com/url-filtering.html> for everything you need to know about URL Filtering.
 - Follow the complete work flow to [configure URL Filtering](#), and start enforcing security policy based on URL categories.
 - Learn about the [New Security-Focused URL Categories](#) that allow you to control site access and how users interact with online content based on site safety.

Built-In External Dynamic List for Bulletproof Hosts

Because bulletproof hosting providers place few, if any, restrictions on content, attackers frequently use these services to host and distribute malicious, illegal, and unethical material. A Threat Prevention subscription now includes a new built-in external dynamic list (EDL) that you can use to block IP addresses supplied by a bulletproof hosting provider.

Daily antivirus content updates refresh the list, and the latest version of the list replaces the older version. Because the bulletproof hosts list is built-in to the firewall, you cannot modify its contents. However, if you'd like to exclude certain list entries or add to the list, you can create a new external dynamic list that uses the bulletproof host list as a source.



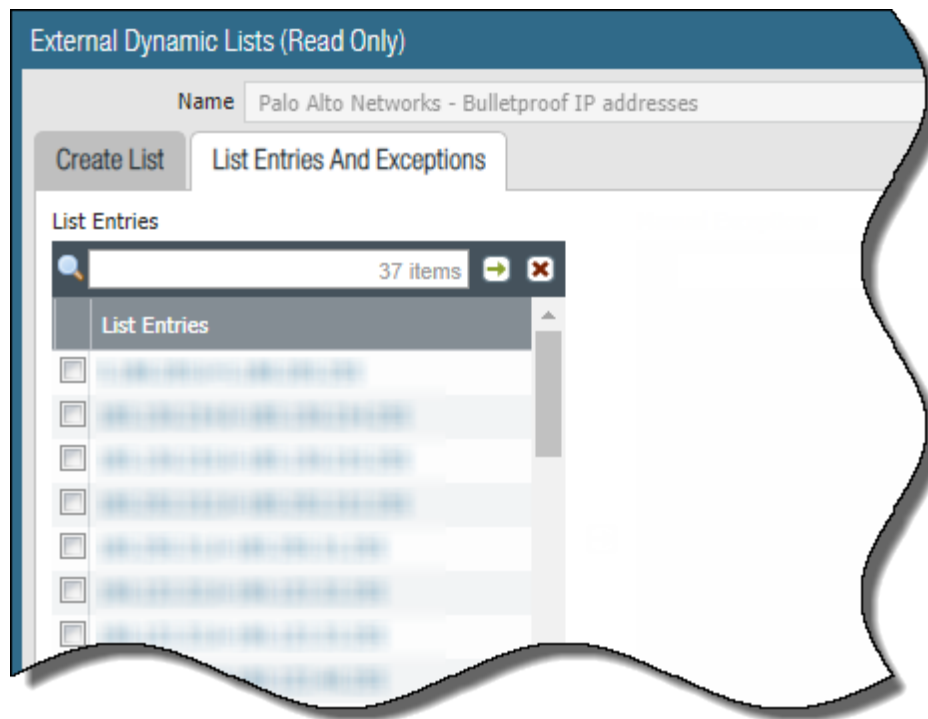
To start blocking malicious hosts that use bulletproof hosting providers:

STEP 1 | Confirm that the firewall can access and update the bulletproof ISP external dynamic list:

- Confirm that your [Threat Prevention](#) subscription license is active (select **Device** > **Licenses**).
- Confirm that the latest Antivirus and Applications and Threats [content updates](#) are installed (**Device** > **Dynamic Updates**).

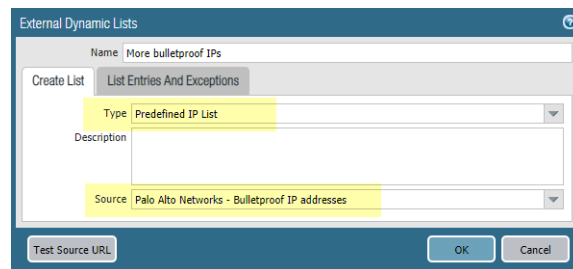
STEP 2 | View bulletproof IP address [list contents](#):

1. Select **Objects** > **External Dynamic Lists**.
2. Under Dynamic IP Lists, select **Palo Alto Networks - Bulletproof IP addresses** and then select **List Entries and Exceptions**. You cannot modify the contents of this list.



STEP 3 | You can exclude or add list entries by using the bulletproof IP address list as a source for a new list (you cannot directly modify the bulletproof IP address list contents):

1. **Add** a new external dynamic list.
2. Set the list **Type** to **Predefined IP List**.
3. Add the bulletproof IP address list as the **Source** for the new list.



STEP 4 | To block hosts that use bulletproof ISPs to provide malicious, illegal, and/or unethical content, [use the bulletproof IP address list in policy](#).

1. Select **Policies > Security**.
2. **Add** or modify a security policy rule.
3. In the **Source/Destination** tabs, select the bulletproof IP address list to be used as the policy rule **Source/Destination Address**.
4. Set the rule **Action** to **Deny**.

STEP 5 | To test the policy rule action:

1. View the [list contents](#) and attempt to access one of the IP addresses in the list.
2. Verify that the policy action you defined is enforced.
3. Select **Monitor > Logs > Traffic** to view the log entry for the session.


EDL Capacity Increases




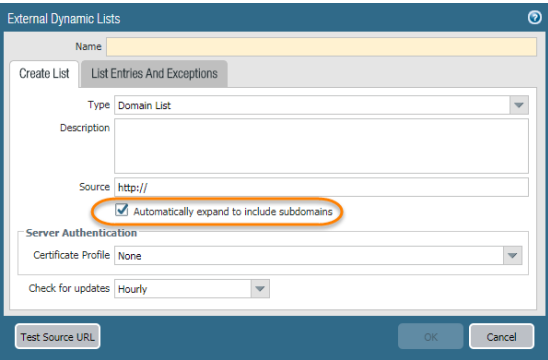
An [external dynamic list](#) is a text file of IP addresses, domains, or URLs hosted on an external web server. You can configure the firewall to import an external dynamic list and to block or allow traffic based on the entries listed in the file. The following enhancements provide increased EDL capacity limits for select appliances and the flexibility to prioritize the list in order to make sure your most important EDLs are committed before capacity limits are met. Moreover, you can now configure domain EDLs to expand domain names to include subdomains, as well as the ability to use exact matches and top-level domain entries, to help you create more comprehensive domain lists.

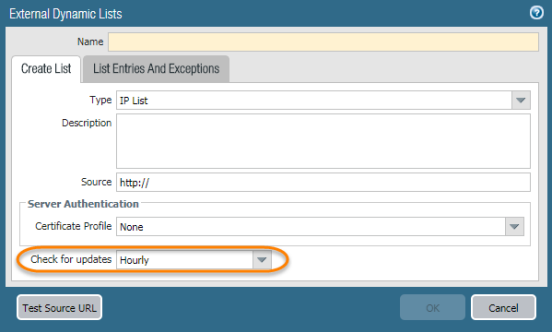


Upgrade Information

- As a best practice, Palo Alto Networks recommends using shared EDLs when multiple virtual systems are used. Using individual EDLs with duplicate entries for each vsys uses more memory, which might over-utilize firewall resources.
- EDL entry counts on firewalls operating multi-virtual systems take additional factors into account (such as DAGs, number of vsys, rules bases) to generate a more accurate capacity consumption listing. This might result in a discrepancy in capacity usage after upgrading from PAN-OS 8.x releases.
- Depending on the features enabled on the firewall, memory usage limits might be exceeded before EDL capacity limits are met due to memory allocation changes. As a best practice, Palo Alto Networks recommends reviewing EDL capacities and, when necessary, removing or consolidating EDLs into shared lists to minimize memory usage.

External Dynamic List Enhancement	Description															
Increased Domain and URL EDL capacities.	<p>The capacity limits for domain and URL EDLs have been substantially increased across the board for supported platforms. This increases the <i>total</i> number of allowable entries for domain and URL lists.</p> <ol style="list-style-type: none">1. Select Objects > External Dynamic Lists.2. Click List Capacities to compare how many IP addresses, domains, and URLs are currently used in policy with the total number of entries that the firewall supports for each list type. <div><div>Capacities</div><table><tr><th>List type</th><th>Currently used in policy</th><th>Total capacity</th></tr><tr><td>IPs</td><td>0</td><td>50000</td></tr><tr><td>Predefined IPs</td><td>0</td><td>50000</td></tr><tr><td>Domains</td><td>0</td><td>2000000</td></tr><tr><td>URLs</td><td>0</td><td>100000</td></tr></table><div>Close</div></div> <div> <i>External dynamic list entry calculation improvements in PAN-OS 9.0 generate a more accurate consumption list. These calculations take additional factors into account (such as DAGs, number of vsys, rules bases), however, this might also result in a discrepancy in capacity usage from previous PAN-OS 8.x releases. Palo Alto Networks recommends reviewing EDL capacities</i></div>	List type	Currently used in policy	Total capacity	IPs	0	50000	Predefined IPs	0	50000	Domains	0	2000000	URLs	0	100000
List type	Currently used in policy	Total capacity														
IPs	0	50000														
Predefined IPs	0	50000														
Domains	0	2000000														
URLs	0	100000														

External Dynamic List Enhancement	Description
	<p><i>and, when necessary, removing or consolidating EDLs into shared lists to minimize memory usage.</i></p>
<p>Prioritization of EDLs.</p>	<p>The EDLs in the Objects > External Dynamic Lists menu are shown top to bottom, in order of evaluation. Use the directional controls at the bottom of the page to change the list order. This allows you to reorder the lists to make sure the most important EDLs are committed before capacity limits are reached.</p>  <p> <i>You cannot change the EDL order when Group By Type has been selected.</i></p>
<p>Automatically Expand Domains on a Per-List Basis</p>	<p>When enabled, this feature allows you to configure your domain EDLs to automatically include the subdomains of a specified domain. For example, if your domain list includes paloaltonetworks.com, all lower level components of the domain name (e.g., *.paloaltonetworks.com) will also be included as part of the list.</p> <p> <i>When this setting is enabled, each domain in a given list requires an additional entry, effectively doubling the number of entries that are consumed. You can check your capacity usage by clicking on List Capacities.</i></p> 
<p>Domain List Enhancements</p>	<p>Domain lists now support use of exact matches and top-level domain entries.</p> <p>This allows you to specify a single specific entry to match against a website, subdomains, and pages. You can also match against entire top-level domains, allowing you to add TLDs associated with malicious content to your EDLs.</p> <ul style="list-style-type: none"> • (^)—Use carets (^) to indicate an exact match of a domain. For example, ^paloaltonetworks.com

External Dynamic List Enhancement	Description
	<p>matches only to paloaltonetworks.com. This entry does not match to any other site.</p> <ul style="list-style-type: none"> (*)—Use (*) in front of a top-level domain to match with all websites associated with the specified TLD. For example, *.work matches with all websites ending with the TLD of .work.
User Interface Enhancement	<p>The description for the dropdown used to specify the frequency at which the firewall retrieves the EDL on the Objects > External Dynamic Lists > external_dynamic_list page has been changed from Repeat to Check for updates.</p> 

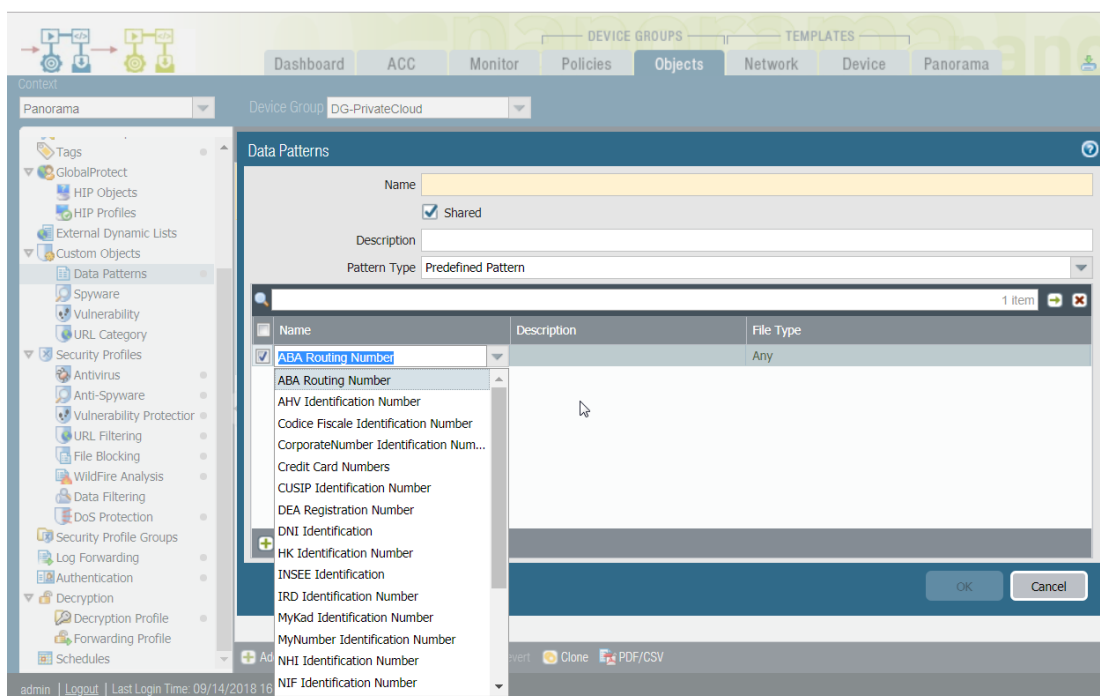
Support for New Predefined Data Filtering Patterns

To enable compliance for standards such as HIPAA, GDPR, Gramm-Leach-Bliley Act, the firewall now supports 19 new predefined [data filtering patterns](#) that help prevent the loss of sensitive information and records. These new patterns also support checksum validation algorithms to ensure that data patterns are matched correctly and help significantly reduce the possibility of false positives. The new data filtering patterns included in PAN-OS 9.0.0 are:

- ABA Routing Number —The American Banking Association Routing Number.
- CUSIP Identification Number —Committee on Uniform Security Identification Procedures Identification Number
- DEA Registration Number —U.S. Drug Enforcement Administration Registration Number
- INSEE Identification Number —French National Institute of Statistics and Economic Studies identification number
- Codice Fiscale Identification Number —Italian Fiscal Tax Code Card Identification Number
- DNI Identification Number —Spanish Documento nacional de identidad Identification Number number
- NIF Identification Number —Spanish Tax Identification Number
- AHV Identification Number —Swiss Alters und Hinterlassenenversicherungsnummer
- NHI Identification Number —New Zealand National Health Index Number
- IRD Identification Number —New Zealand Internal Revenue Department Identification Number
- MyNumber Identification Number—Japanese Social Security and Tax Number System Identification Number
- CorporateNumber Identification Number —Japanese National Tax Agency Corporate Number
- PRC Identification Number —People's Republic of China Resident Identification Number
- HK Identification Number —Hong Kong Residents Identification Number
- Permanent Account Identification Number —India Permanent Account Number of Indian nationals.
- NRIC Identification Number—Singapore National Registration Identity Card Identification Number
- MyKad Identification Number —Malaysia MyKad Identity Card Identification Number
- RRN Identification Number —Republic of South Korea Resident Registration Number
- NIN Identification Number —Taiwan Identification Card Number

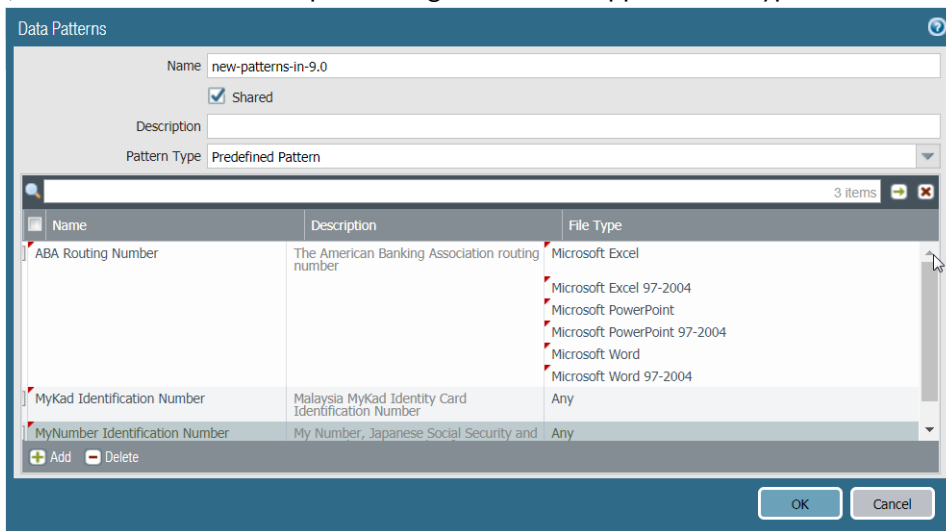
STEP 1 | Define a new data pattern object to detect the information you want to filter.

1. Select **Objects > Custom Objects > Data Patterns** and **Add** a new object.
2. Provide a descriptive **Name** for the new object.
3. Set the **Pattern Type** to **Predefined Pattern** and **Add** a new rule to the data pattern object.



4. Select the data patterns that you want to monitor on your network, specify the file types in which to look for these patterns, and **OK** to save the data pattern.

By default, the firewall matches the patterns against all the supported file types.



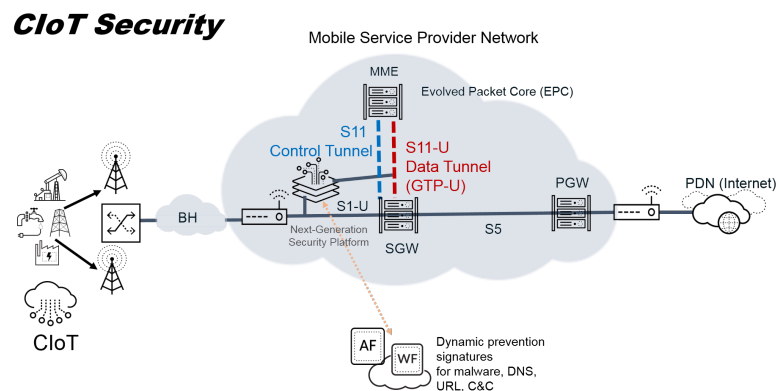
STEP 2 | See [Set up data filtering](#) to add the data pattern object to a data filtering profile, and use the settings to inspect traffic on your network.

Cellular IoT Security

Cellular Internet of Things (CloT) security allows you to protect your mobile network and CloT traffic from attacks and provides visibility into CloT communications in your network. If you are a mobile network operator (MNO) or a mobile virtual network operator (MVNO), you can secure CloT traffic. An example is a utility company that focuses on oil, gas, or energy and operates as an MVNO. As networks evolve with new technologies and you deploy firewalls in different locations, the firewall supports these CloT technologies (S11-U tunnels and narrow-band IoT [NB-IoT]). The firewall also supports device-to-device (D2D) communications over your network.

Cellular IoT security includes:

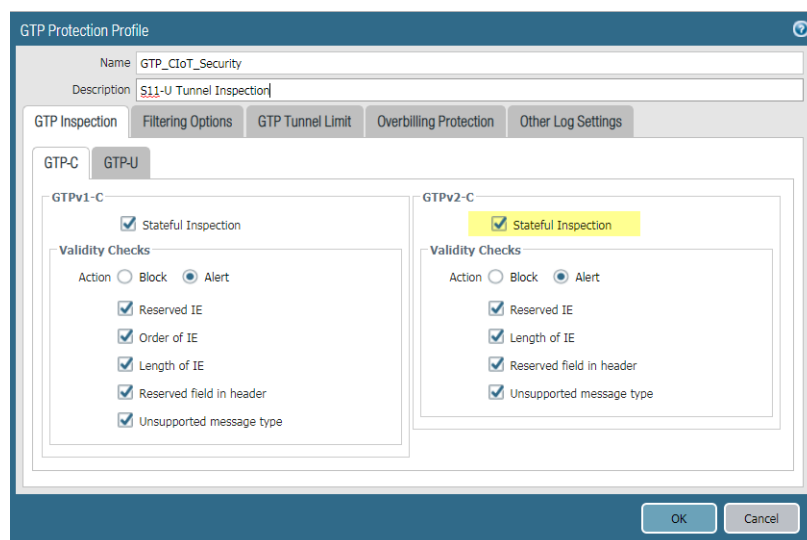
- Support for CloT Evolved Packet System (EPS) optimization.
 - GTP Stateful Inspection of S11 and S11-U tunnels.
 - GTP-U Content Inspection of S11-U tunnels (inspect the content of inner IP sessions of S11 GTP-U tunnels).
- Filtering traffic from IoT devices that connect a mobile network using EUTRAN-NB-IoT (Radio Access Network for NB-IoT). For example, allowing only devices that use NB-IoT access to the network.
- Displaying and reporting on D2D communication to see the Remote User ID and Remote User IP address of devices sending traffic.
- Support for 3GPP TS 29.274 up to Release 15.2.0 for GTPv2-C protocol
- Support for 3GPP TS 29.060 up to Release 15.1.0 for GTPv1-C protocol



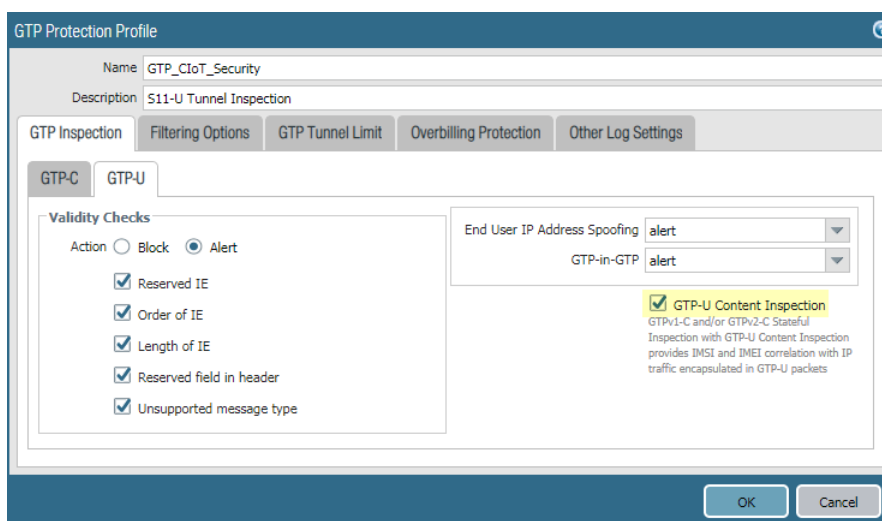
The preceding [CloT security deployment](#) graphic illustrates the S11-U data tunnel, which carries encapsulated data messages using GTP-U. If mobile-originated or mobile-terminated data is transported in control plane CloT EPS Optimization with PGW connectivity, the MME and SGW use an S11-U tunnel.

You can protect your mobile network and CloT traffic that uses 3GPP technologies.

- After you enable **GTP Security**, create a [GTP Protection profile](#) to [enable GTPv2-C Stateful Inspection](#).



- On the **GTP-U** tab, enable **GTP-U Content Inspection**.



GTP-U Content Inspection allows you to view Remote User ID (international mobile subscriber identity [IMSI]) and Remote User IP address data for GTP-U packets.

- If you use narrow-band IoT (NB-IoT) as Radio Access Technology (RAT), filter GTP traffic generated for IoT devices to safely allow only NB-IoT traffic from trusted services.

GTP Protection Profile

Name:

Description:

☒ Shared

RAT	Action
UTRAN	block
GERAN	block
WLAN	block
GAN	block
HSPA Evolution	block
EUTRAN	block
Virtual	block
EUTRAN-NB-IoT	allow

- Attach the GTP Protection profile to a Security policy rule and apply the rule on network elements that use GTP, such as between an MME and SGW.
- Monitor GTP or Unified log messages (**Monitor > Logs > GTP** or **Monitor > Logs > Unified**) and display the Remote User ID and Remote User IP address. The following is an example of viewing details of Remote user equipment (UE) using 3GPP D2D technology.

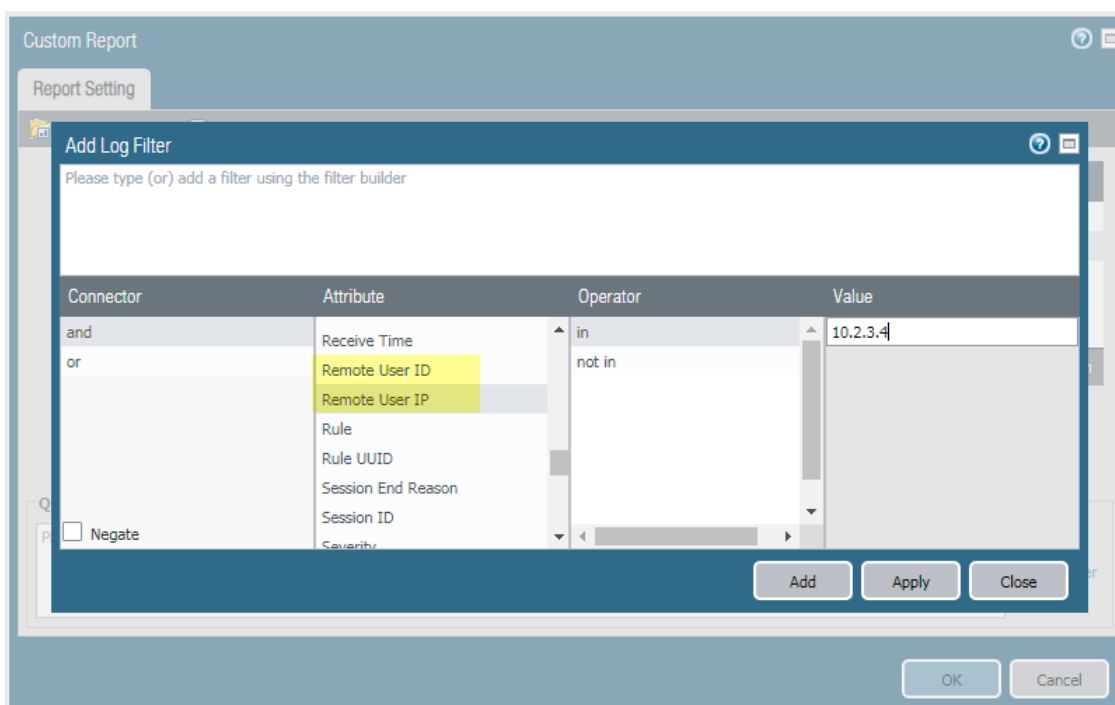
paloalto NETWORKS

Dashboard ACC **Monitor** Policies Objects Network Device

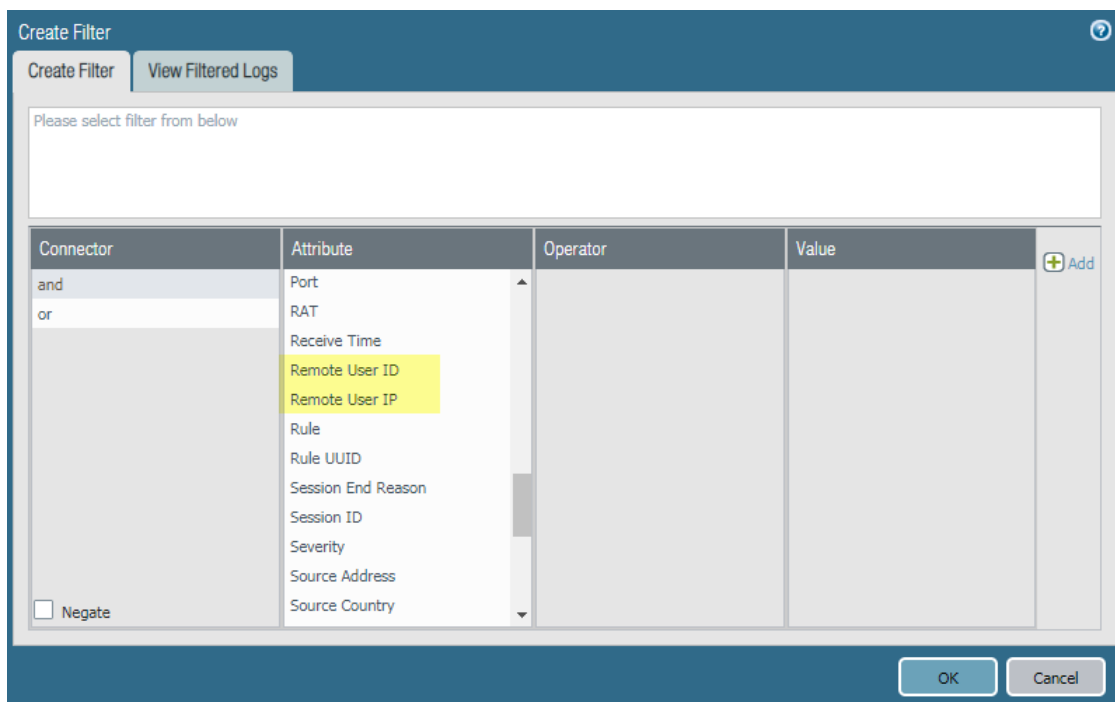
Virtual System **All**

	Receive Time	GTP Event Type	IMSI	GTP Message Type	Remote User ID	Remote User IP
	08/02 17:09:19	GTP-U G-PDU message	5050241012150...	G-PDU	42732089418...	10.2.45.2

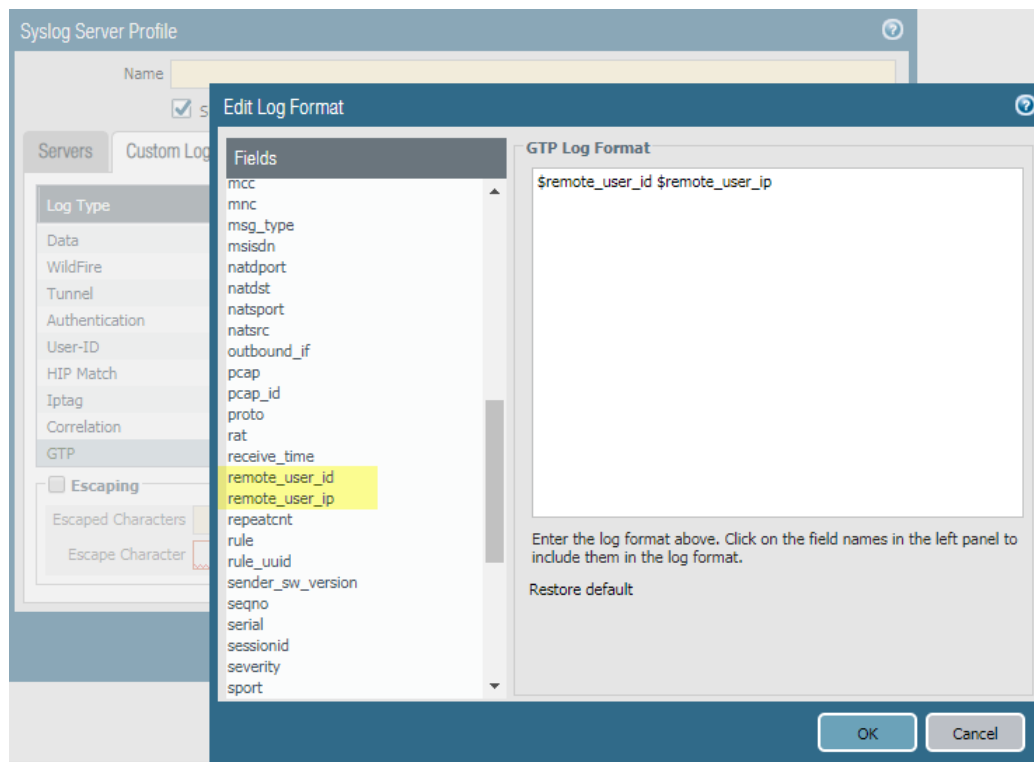
- Generate custom reports (**Monitor > Manage Custom Reports**) from the GTP Summary or GTP Detailed database and display Remote User ID and Remote User IP addresses. You can also select Filter Builder and add a log filter based on Remote User ID and Remote User IP address.



- Forward logs (**Objects > Log Forwarding**) and when you create a log forwarding profile, for the **gtp** log type, use Filter Builder to create a filter based on the Remote User IP address and Remote User ID attributes.



- While forwarding logs, if the Forward Method is Email, Syslog, or HTTP, add an Email Server Profile, Syslog Server Profile, or HTTP Server Profile respectively, and in the Custom Log Format tab, select GTP and remote_user_id or remote_user_ip to include either (or both) in the log format.



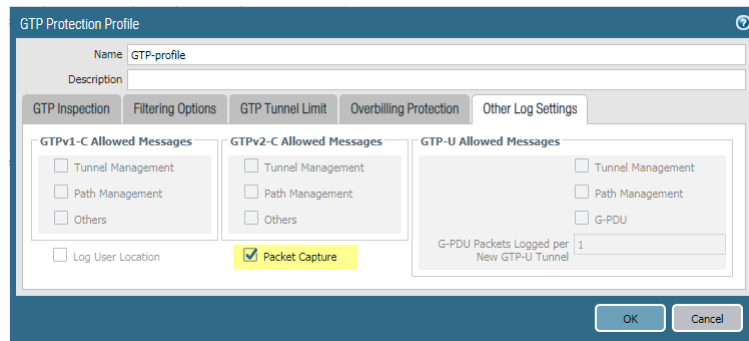
GTP Event Packet Capture

Mobile networks have a high volume of GTP traffic and if you need to troubleshoot GTP, it is easier to examine a packet capture of a single GTP event than it is to examine a device-level packet capture of many megabytes. You can now capture a single GTP packet that triggered an erroneous GTP event. A GTP packet capture includes the following events:

- GTP-in-GTP
- End-user IP address spoofing
- Abnormal GTPv1-C, GTPv2-C, and GTP-U messages that have a missing mandatory Information Element (IE), invalid IE, out-of-order IE, invalid header, or unsupported message type
- Other abnormal GTPv1-C, GTPv2-C, and GTP-U messages


STEP 1 | Enable GTP.

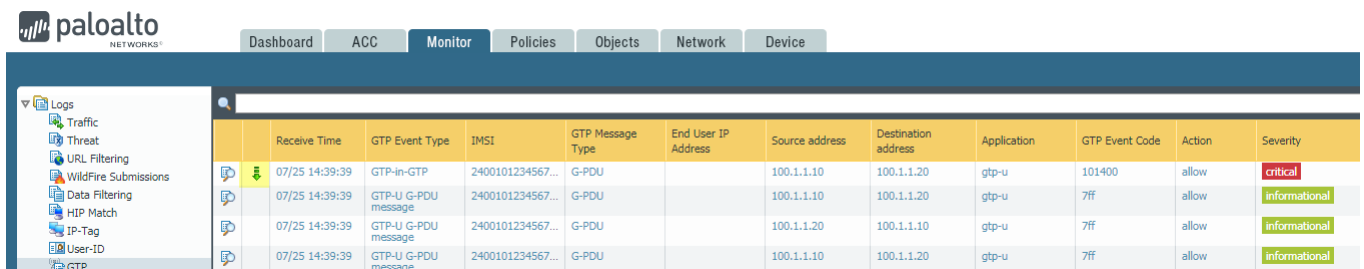
STEP 2 | Enable packet capture in a [GTP Protection profile](#).







STEP 3 | Apply the GTP Protection profile to a [Security policy rule](#) that applies to the zone you are protecting.

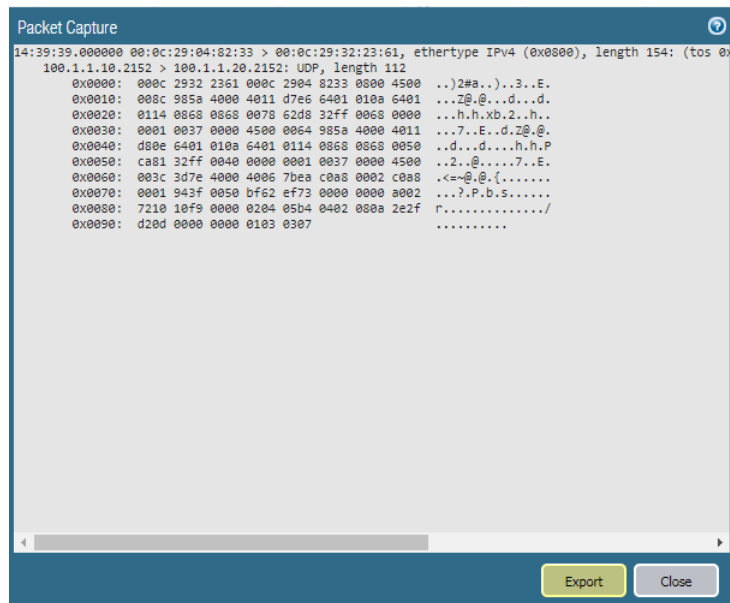
STEP 4 | **Commit** your changes.

STEP 5 | If the [Application Command Center \(ACC\)](#) on your firewall indicates a GTP problem that you want to troubleshoot, select **Monitor** > **Logs** > **GTP** and look for the GTP packet capture icon () at the beginning of rows that capture troublesome GTP packets. View the GTP Event Type (such as GTP-in-GTP), the international mobile subscriber identity (IMSI), source and destination IP address of the packet, and other information.

The image shows the Palo Alto Networks management interface with the 'Monitor' tab selected. The 'Logs' section is expanded, and the 'GTP' log is selected. The log table displays the following data:

	Receive Time	GTP Event Type	IMSI	GTP Message Type	End User IP Address	Source address	Destination address	Application	GTP Event Code	Action	Severity
	07/25 14:39:39	GTP-in-GTP	2400101234567...	G-PDU		100.1.1.10	100.1.1.20	gtp-u	101400	allow	critical
	07/25 14:39:39	GTP-U G-PDU message	2400101234567...	G-PDU		100.1.1.10	100.1.1.20	gtp-u	7ff	allow	informational
	07/25 14:39:39	GTP-U G-PDU message	2400101234567...	G-PDU		100.1.1.20	100.1.1.10	gtp-u	7ff	allow	informational
	07/25 14:39:39	GTP-U G-PDU message	2400101234567...	G-PDU		100.1.1.10	100.1.1.20	gtp-u	7ff	allow	informational

STEP 6 | If you want to verify the event, download () a packet capture file.



STEP 7 | Export the file to readable format and verify that the details support the GTP event type.

GlobalProtect Features

- > Endpoint Tunnel Configurations Based on Source Region or IP Address
- > Portal Configuration Assignment and HIP-Based Access Control Using New Endpoint Attributes
- > HIP Report Redistribution
- > DNS Configuration Assignment Based on Users or User Groups
- > Tunnel Restoration and Authentication Cookie Usage Restrictions
- > Mixed Authentication Method Support for Certificates or User Credentials
- > Pre-Logon Followed by Two-Factor Authentication
- > Pre-Logon Followed by SAML Authentication
- > GlobalProtect Gateway and Portal Location Configuration
- > User Location Visibility on GlobalProtect Gateways and Portals
- > Concurrent Support for IPv4 and IPv6 DNS Servers
- > Support for IPv6-Only GlobalProtect Deployments

Endpoint Tunnel Configurations Based on Source Region or IP Address

Software Support: PAN-OS® 9.0 and later releases

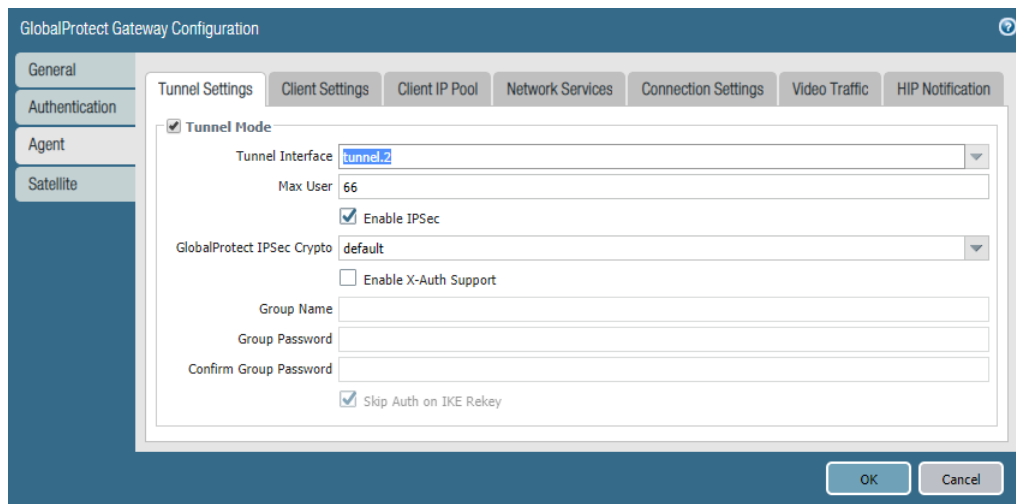
You can now deploy tunnel configurations for multiple user locations (internal, external, and specific source regions) from a single GlobalProtect gateway. This enhancement simplifies gateway deployment and management by enabling users to connect to the same gateway from different locations. Based on the location from which they are connecting, users receive the associated tunnel configuration with specific authentication override, IP pool, split tunnel, and DNS settings. For example, you may need to provide secure network access for both branch office users and roaming mobile users through GlobalProtect. With this feature, you can configure a GlobalProtect gateway to allow traffic for local subnet access (for example, local network printing) to bypass the VPN tunnel when end users connect from a branch office but require all traffic to route through the VPN tunnel for inspection and policy enforcement when users connect remotely from an unknown or untrusted network (such as a coffee shop or library).

Use the following steps to configure a GlobalProtect gateway with location-based tunnel configurations:

STEP 1 | [Configure a GlobalProtect gateway.](#)

STEP 2 | [Enable tunneling and then configure the tunnel parameters.](#)

If you want to configure the gateway to support tunnel configurations for both internal and external users, you must configure the tunnel parameters. This ensures that all user traffic for this gateway (including internal user traffic) goes through the VPN tunnel for inspection and policy enforcement.



The screenshot shows the 'GlobalProtect Gateway Configuration' window with the 'Tunnel Settings' tab selected. The 'Tunnel Mode' checkbox is checked. The 'Tunnel Interface' is set to 'tunnel.2'. The 'Max User' is set to '66'. The 'Enable IPsec' checkbox is checked. The 'GlobalProtect IPsec Crypto' is set to 'default'. The 'Enable X-Auth Support' checkbox is unchecked. The 'Group Name', 'Group Password', and 'Confirm Group Password' fields are empty. The 'Skip Auth on IKE Rekey' checkbox is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

STEP 3 | [Configure a client settings configuration.](#)

STEP 4 | Specify the [config selection criteria](#) (including the user location) for your client settings configuration.

The config selection criteria indicates the criteria that users must match against when connecting to a GlobalProtect gateway. If a user matches all specified criteria (**Source User**, **OS**, and **Source Address**), the gateway deploys this client settings configuration to the user.

The screenshot shows the 'Configs' window with the 'Config Selection Criteria' tab selected. The 'Name' field is empty. The 'Config Selection Criteria' section contains a table with two columns: 'Source User' and 'OS'. The 'Source User' column has a dropdown menu set to 'any'. The 'OS' column has a checkbox labeled 'Any' which is checked. Below the table are 'Add' and 'Delete' buttons. The 'Source Address' section contains a table with two columns: 'Region' and 'IP Address'. The 'IP Address' column has a checkbox labeled '10.10.10.0/24' which is checked. Below the table are 'Add' and 'Delete' buttons. At the bottom, there is a note: 'The configuration must match User and OS and either Region or IP Address if specified.' and 'OK' and 'Cancel' buttons.

STEP 5 | Save the gateway configuration.

Click **OK** twice.

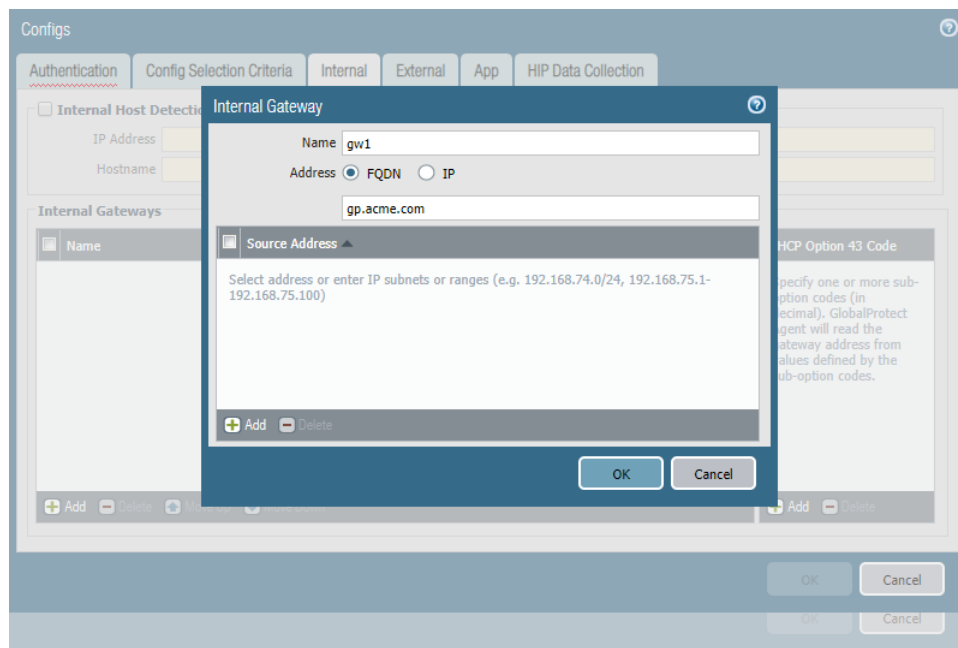
STEP 6 | (Optional) Repeat steps 3-5 to configure additional client settings configurations for different user locations.

STEP 7 | Set up access to the GlobalProtect portal.

STEP 8 | Define an agent configuration on the portal.

If you configure a GlobalProtect gateway to support tunnel configurations for both internal and external users, you must configure the following options in the portal agent configuration:

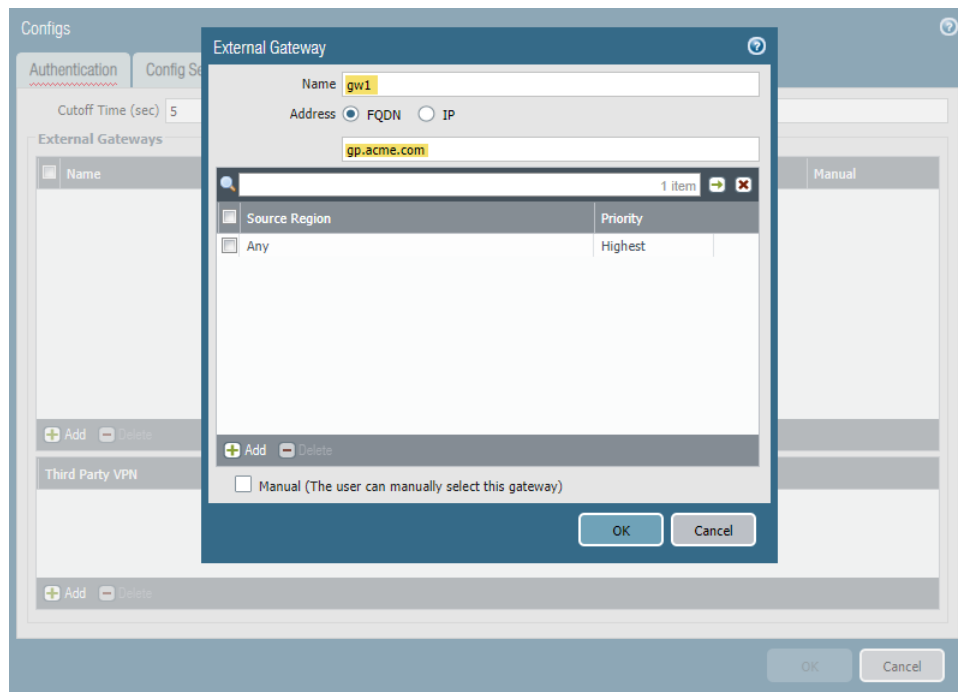
- **Enable internal host detection.**
Internal host detection allows the GlobalProtect app to determine whether a user's endpoint is inside or outside the enterprise network.
- Enable users with this portal agent configuration to connect to the same gateway both internally and externally:
 1. **Enable users to connect to the gateway internally.**



2. Enable users to connect to the gateway externally.

You must **Add** the same gateway that you added to the **Internal** gateway configuration.

- Enter the same gateway **Name** that you entered in the **Internal** gateway configuration.
- Enter the same **FQDN** or **IP** address that you entered in the **Internal** gateway configuration.



Portal Configuration Assignment and HIP-Based Access Control Using New Endpoint Attributes

Software Support: PAN-OS® 9.0 and later releases

You can now deploy different configurations for managed endpoints and unmanaged endpoints from a single GlobalProtect portal or gateway. To identify the managed status of an endpoint, GlobalProtect portals and gateways can use any of the following information:

- **The endpoint's machine certificate:** The GlobalProtect portal and gateway can determine whether an endpoint is managed or unmanaged by verifying that the endpoint's machine certificate matches the certificate profile that you configure for your portal or gateway. For a successful match, the machine certificate must be signed and issued by a CA certificate and (optional) template that you configure in the certificate profile. In addition, the gateway can identify the endpoint status based on the presence of specific attributes in the endpoint's machine certificate.
- **Presence of the endpoint serial number in the Active Directory or Azure AD:** The GlobalProtect portal and gateway can determine whether an endpoint is managed or unmanaged by verifying the presence of the endpoint serial number in the Active Directory or Azure AD. If an endpoint is managed, you can bind the serial number of the endpoint to the machine account of the endpoint in your directory server (such as Active Directory). The firewall can then pre-fetch the list of endpoint serial numbers by retrieving [group mapping](#) information from the directory server. When a user attempts to establish a GlobalProtect connection, the GlobalProtect app sends the serial number of the connecting endpoint to the portal or gateway to match against the list of serial numbers on the firewall. If the serial number exists, the endpoint is managed. If the serial number does not exist, the endpoint is unmanaged.
- **Specific software and settings that are required for managed endpoints:** The GlobalProtect portal and gateway can determine whether an endpoint is managed or unmanaged by verifying the presence of specific software and app settings on the endpoint, as defined in the [Windows Registry](#) and [macOS plist](#).

Based on the endpoint attributes, the portal pushes the associated configuration to the endpoint (for example Always On VPN for managed endpoints and Remote Access VPN for unmanaged endpoints) and gateways enforce specific HIP-based security policies for fine-grained access control.

Refer to the following sections for more information on identification and policy enforcement for managed and unmanaged endpoints:

- [Agent Configurations Based on the Endpoint's Machine Certificate](#)
- [Agent Configurations Based on the Endpoint Serial Number](#)
- [Agent Configurations Based on Software and App Settings](#)
- [HIP-Based Policy Enforcement Based on the Endpoint Status](#)

Agent Configurations Based on the Endpoint's Machine Certificate

Use the following steps to push agent configurations to connecting endpoints based on the endpoint's machine certificate:

STEP 1 | If you want to use the endpoint's machine certificate to identify the endpoint status, [configure a certificate profile](#).

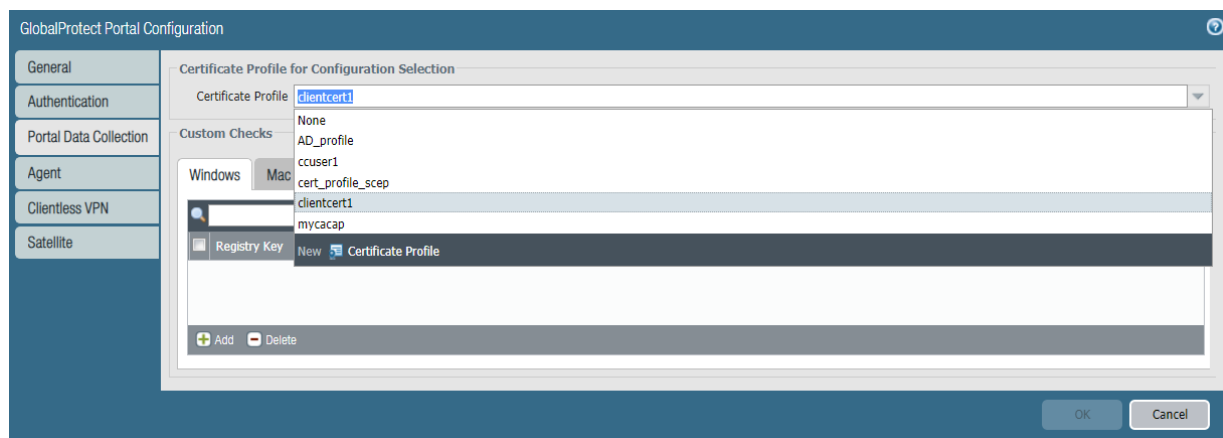
The GlobalProtect portal uses this certificate profile to match the machine certificate sent by the GlobalProtect app. For a successful match, the machine certificate must be signed and issued by the

same CA certificate and (optional) template that you configure in the certificate profile. If you do not configure a template, the machine certificate matches based on only the configured CA certificate.

STEP 2 | Set up access to the GlobalProtect_portal.

STEP 3 | Define the data that the GlobalProtect app collects from connecting endpoints after users successfully authenticate to the portal.

To specify the machine certificates that you want the GlobalProtect app to collect from connecting endpoints, select the **Certificate Profile** that you configured in [Step 1](#).



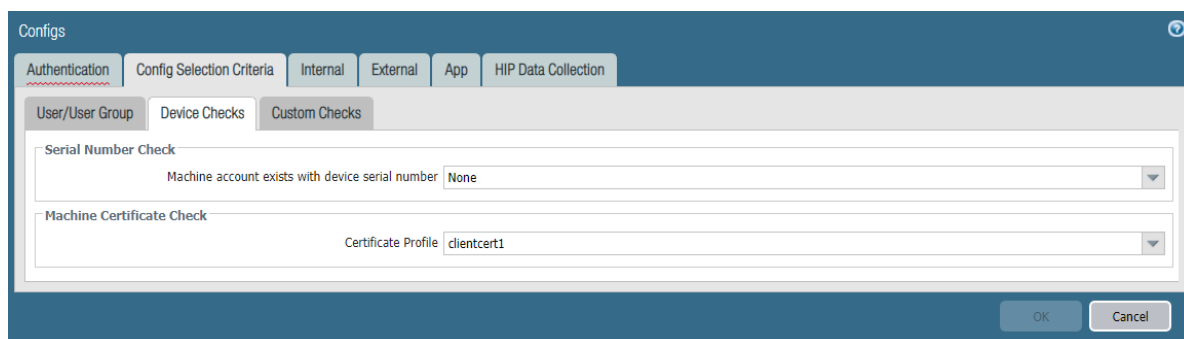
STEP 4 | Define an agent configuration_on the portal.

STEP 5 | Add config selection criteria for your agent configuration based on certificate profiles.

After the GlobalProtect app collects machine certificates from connecting endpoints (as defined in [Step 3](#)), it sends the certificates to the portal to match against the certificate profile that you specify in the config selection criteria for each agent configuration. If an endpoint matches all config selection criteria for an agent configuration, the portal pushes that agent configuration to the endpoint.

To deliver your agent configuration to connecting endpoints based on the endpoints' machine certificate, use the following steps:

1. Select **Config Selection Criteria > Device Checks**.
2. In the Machine Certificate Check area, select a **Certificate Profile** to match against the machine certificates installed on the endpoints.



STEP 6 | Save the portal configuration.

1. Click **OK** twice.
2. **Commit** your changes.

Agent Configurations Based on the Endpoint Serial Number

Use the following steps to push agent configurations to connecting endpoints based on the presence of the endpoint serial number in the Active Directory or Azure AD:



This enhancement is applicable only to Android, Windows, macOS, and Linux endpoints.



To verify the presence of an endpoint serial number on the firewall, you must first populate a directory server with the list of serial numbers for all managed endpoints.

STEP 1 | Enable group mapping.

To identify the endpoint status based on the endpoint serial number, you must configure [group mapping](#). If an endpoint is managed, you can bind the serial number of the endpoint to the machine account of the endpoint in your directory server (such as Active Directory). The firewall can then pre-fetch the serial numbers of these managed endpoints when it retrieves group mapping information from the directory server.

In your Group Mapping configuration (**Device > User Identification > Group Mapping Settings > <group-mapping-config>**), you must enable the option to **Fetch list of managed devices**. This allows the firewall to retrieve serial numbers from the directory server.

STEP 2 | Set up access to the GlobalProtect_portal.

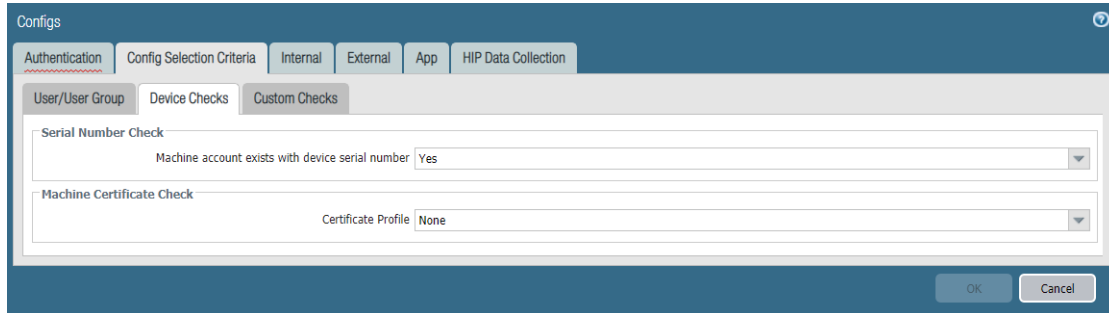
STEP 3 | Define an agent configuration_on_the portal.

STEP 4 | Add [config selection criteria](#) for your agent configuration based on the presence of the endpoint serial number in the Active Directory or Azure AD.

When a user attempts to establish a GlobalProtect connection, the GlobalProtect app sends the serial number of the connecting endpoint to the portal to match against the list of serial numbers in the Active Directory or Azure AD. If an endpoint matches all config selection criteria for an agent configuration, including the presence of the endpoint serial number in the Active Directory or Azure AD, the portal pushes that agent configuration to the endpoint.

To deliver your agent configuration to connecting endpoints based on the presence of the endpoint serial number in the Active Directory or Azure AD, use the following steps:

1. Select **Config Selection Criteria > Device Checks**.
2. In the Serial Number Check area, select an option from the **Machine account exists with device serial number** drop-down. If you set this option to **Yes**, the agent configuration applies only to endpoints with a serial number that exists (managed endpoints). If you set this option to **No**, the agent configuration applies only endpoints with a serial number that does not exist (unmanaged endpoints). If you set this option to **None**, the configuration is not delivered to apps based on the presence of the endpoint serial number.



STEP 5 | Save the portal configuration.

1. Click **OK** twice.
2. **Commit** your changes.

Agent Configurations Based on Software and App Settings

Use the following steps to push agent configurations to connecting endpoints based on the presence of specific software and app settings on the endpoint:

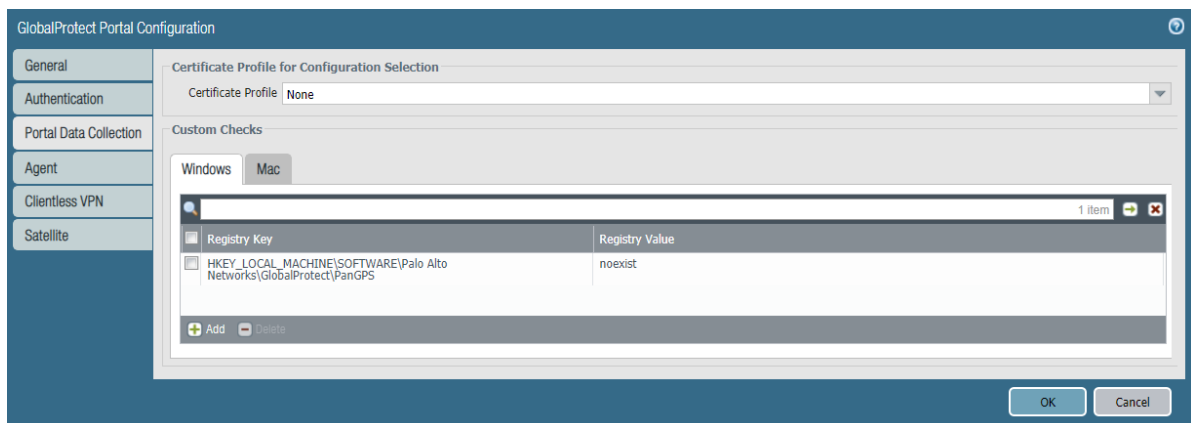
STEP 1 | (Optional) Deploy app settings using the Windows Registry or macOS plist.

The Windows Registry and macOS plist enable you to deploy app settings directly to endpoints.

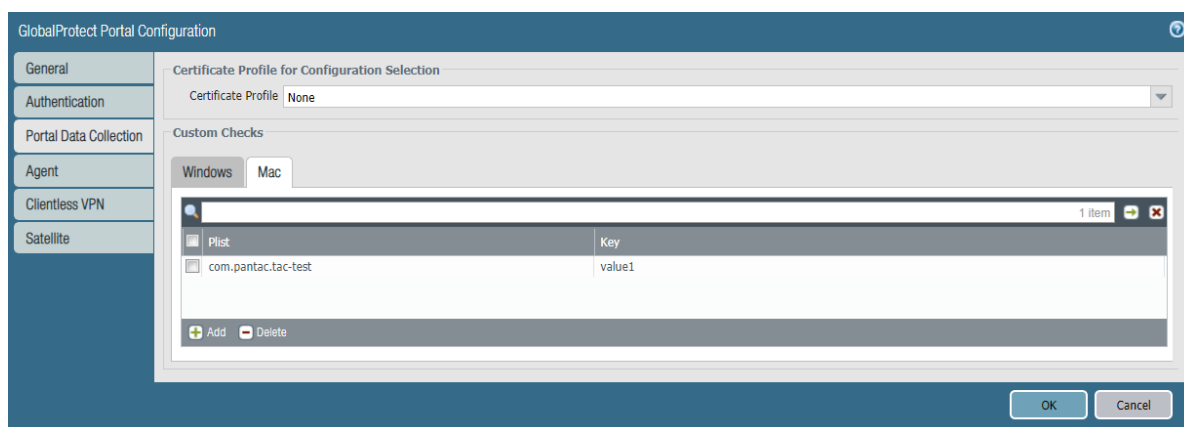
STEP 2 | Set up access to the GlobalProtect portal.

STEP 3 | Define the data that the GlobalProtect app collects from connecting endpoints after users successfully authenticate to the portal.

- To collect registry data from Windows endpoints, select **Windows** and then **Add** the **Registry Key** and corresponding **Registry Value**.



- To collect plist data from macOS endpoints, select **Mac** and then **Add** the **Plist** key and corresponding **Key** value.



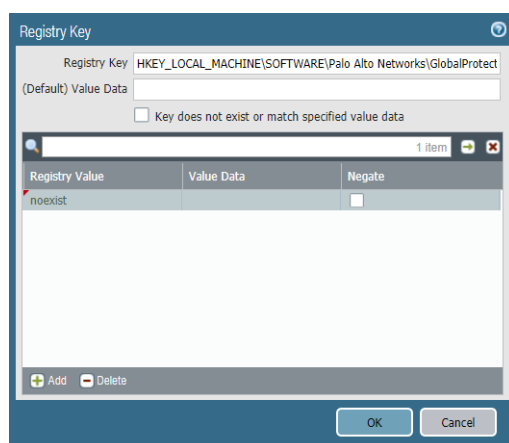
STEP 4 | Define an agent configuration on the portal.

STEP 5 | Add custom [config selection criteria](#) for your agent configuration.

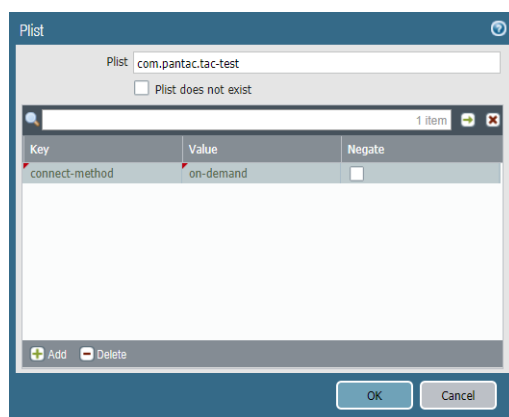
The portal can determine whether an endpoint is managed or unmanaged by verifying the presence of specific software and app settings on the endpoint, as defined in the Windows Registry and macOS plist ([Step 1](#)). After the GlobalProtect app collects data from connecting endpoints (as defined in [Step 3](#)), it sends this data to the portal to match against the custom checks that you specify in the config selection criteria for each agent configuration. If an endpoint matches all config selection criteria for an agent configuration, the portal pushes that agent configuration to the endpoint.

To deliver your agent configuration to connecting endpoints based on custom host information, use the following steps:

1. Select **Config Selection Criteria > Custom Checks**.
2. Enable **Custom Checks** and then define any of the following registry and plist data to match:
 - To check Windows endpoints for a specific registry key, use the following steps:
 1. **Add** a new registry key (**Custom Checks > Registry Key**).
 2. When prompted, enter the **Registry Key** to match.
 3. (**Optional**) To deliver this configuration only if the endpoint does not have the specified registry key or key value, select **Key does not exist or match the specified value data**.
 4. (**Optional**) To deliver this configuration based on specific registry values, **Add** the **Registry Value** and corresponding **Value Data**. To deliver this configuration only if the endpoint does not have the specified **Registry Value** or **Value Data**, select **Negate**.



- To check macOS endpoints for a specific entry in the plist, use the following steps:
 1. **Add** a new plist (**Custom Checks > Plist**).
 2. When prompted, enter the **Plist** name.
 3. **(Optional)** To deliver this configuration only if the endpoint does not have the specified plist, select **Plist does not exist**.
 4. **(Optional)** To deliver this configuration based on specific key-value pairs within the plist, click **Add** and then enter the **Key** and corresponding **Value**. To match only if endpoints do not have the specified key or value, select **Negate**.



STEP 6 | Save the portal configuration.

1. Click **OK** twice.
2. **Commit** your changes.

HIP-Based Policy Enforcement Based on the Endpoint Status

Use the following steps to enforce HIP-based security policies based on the status of connecting endpoints:

STEP 1 | To identify the endpoint status and enforce HIP-based security policies based on the endpoint's machine certificate, [configure a certificate profile](#).

The GlobalProtect gateway uses this certificate profile to match the machine certificate sent by the GlobalProtect app in the HIP report. For a successful match, the machine certificate must be signed and issued by the same CA certificate and (optional) template that you configure in the certificate profile. If you do not configure a template, the machine certificate matches based on only the configured CA certificate.

STEP 2 | To identify the endpoint status and enforce HIP-based security policies based on the presence of the endpoint serial number, [enable group mapping](#).

If an endpoint is managed, you can bind the serial number of the endpoint to the machine account of the endpoint in your directory server (such as Active Directory). The firewall can then pre-fetch the serial numbers for these managed endpoints when it retrieves [group mapping](#) information from the directory server.

In your Group Mapping configuration (**Device** > **User Identification** > **Group Mapping Settings** > *<group-mapping-config>*), you must enable the option to **Fetch list of managed devices**. This allows the firewall to retrieve serial numbers from the directory server.

STEP 3 | (Optional) To identify the endpoint status and enforce HIP-based security policies based on the presence of specific software and settings, you can [deploy app settings using the_Windows Registry or macOS plist](#).

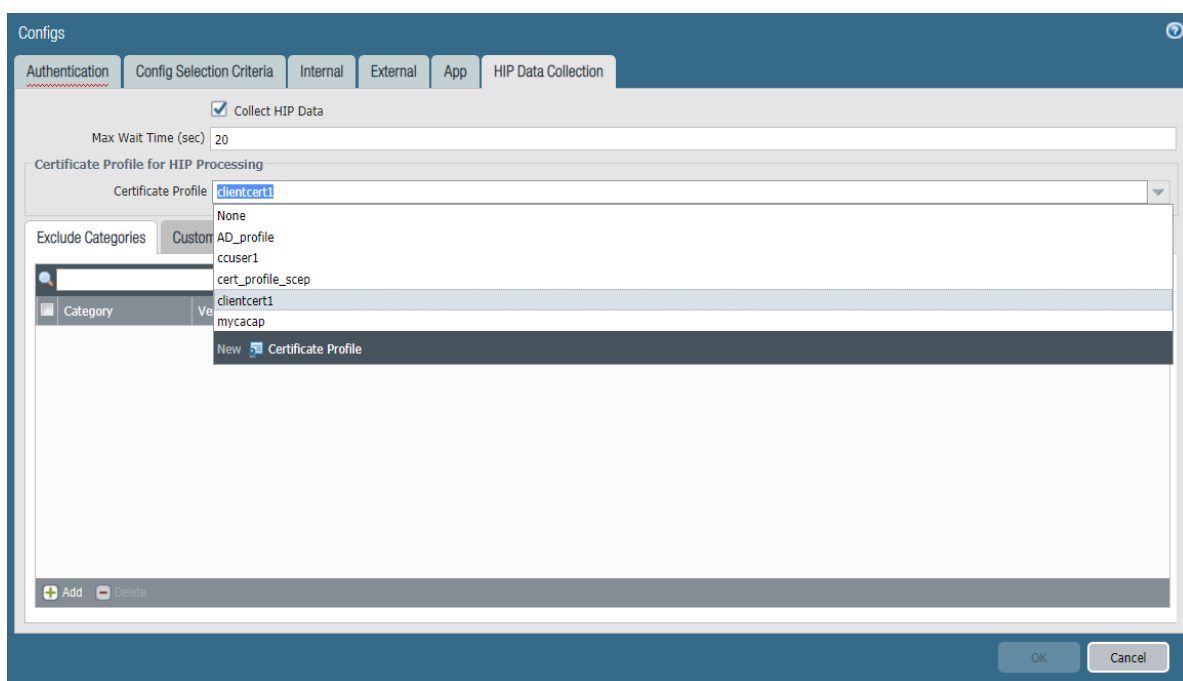
The Windows Registry and macOS plist enable you to deploy app settings directly to endpoints.

STEP 4 | [Set up access to the GlobalProtect_portal](#).

STEP 5 | [Define an agent configuration_on the portal](#).

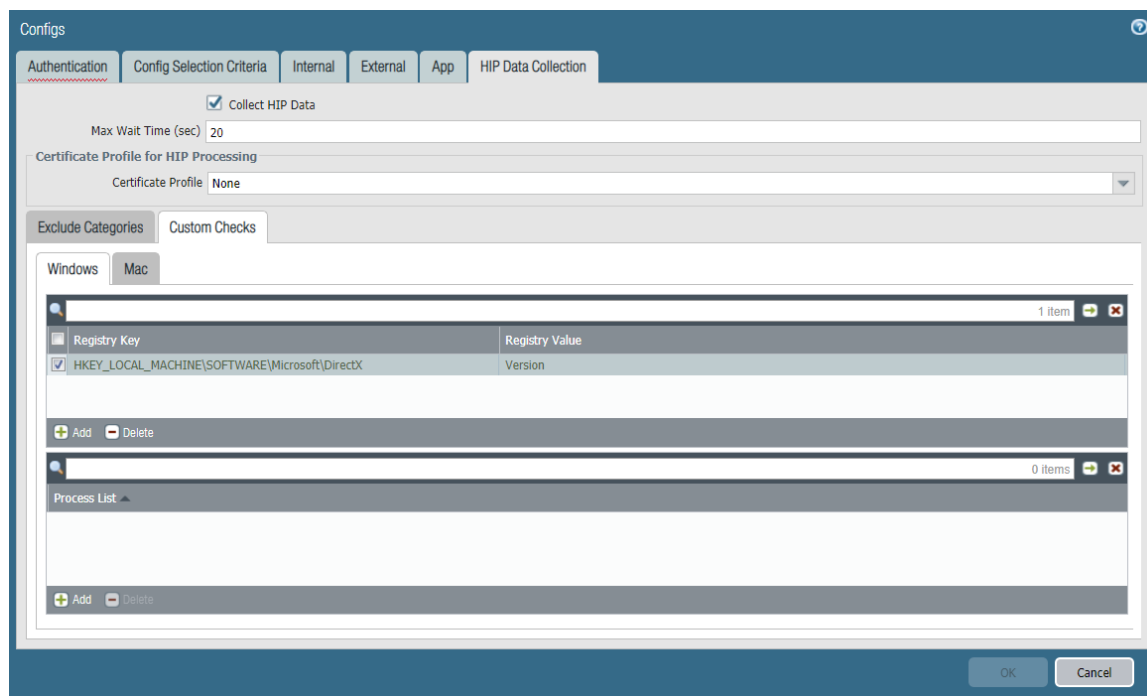
STEP 6 | Enable the GlobalProtect app to [collect HIP data](#) from endpoints.

- To enable the GlobalProtect app to collect machine certificates from endpoints with this agent configuration, select the **Certificate profile** that you configured in [Step 1](#).

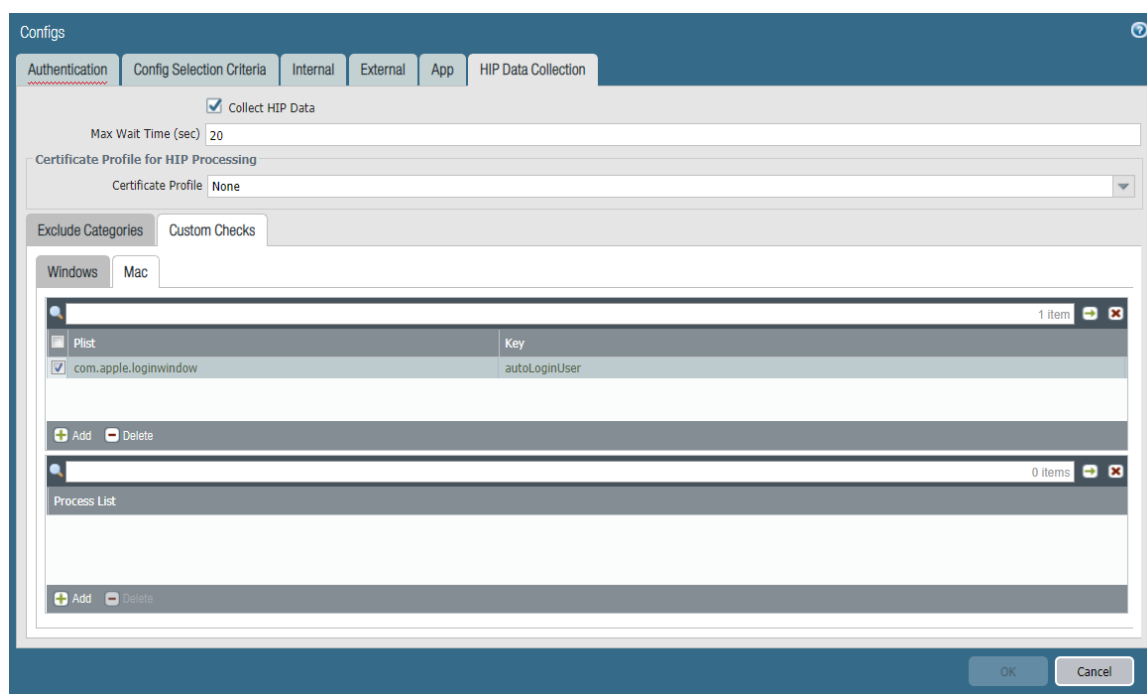


- To enable the GlobalProtect app to collect information about the software and settings that are configured on endpoints with this agent configuration, select **Custom Checks** and configure any of the following options:
- Windows**—Add the **Registry Key** for which you want to collect data. To restrict data collection to a specific value within the **Registry Key**, add the corresponding **Registry Value**.

You can also **Add a Process List** to check for specific processes (software) on Windows endpoints.



- Mac**—Add the **Plist** and corresponding **Key** for which you want to collect data.
- You can also **Add a Process List** to check for specific processes (software) on Windows endpoints.



STEP 7 | Configure a GlobalProtect gateway.

STEP 8 | Configure HIP-based policy enforcement.

When you configure HIP-based policy enforcement, you can create HIP objects to match based on the status of connecting endpoints.

Configure any of the following options in your HIP object to enable HIP matching based on the endpoint status:

- Configure HIP matching based on the managed status of the endpoint:

You can identify the managed status of an endpoint by verifying the presence of the endpoint serial number in the Active Directory or Azure AD. If the serial number exists, the endpoint is managed. If the serial number does not exist, the endpoint is unmanaged.

1. Select **General**.
2. Select **Host Info** to enable matching based on general host information.
3. Configure the HIP object to match based on the **Managed** status of the endpoint:
 - If you set this option to **Yes**, the HIP object matches only if the endpoint is managed.
 - If you set this option to **No**, the HIP object matches only if the endpoint is unmanaged.
 - If you set this option to **None**, the HIP object does not match based on the **Managed** status.

HIP Object

General

Configuration

Name:

☐ Shared

Description:

☒ **Host Info**

Managed:

Domain:

OS:

Client Version:

Host Name:

Host ID:

Serial Number:

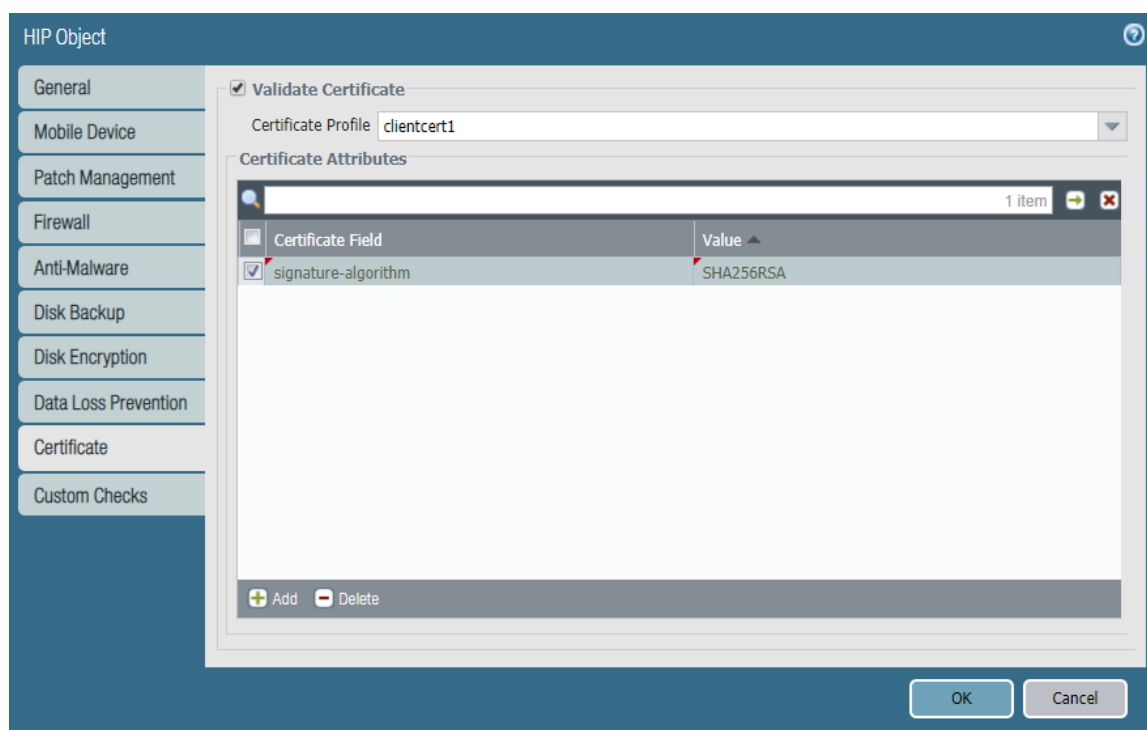
Mobile Device Network Info

Network:

This match criteria applies to mobile devices only.

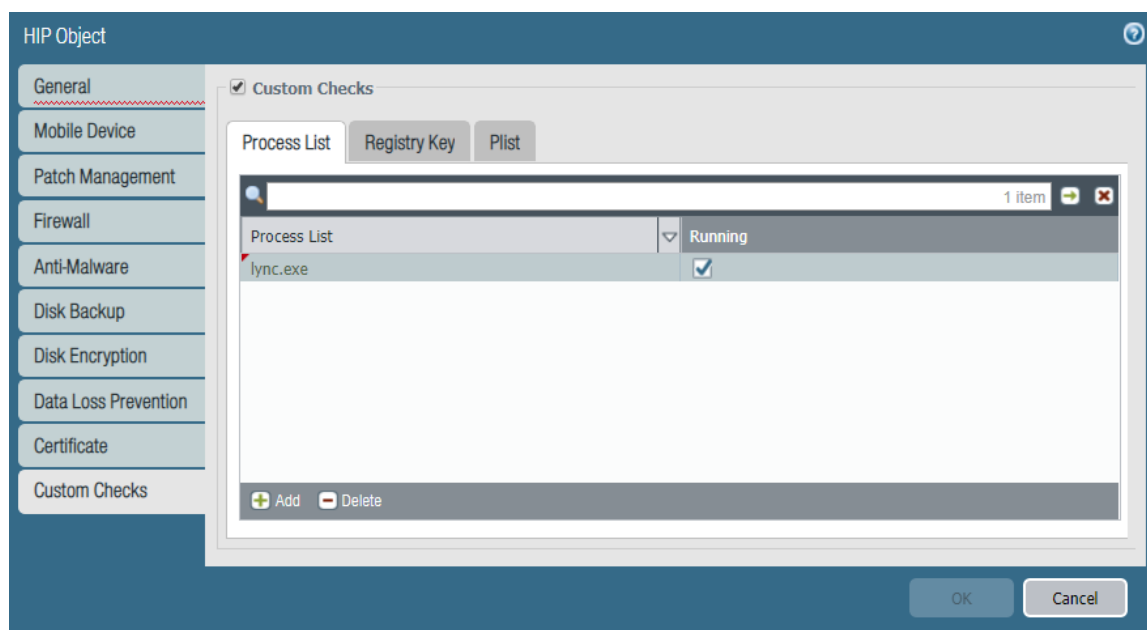
OK Cancel

- Configure HIP matching based on a certificate profile or specific attributes in the endpoint's machine certificate:
 1. Select **Certificate**.
 2. Select **Validate Certificate** to enable matching based on the certificate profile and certificate attributes.
 3. Select the **Certificate Profile** that you configured in [Step 1](#). The GlobalProtect gateway uses this certificate profile to match the machine certificate sent by the GlobalProtect app in the HIP report.
 4. To match based on specific attributes in the endpoint's machine certificate, **Add** the **Certificate Field** and corresponding **Value** in the Certificate Attributes area.

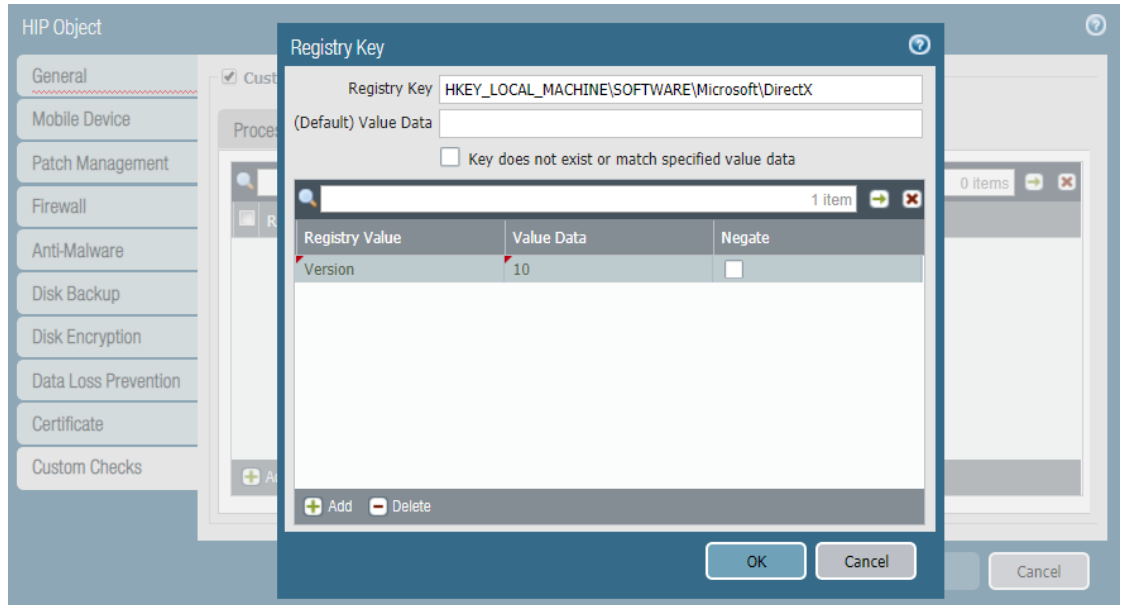


- Configure HIP matching based on the presence of specific software and settings on the endpoint:
 1. Select **Custom Checks**.
 2. Select **Custom Checks** to enable matching based on the presence of software and settings on the endpoint.
 3. To check for a specific process (software) on the endpoint, select **Process List** and then click **Add**. When prompted, enter the process name.

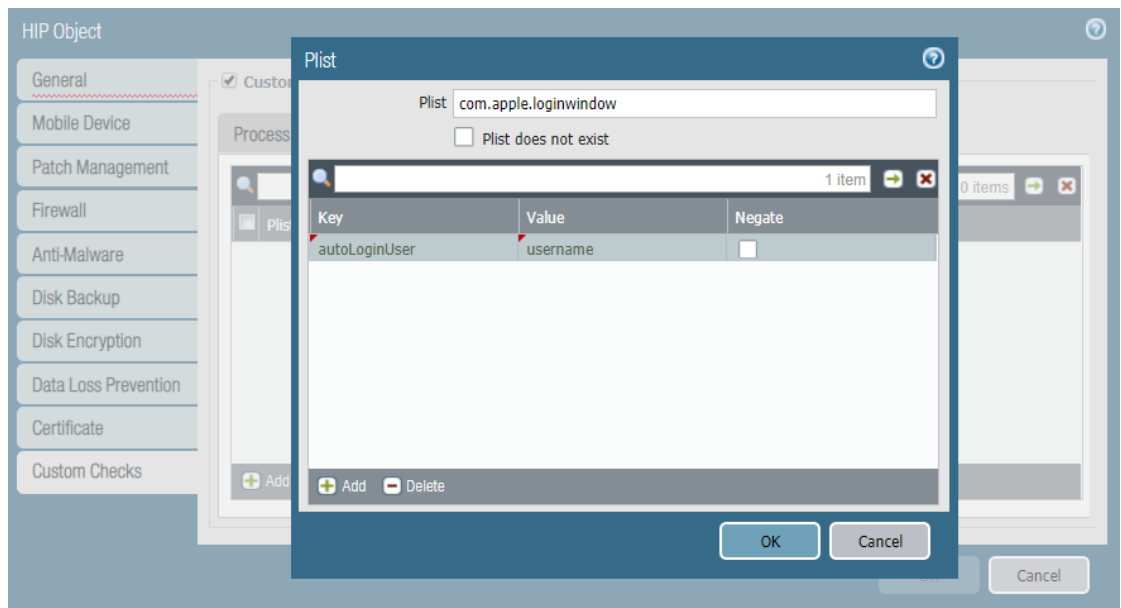
By default, the app checks for running processes; if you want to see if a specific process is not running, clear the **Running** selection. Processes can be operating system level processes or user-space application processes.



4. To check Windows endpoints for a specific registry key, select **Registry Key** and then click **Add**. When prompted, enter the **Registry Key** and then configure any of the following options:
 - To match only the endpoints that lack the specified registry key or key value, select **Key does not exist or match the specified value data**.
 - To match on specific registry values, **Add** the **Registry Value** and corresponding **Value Data**. To match endpoints that do not have the specified value or value data, select **Negate**.



5. To check macOS endpoints for a specific plist entry, select **Plist** and then click **Add**. When prompted, enter the **Plist** name and then configure any of the following options:
 - To match only the endpoints that do not have the specified plist, select **Plist does not exist**.
 - To match on specific key-value pairs within the plist, **Add** the plist **Key** and corresponding **Value**. To match endpoints that do not have the specified key or value, select **Negate**.



STEP 9 | Commit your changes.

HIP Report Redistribution

To ensure consistent Host Information Profile (HIP) policy enforcement and to simplify policy management, the HIP Report Redistribution feature enables you to distribute HIP reports received from the GlobalProtect app—and sent to an internal or external GlobalProtect gateway—to other gateways, firewalls, Dedicated Log Collectors (DLC), and Panorama appliances in the enterprise.

Use HIP report redistribution in the following use cases:

- You want to apply consistent policies to both internal and external GlobalProtect gateways. Previously, you could use only internal gateways to enforce HIP rules for traffic coming from external gateways and had to configure the internal gateways with exception policies to not enforce HIP rules for traffic coming from external gateways; or you could duplicate every HIP profile and policy of every internal gateway on every external gateway to consistently enforce HIP policies.
- You want to apply consistent HIP policies for traffic for a specific user that goes through multiple firewalls. Previously, you only could configure each internal gateway to receive a HIP report from each individual endpoint, which caused delays and excessive traffic load on the firewall.
- You have a distributed enterprise deployment (for example, a retail store with many locations) and you want to use the data center gateways more efficiently.

Users access the internal network from multiple gateways and, at each entry point, the gateway runs HIP and User-ID-based policies. After the users enter the internal network, they access applications in the data center. However, to enforce user and HIP-based policies, you need to configure every data center firewall as an internal GlobalProtect gateway.

After you enable HIP report redistribution, you need to configure only the entry points as internal gateways—you do not need to configure the data center firewalls as internal gateways—to enforce policies based on User-ID and host information.

Use the same firewall and gateway deployment scheme for HIP report redistribution as you do for User-ID redistribution. See [Firewall Deployment for User-ID Redistribution](#) for recommendations and best practices.

Use the following workflow to configure HIP report redistribution:

STEP 1 | [Configure HIP-Based Policy Enforcement](#) for your gateways and firewalls.

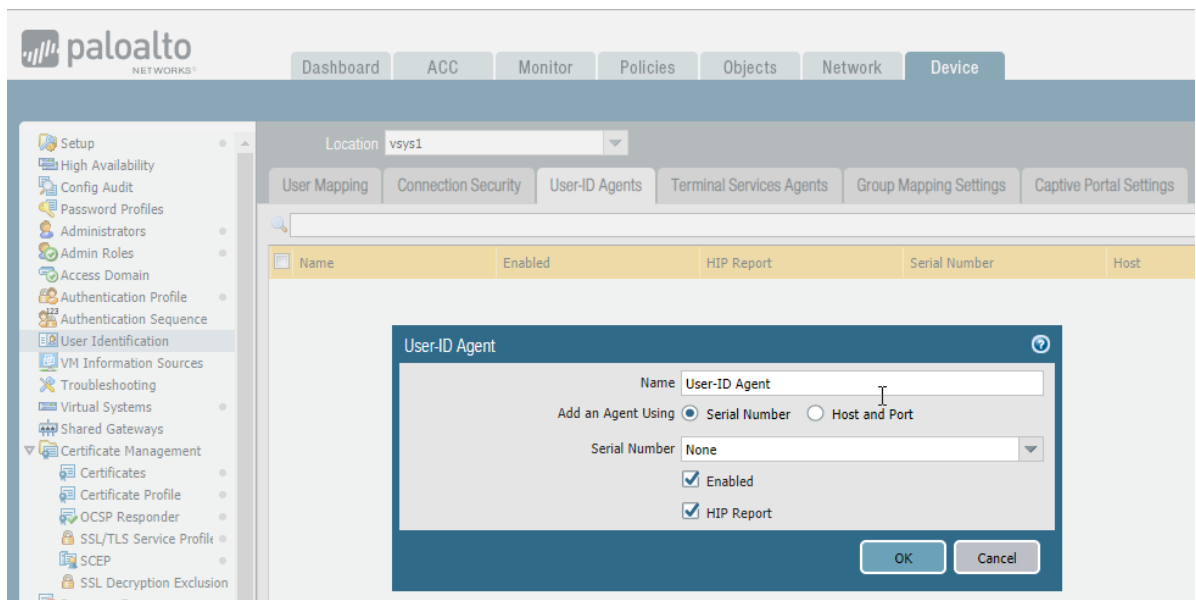
STEP 2 | Configure HIP report redistribution.

1. Select **Device > User Identification > User-ID Agents**.
2. Select an existing or **Add** a new User-ID agent.



The agent must be a Palo Alto Networks next-generation firewall, a GlobalProtect gateway, a DLC, or a Panorama appliance.

3. Select **HIP Report**.



4. Click **OK**.

STEP 3 | Redistribute the HIP reports to your managed Panorama appliances, gateways, firewalls, and virtual systems using the same workflow you use to [Redistribute User-ID Information to Managed Firewalls](#).

DNS Configuration Assignment Based on Users or User Groups

Software Support: PAN-OS 9.0® and later releases

You can now configure GlobalProtect gateways to send different DNS server and DNS suffix configurations to connecting endpoints based on the individual users or users within a specific user group who have logged in to these endpoints. This enhancement reduces the number of gateways and firewalls that you must deploy for your users, as you are no longer required to configure separate gateways for each set of DNS server and DNS suffix configurations. For example, you can configure the Partner 1 user group to use a specific DNS server and set of DNS suffixes. On the same gateway, you can then configure the Partner 2 user group to use a different DNS server and different set of DNS suffixes.

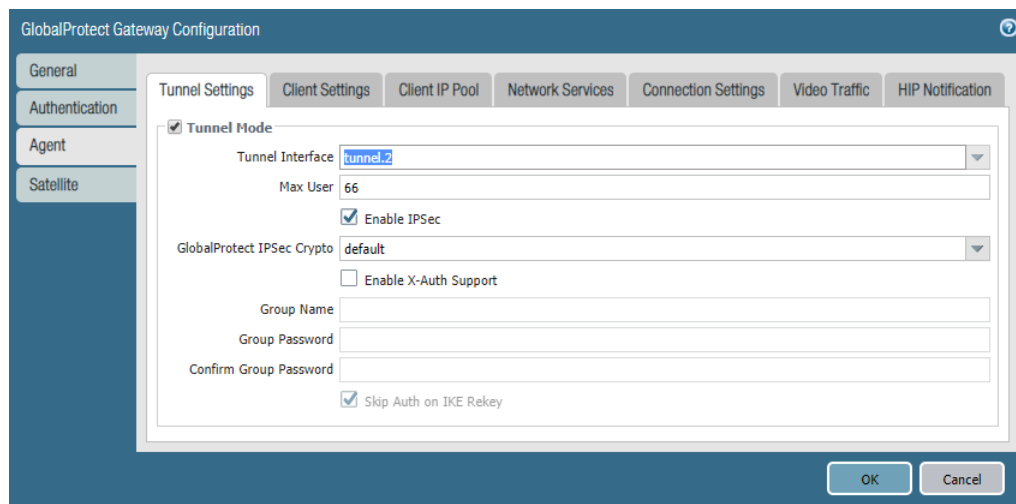
Use the following steps to configure a DNS server or DNS suffix based on a user or user group:

STEP 1 | (Optional) Map users to groups.

You can map users to user groups to define policy rules and configurations based on group membership instead of individual users.

STEP 2 | Configure a GlobalProtect gateway.

STEP 3 | Enable tunneling and then configure the tunnel parameters.



The screenshot shows the 'GlobalProtect Gateway Configuration' dialog box with the 'Tunnel Settings' tab selected. The 'Tunnel Mode' checkbox is checked. The 'Tunnel Interface' dropdown is set to 'tunnel.2'. The 'Max User' field is set to '66'. The 'Enable IPsec' checkbox is checked. The 'GlobalProtect IPsec Crypto' dropdown is set to 'default'. The 'Enable X-Auth Support' checkbox is unchecked. The 'Group Name', 'Group Password', and 'Confirm Group Password' fields are empty. The 'Skip Auth on IKE Rekey' checkbox is checked. The 'OK' and 'Cancel' buttons are at the bottom right.

STEP 4 | Configure a client settings configuration.

STEP 5 | Specify the config selection criteria (including the user or user group) for your client settings configuration.

The config selection criteria indicates the criteria that users must match against when connecting to a GlobalProtect gateway. If a user matches all specified criteria (**Source User**, **OS**, and **Source Address**), the gateway deploys this client settings configuration to the user.

Configs

Config Selection Criteria Authentication Override IP Pools Split Tunnel Network Services

Name default

Config Selection Criteria

select

☒ Any

Source User

☒ cc1

☒ hle

Add Delete

Source Address

Region

IP Address

Add Delete

The configuration must match User and OS and either Region or IP Address if specified.

OK Cancel

STEP 6 | Configure the DNS settings for your client settings configuration.

- Specify the IP address of the **DNS Server** to which the GlobalProtect app with this client settings configuration sends DNS queries. You can add multiple DNS servers by separating each DNS server with a comma.

Configs

Config Selection Criteria Authentication Override IP Pools Split Tunnel Network Services

DNS Server 8.8.8.8, 10.1.4.10

DNS Suffix Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)

OK Cancel

- Specify the **DNS Suffix** that the endpoint should use locally when an unqualified hostname, which the endpoint cannot resolve, is entered. You can enter multiple DNS suffixes (up to 100) by separating each suffix with a comma.


Configs

Config Selection Criteria Authentication Override IP Pools Split Tunnel Network Services

DNS Server Enter comma-separated DNS server for client (e.g. 192.168.75.1, 2001:aa::1-2001:aa::10)

DNS Suffix domain1.local, domain2.local, domain3.local

OK Cancel

 If you configure at least one DNS server or DNS suffix at the client level (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Client Settings > <client-settings-config> > Network Services), the gateway sends the client level configuration

for both the DNS server and DNS suffix to the endpoint. This occurs even when you configure gateway level (global) DNS servers and DNS suffixes.

If you do not configure any DNS servers or DNS suffixes at the client level, the gateway sends the global DNS servers and DNS suffixes to the endpoint, if configured (Network > GlobalProtect > Gateways > <gateway-config> > Agent > Network Services).

STEP 7 | Save the gateway configuration.

1. Click **OK** twice.
2. **Commit** your changes.

Tunnel Restoration and Authentication Cookie Usage Restrictions

Software Support: PAN-OS® 9.0 and later releases

If you configure GlobalProtect to enable automatic restoration of the VPN connection after disconnecting and cookie usage for transparent authentication, you can now enforce additional restrictions to provide enhanced security:

- **Automatic restoration of SSL VPN tunnels at the gateway level:**

You can now configure automatic restoration of SSL VPN tunnels at the gateway level. This can be useful if you want to prevent the GlobalProtect app from automatically reestablishing the VPN tunnel only for specific gateways, such as external gateways.

- **Source IP enforcement for authentication cookies:**

You can now configure the GlobalProtect portal or gateway to accept cookies from endpoints only when the IP address of the endpoint matches the original source IP addresses for which the cookie was issued or the IP address of the endpoint matches a specific network IP address range. You can define the network IP address range using a CIDR subnet mask, such as /24 or /32. For example, if an authentication cookie was originally issued to an endpoint with a public source IP address of 201.109.11.10, and the subnet mask of the network IP address range is set to /24, the authentication cookie is subsequently valid on endpoints with public source IP addresses within the 201.109.11.0/24 network IP address range.



These settings provide a more restricted user connection experience.

- Use the following steps to configure automatic VPN tunnel restoration for a GlobalProtect gateway:
 1. [Configure a GlobalProtect gateway.](#)
 2. [Configure automatic restoration of the SSL VPN tunnel.](#)
 - To prevent the GlobalProtect app from automatically reestablishing the VPN tunnel for this gateway, select the option to **Disable Automatic Restoration of SSL VPN**.

GlobalProtect Gateway Configuration

General Authentication Agent Satellite

Tunnel Settings Client Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification

Timeout Configuration

Login Lifetime Days 30

Inactivity Logout Hours 3

Disconnect On Idle Minutes 180

Users are logged out of GlobalProtect when the gateway does not receive a HIP check from the GlobalProtect app in the specified amount of time.

Users are logged out of GlobalProtect when the GlobalProtect app has not sent traffic through the VPN tunnel in the specified amount of time. (This setting is only applicable to clients using the on-demand Connect Method to connect to GlobalProtect).

Authentication Cookie Usage Restrictions

☒ **Disable Automatic Restoration of SSL VPN**

If the Automatic Restoration of VPN Connection setting is enabled in the GlobalProtect Portal, this setting can be used to disable it for this gateway.

☐ **Restrict Authentication Cookie Usage(for Automatic Restoration of VPN tunnel or Authentication Override)**

to:

☒ The original Source IP for which the authentication cookie was issued ☐ The original Source IP network range

Specify using a netmask, the range of source IP addresses from which the authentication cookie can be used.

OK Cancel

- To allow the GlobalProtect app to automatically reestablish the VPN tunnel for this gateway, clear the option to **Disable Automatic Restoration of SSL VPN** (default).

GlobalProtect Gateway Configuration

General Authentication Agent Satellite

Tunnel Settings Client Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification

Timeout Configuration

Login Lifetime Days 30

Inactivity Logout Hours 3

Disconnect On Idle Minutes 180

Users are logged out of GlobalProtect when the gateway does not receive a HIP check from the GlobalProtect app in the specified amount of time.

Users are logged out of GlobalProtect when the GlobalProtect app has not sent traffic through the VPN tunnel in the specified amount of time. (This setting is only applicable to clients using the on-demand Connect Method to connect to GlobalProtect).

Authentication Cookie Usage Restrictions

☐ **Disable Automatic Restoration of SSL VPN**

If the Automatic Restoration of VPN Connection setting is enabled in the GlobalProtect Portal, this setting can be used to disable it for this gateway.

☐ **Restrict Authentication Cookie Usage(for Automatic Restoration of VPN tunnel or Authentication Override)**

to:

☒ The original Source IP for which the authentication cookie was issued ☐ The original Source IP network range

Specify using a netmask, the range of source IP addresses from which the authentication cookie can be used.

OK Cancel

3. Save the gateway configuration.

- Click **OK**.
- Commit** your changes.

- Use the following steps to configure source IP address enforcement for authentication cookies:
 - [Configure a GlobalProtect gateway.](#)
 - [Configure authentication cookie usage restrictions](#)

To configure the GlobalProtect portal or gateway to accept cookies only from endpoints with a specific IP address or within a specified IP address range, enable the option to **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override)** to, and then configure one of the following conditions:

- If you select **The original Source IP for which the authentication cookie was issued**, the authentication cookie is valid only if the public source IP address of the endpoint attempting to use the cookie is the same public source IP address of the endpoint to which the cookie was originally issued.

GlobalProtect Gateway Configuration

General Authentication Agent Satellite

Tunnel Settings Client Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification

Timeout Configuration

Login Lifetime Days 30

Inactivity Logout Hours 3

Disconnect On Idle Minutes 180

Users are logged out of GlobalProtect when the gateway does not receive a HIP check from the GlobalProtect app in the specified amount of time.

Users are logged out of GlobalProtect when the GlobalProtect app has not sent traffic through the VPN tunnel in the specified amount of time. (This setting is only applicable to clients using the on-demand Connect Method to connect to GlobalProtect).

Authentication Cookie Usage Restrictions

☐ Disable Automatic Restoration of SSL VPN
If the Automatic Restoration of VPN Connection setting is enabled in the GlobalProtect Portal, this setting can be used to disable it for this gateway.

☒ Restrict Authentication Cookie Usage(for Automatic Restoration of VPN tunnel or Authentication Override) to:

☒ The original Source IP for which the authentication cookie was issued ☐ The original Source IP network range

Specify using a netmask, the range of source IP addresses from which the authentication cookie can be used.

OK Cancel

- If you select **The original Source IP network range**, the authentication cookie is valid only if the public source IP address of the endpoint attempting to use the cookie is within the designated network IP address range. Enter a **Source IPv4 Netmask** or **Source IPv6 Netmask** to define the subnet mask of the network IP address range for which the authentication cookie is valid (for example, 32 or 128).

GlobalProtect Gateway Configuration

General Authentication Agent Satellite

Tunnel Settings Client Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification

Timeout Configuration

Login Lifetime Days 30

Inactivity Logout Hours 3

Disconnect On Idle Minutes 180

Users are logged out of GlobalProtect when the gateway does not receive a HIP check from the GlobalProtect app in the specified amount of time.

Users are logged out of GlobalProtect when the GlobalProtect app has not sent traffic through the VPN tunnel in the specified amount of time. (This setting is only applicable to clients using the on-demand Connect Method to connect to GlobalProtect).

Authentication Cookie Usage Restrictions

☐ Disable Automatic Restoration of SSL VPN
If the Automatic Restoration of VPN Connection setting is enabled in the GlobalProtect Portal, this setting can be used to disable it for this gateway.

☒ Restrict Authentication Cookie Usage(for Automatic Restoration of VPN tunnel or Authentication Override) to:

☐ The original Source IP for which the authentication cookie was issued ☒ The original Source IP network range

Source IPv4 Netmask 32

Source IPv6 Netmask [0 - 128]

Specify using a netmask, the range of source IP addresses from which the authentication cookie can be used.

OK Cancel

3. Save the gateway configuration.

1. Click **OK**.
2. **Commit** your changes.

Mixed Authentication Method Support for Certificates or User Credentials

Software Support: PAN-OS® 9.0 and later releases

A single GlobalProtect portal or gateway can now support multiple combinations of authentication methods with user credentials and/or client certificates. You can define whether user credentials and client certificates are required for portal or gateway authentication within each client authentication configuration. For example, you can configure Windows and macOS users to authenticate to a portal or gateway using both their Active Directory (AD) user credentials and a client certificate. On the same portal or gateway, you can then configure Android or iOS users to authenticate using either their AD user credentials or a client certificate.

Use the following steps to configure a GlobalProtect portal or gateway to authenticate users with user credentials and/or client certificates:

STEP 1 | (Optional) To enable users to authenticate to a GlobalProtect portal or gateway using a client certificate, [configure a certificate profile](#).

The portal or gateway uses this certificate profile to match the client certificate sent by the GlobalProtect app. For a successful match, the client certificate must be signed and issued by the same CA certificate and (optional) template that you configure in the certificate profile. If you do not configure a template, the client certificate matches based on only the configured CA certificate.

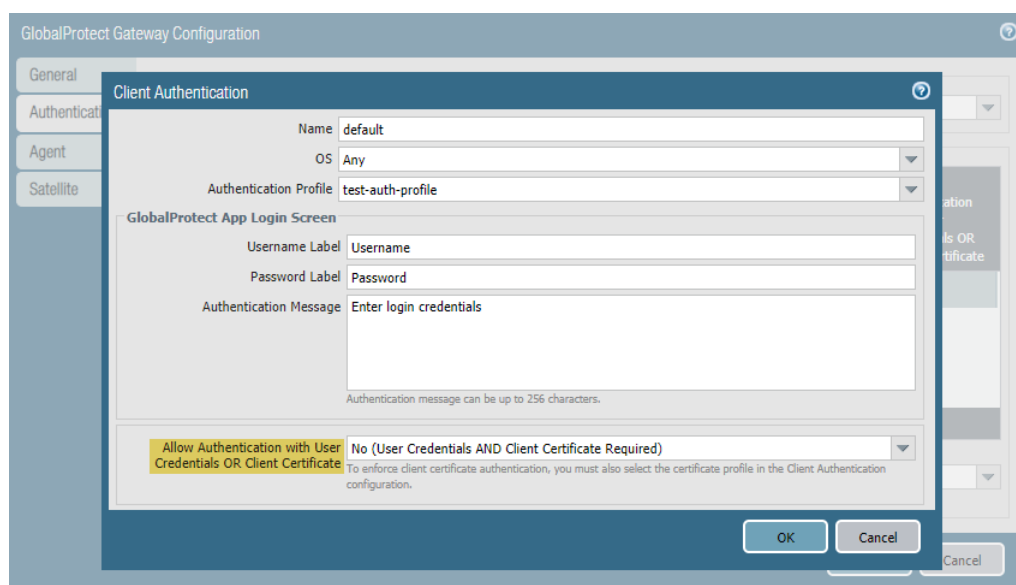
STEP 2 | (Optional) To enable users to authenticate to a GlobalProtect portal or gateway using their user credentials, [configure an authentication profile](#).

The authentication profile defines the authentication service that validates user credentials when end users connect to GlobalProtect.

STEP 3 | [Set up access to a GlobalProtect portal](#) or [configure a GlobalProtect gateway](#).

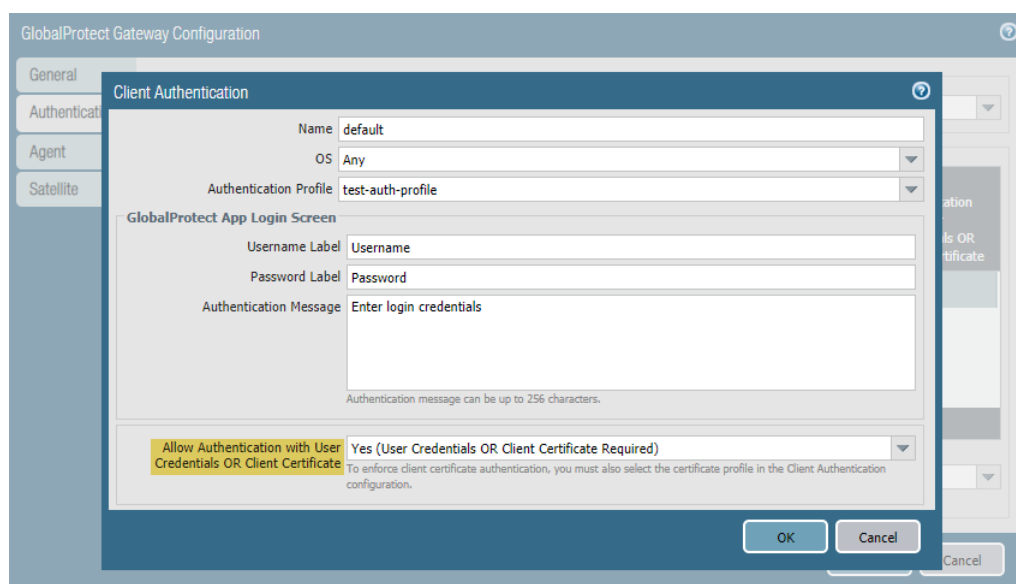
STEP 4 | [Specify how the portal or gateway authenticates users](#).

- From your client authentication configuration (**Network > GlobalProtect > Portals > <portal-config> > Authentication > <client-authentication-config>**), you can specify whether users can authenticate to the portal or gateway using credentials and/or client certificates by selecting one of the following options:
 - To require users to authenticate to the portal or gateway using both user credentials AND a client certificate, set the **Allow Authentication with User Credentials OR Client Certificate** option to **No (User Credentials AND Client Certificate Required)** (default).



- To allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, set the **Allow Authentication with User Credentials OR Client Certificate** option to **Yes (User Credentials OR Client Certificate Required)**.

When you set this option to **Yes**, the portal or gateway first checks the endpoint for a client certificate. If the endpoint does not have a client certificate or you do not configure a certificate profile for your client authentication configuration, the endpoint user can then authenticate to the portal or gateway using his or her user credentials.



- From your client authentication configuration (**Network > GlobalProtect > Portals > <portal-config> > Authentication > <client-authentication-config>**), you can enable users to authenticate to the portal or gateway using credentials by selecting the **Authentication Profile** that you configured in [Step 2](#).
- If you want to require users to authenticate to the portal or gateway using both user credentials AND a client certificate, both the **Authentication Profile** and [Certificate Profile](#) are required.
- If you want to allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, and you select a [Certificate Profile](#) for user authentication, the **Authentication Profile** is optional.

- If you want to allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, but you do not select a [Certificate Profile](#) for user authentication (or you set the **Certificate Profile** to **None**), the **Authentication Profile** is required.
- From your portal authentication configuration (**Network > GlobalProtect > Portals > <portal-config> > Authentication**), you can enable users to authenticate to the portal or gateway using a client certificate by selecting the **Certificate Profile** that you configured in [Step 1](#). The portal uses this certificate profile to match the client certificate on connecting endpoints. A valid client certificate must be pre-deployed on all endpoints.
- If you want to require users to authenticate to the portal or gateway using both user credentials AND a client certificate, both the **Certificate Profile** and [Authentication Profile](#) are required.
- If you want to allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, and you select an [Authentication Profile](#) for user authentication, the **Certificate Profile** is optional.
- If you want to allow users to authenticate to the portal or gateway using either user credentials OR a client certificate, and you do not select an [Authentication Profile](#) for user authentication, the **Certificate Profile** is required.
- If you do not configure any [Authentication Profiles](#) that match a specific OS, the **Certificate Profile** is required.



If you allow users to authenticate to the portal using either user credentials OR a client certificate, do not select a Certificate Profile with the Username Field set to None.

GlobalProtect Gateway Configuration

General

Authentication

Agent

Satellite

Server Authentication

SSL/TLS Service Profile: ssltls_gp_new

Client Authentication

Name	OS	Authentication Profile	Username Label	Password Label	Authentication Message	Allow Authentication with User Credentials OR Client Certificate
default	Any	test-auth-profile	Username	Password	Enter login credentials	No

+ Add - Delete Clone Move Up Move Down

Certificate Profile: cert_profile_client

For the certificate profile to apply to a Client Authentication configuration, you must also select Enforce Client Certificate.

OK Cancel

STEP 5 | Save the portal or gateway configuration.

1. Click **OK**.
2. **Commit** your changes.

Pre-Logon Followed by Two-Factor Authentication

Software Support: Starting with GlobalProtect™ App 5.0

OS Support: macOS 10.9 and later releases and Windows 7 and 10

The GlobalProtect app for Windows and Mac endpoints now supports pre-logon followed by two-factor authentication for user login. When an endpoint boots up and Internet is readily available, GlobalProtect establishes a pre-logon tunnel using the machine certificate on the endpoint. After the pre-logon tunnel is established, the user can log in to the endpoint and authenticate to GlobalProtect using the [configured two-factor authentication method](#). If authentication is successful on Windows endpoints, the pre-logon tunnel is seamlessly renamed to User tunnel and the GlobalProtect connection is established. If authentication is successful on Mac endpoints, a new tunnel is created and the GlobalProtect connection is established.

Use the following steps to configure the GlobalProtect app to use pre-logon followed by two-factor authentication for user login:

[STEP 1 | Configure remote access VPN with pre-logon.](#)

[STEP 2 | Set up two-factor authentication.](#)

Pre-Logon Followed by SAML Authentication

Software Support: Starting with GlobalProtect™ App 5.0 and with PAN-OS® 8.0 and later releases

OS Support: macOS 10.9 and later releases and Windows 7 and 10

The GlobalProtect app for Windows and Mac endpoints now supports pre-logon followed by SAML authentication for user login. When an endpoint boots up and Internet is readily available, GlobalProtect establishes a pre-logon tunnel using the machine certificate on the endpoint. After the pre-logon tunnel is established, the user can log in to the endpoint and authenticate to GlobalProtect using the configured SAML identity provider (IDP). If SAML authentication is successful on Windows endpoints, the pre-logon tunnel is seamlessly renamed to User tunnel and the GlobalProtect connection is established. If SAML authentication successful on Mac endpoints, a new tunnel is created and the GlobalProtect connection is established.

Use the following steps to configure the GlobalProtect app to use pre-logon followed by SAML authentication for user login:

[STEP 1 | Configure remote access VPN with pre-logon.](#)

[STEP 2 | Set up SAML authentication.](#)

GlobalProtect Gateway and Portal Location Configuration

Software Support: Starting with GlobalProtect™ App 5.0 and with PAN-OS® 9.0 and later releases

You can now configure a label to identify the physical location of GlobalProtect gateways and portals using the CLI or the XML API. The GlobalProtect app displays the location label for the gateway to which users connect. For Clientless VPN, the portal landing page displays the physical location of the portal to which Clientless VPN users are logged in.



If you do not configure the gateway or portal location, the GlobalProtect app or Clientless VPN portal landing page displays an empty location field.

When end users experience unusual behavior, such as poor network performance, they can provide the location information to their support or Help Desk professionals to assist with troubleshooting. They can also use this location information to determine their proximity to the portal or gateway. Based on their proximity, they can evaluate whether they need to switch to a closer portal or gateway.

Refer to the [GlobalProtect App 5.0 New Features Guide](#) for more information on gateway and portal location visibility for end users.

CLI

Use the following CLI command to specify the physical location of the firewall on which you configured the portal and/or gateway:

```
username@hostname> set deviceconfig setting global-protect location <location>
```

XML API

Use the following XML API to specify the physical location of the firewall on which you configured the portal and/or gateway:

- **devices**—name of the firewall on which you configured the portal and/or gateway
- **location**—location of the firewall on which you configured the portal and/or gateway

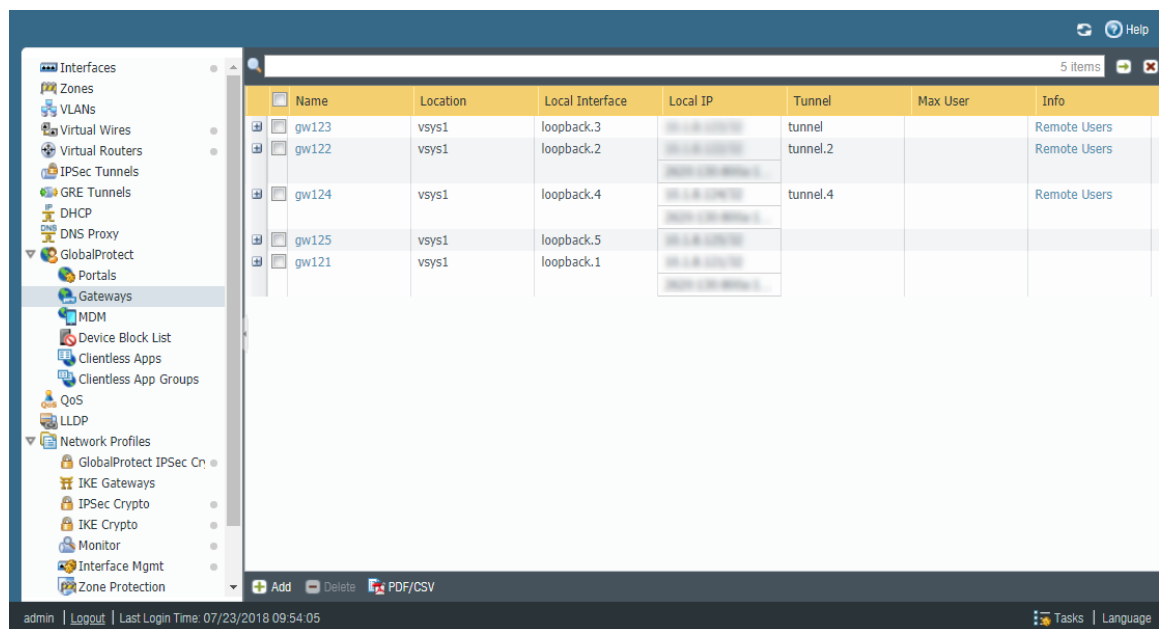
```
curl -k -F file=@filename.txt -g 'https://<firewall>/api/?  
key=<apikey>&type=config&action=set&xpath=/config/devices/  
entry[@name='<device-name>']/deviceconfig/setting/global-  
protect&element=<location><location-string></location>'
```

User Location Visibility on GlobalProtect Gateways and Portals

Software Support: PAN-OS® 9.0 and later releases

You can now identify the source regions from where end users are connected to GlobalProtect. The user information on the GlobalProtect gateway provides the locations of end users who connect to the gateway. The user information on the GlobalProtect portal provides the locations of Clientless VPN users who log in to the Clientless VPN portal. This enhancement provides improved reporting and user activity analysis for end users who are currently connected to GlobalProtect or have previously connected to GlobalProtect (gateways only).

- Use the following steps to view the source regions of users who are currently connected to a gateway or have previously connected to a gateway:
 1. Open the user information for a GlobalProtect gateway.
 1. Select **Network > GlobalProtect > Gateways**.
 2. From the gateway configuration list, select **Remote Users** for the gateway for which you want to view user information.



2. In the User Information dialog, select one of the following tabs to view the **Source Region** of all currently connected users or all previously connected users:
 - **Current User**—Select **Current User** to view the **Source Region** of all users who are currently connected to the gateway.

User Information - gw122 - Santa Clara

Current User Previous User

1 item

Domain	User	Primary Username	Computer	Client	Private IP	Public IP	Source Region	Tunnel Type	Login At	Lifetime (s)	Logout
	jjia	jjia	Acer Chromeb... R11 (CB5-132T / C738T)-unknown	Android 7.1.1			CN	IPSec	Jul.23 14:10:...	25920...	

Refresh

Close

- **Previous User**—Select **Previous User** to view the *Source Region* of all users who have previously connected to the gateway.

User Information - gw122 - Santa Clara

Current User Previous User

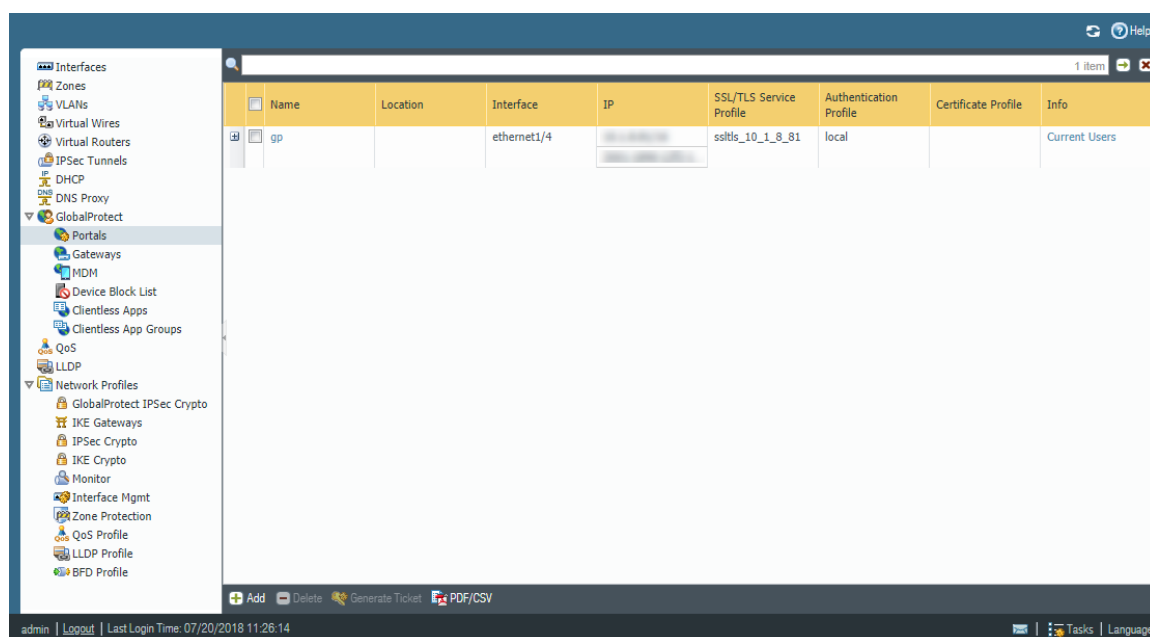
7 items

Domain	User	Primary Username	Computer	Client	Private IP	Public IP	Source Region	Tunnel Type	Login At	Logout At
	yyin	yyin	Yuchen's iPad	Apple iOS 11.4.1			JP	IPSec	Jul.23 14:43:25	Jul.23 14:43:45
	yyin	yyin	DESKTOP-KOHVJHC	Microsoft Windows 10 Enterprise , 64-bit			KR	IPSec	Jul.12 17:18:45	Jul.12 17:26:48
	yyin	yyin	SJCMACG...	Apple Mac OS X 10.13.3			KR	IPSec	Jul.12 16:04:10	Jul.12 16:15:50
	lxia	lxia	DESKTOP-5FQHIM5	Microsoft Windows 10 Enterprise , 64-bit			CN	IPSec	Jul.06 15:53:22	Jul.06 15:53:24

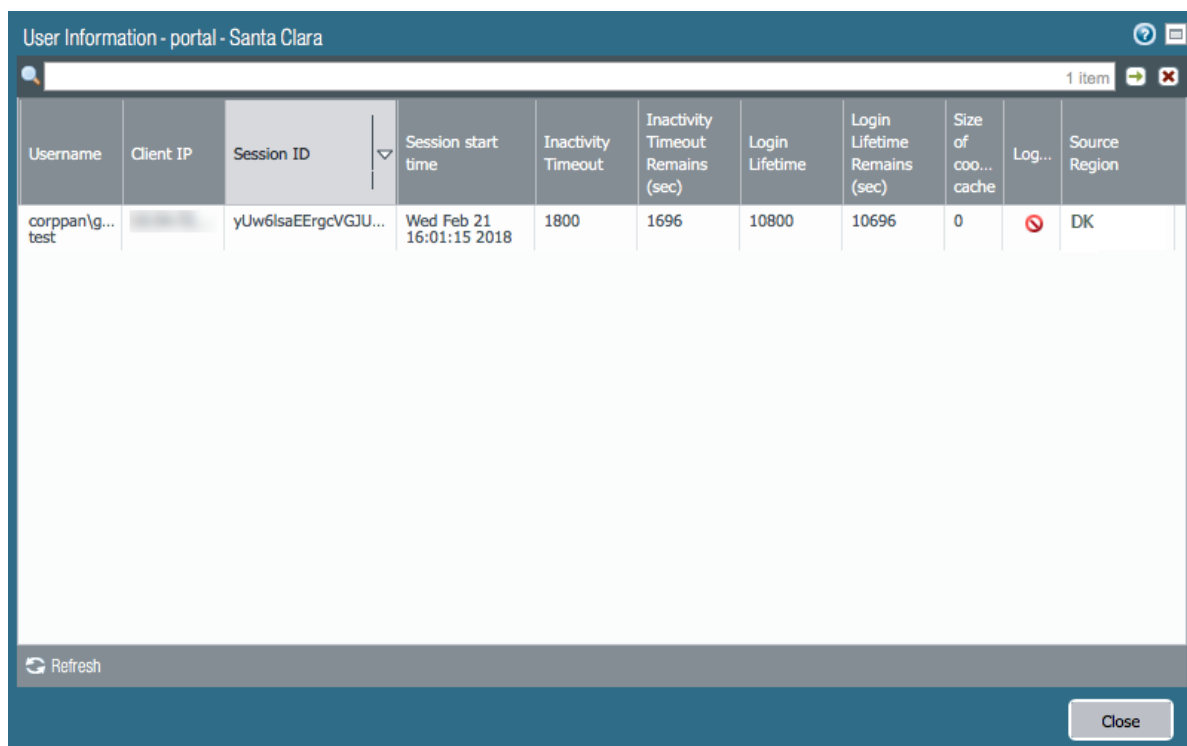
Refresh

Close

- Use the following steps to view the source regions of Clientless VPN users who are currently logged in to a portal:
 1. Open the user information for a GlobalProtect portal.
 1. Select **Network** > **GlobalProtect** > **Portals**.
 2. From the portal configuration list, select **Current Users** for the portal for which you want to view user information.



2. View the **Source Region** of all Clientless VPN users who are currently logged in to the portal.



Concurrent Support for IPv4 and IPv6 DNS Servers

Software Support: Starting with PAN-OS® 9.0

You can now specify up to ten IPv4 and IPv6 DNS servers in a single client settings configuration on the GlobalProtect gateway. This enhancement simplifies the gateway configuration by enabling you to simultaneously assign multiple IPv4 and IPv6 DNS servers to connecting endpoints that receive the specified client settings configuration. For example, if your GlobalProtect deployment supports both IPv4 and IPv6 connections, you will need to specify a separate set of primary and secondary DNS servers for each IP address type in order to resolve both IPv4 and IPv6 DNS queries. By specifying both IPv4 and IPv6 DNS servers in the same client settings configuration, the GlobalProtect app can resolve both IPv4 and IPv6 queries over the VPN tunnel after establishing a connection.

Use the following steps to specify the DNS servers to which the GlobalProtect app can send DNS queries:

STEP 1 | [Configure a GlobalProtect gateway.](#)

STEP 2 | Enable tunneling.

1. From your gateway configuration (**Network > GlobalProtect > Gateways > <gateway-config>**), select **Agent > Tunnel Settings** to enable **Tunnel Mode**.
2. [Configure the tunnel parameters for the GlobalProtect app.](#)

STEP 3 | [Configure a client settings configuration.](#)

- To specify the DNS servers to which the GlobalProtect app with this client settings configuration can send DNS queries, select **Network Services** and then enter the IP address of the **DNS Server**. You can add up to 10 DNS servers by separating each IP address with a comma.



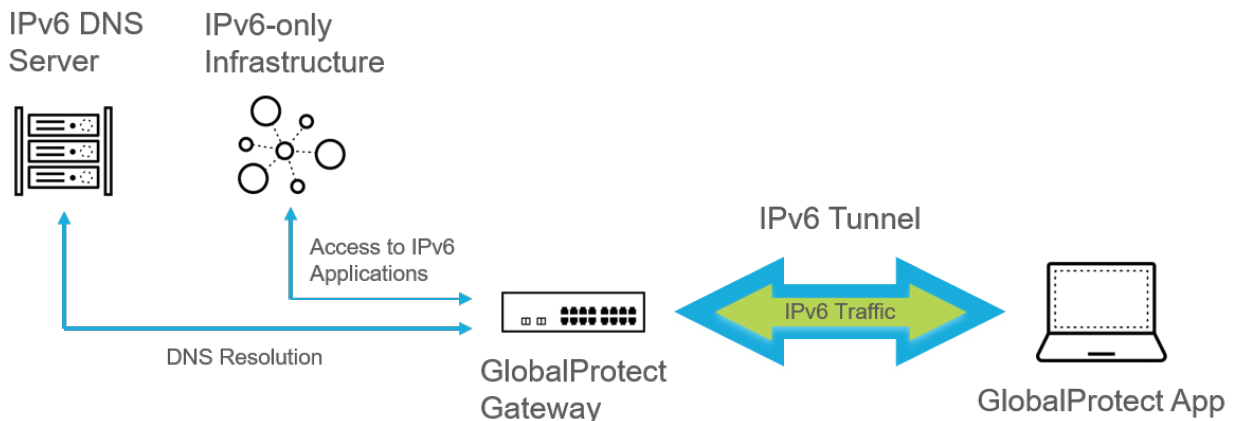
The screenshot shows a configuration window titled "Configs" with a tabbed interface. The "Network Services" tab is selected. It contains two input fields: "DNS Server" with the value "192.168.75.1, 2001:aa::1-2001:aa::10" and "DNS Suffix" with the placeholder text "Enter comma-separated DNS suffix for client (e.g. hr.mycompany.com, mycompany.com)". At the bottom right are "OK" and "Cancel" buttons.

STEP 4 | **Commit** the changes.

Support for IPv6-Only GlobalProtect Deployments

Software Support: Starting with PAN-OS® 9.0

You can now configure GlobalProtect gateways with IP pools that use only IPv6 addresses. With this enhancement, GlobalProtect can support remote access deployments with end-to-end IPv6-only infrastructures. In PAN-OS 8.1 and earlier releases, you are required to configure IP pools with both IPv4 and IPv6 subnets or address ranges in order to assign IPv6 addresses to connecting endpoints.




STEP 1 | [Configure a GlobalProtect gateway.](#)

STEP 2 | Enable tunneling.

1. From your gateway configuration (**Network > GlobalProtect > Gateways > <gateway-config>**), select **Agent > Tunnel Settings** to enable **Tunnel Mode**.
2. [Configure the tunnel parameters for the GlobalProtect app.](#)

STEP 3 | Configure an IPv6-only IP pool.

Use one of the following options to configure an IPv6-only IP pool at either the client level or the gateway level:

-  *You can configure an IP pool at only the client level (**Network > GlobalProtect > Gateways > <gateway-config> > GlobalProtect Gateway Configuration > Agent > Client Settings > <client-setting> > Configs > IP Pools**) or only the gateway level (**Network > GlobalProtect > Gateways > <gateway-config> > GlobalProtect Gateway Configuration > Agent > Client IP Pool**).*
- To assign only IPv6 addresses to connecting endpoints with a specific client settings configuration, configure a client level IPv6-only IP pool:
 1. From your gateway configuration (**Network > GlobalProtect > Gateways > <gateway-config>**), select **Agent > Client Settings**.
 2. Select an existing client settings configuration or **Add** a new one.
 3. Select **IP Pools**.

4. In the IP Pool area, **Add** an IPv6 subnet or address range. To ensure proper routing back to the gateway, you must use a different range of IP addresses from those assigned to existing IP pools on the gateway (if applicable) and to the endpoints that are physically connected to your LAN.

Configs

Config Selection Criteria Authentication Override IP Pools Split Tunnel Network Services

☐ Retrieve Framed-IP-Address attribute from authentication server

Authentication Server IP Pool

Enter IP subnets or ranges to match the Framed IP attribute of the authentication server. Supports IPv4 private/public addresses (e.g. 192.168.74.0/24, 192.168.75.1-192.168.75.100) or IPv6 unique local/public addresses (e.g. 2001:aa::1-2001:aa::10)

+ Add - Delete

These IPs will be added to the firewall's routing table

IP Pool

☒ 2001:aa::1-2001:aa::10

+ Add - Delete Move Up Move Down

These IPs will be added to the firewall's routing table

OK Cancel

5. Click **OK** to save your client settings configuration.
- To assign only IPv6 addresses to all endpoints that connect to the gateway, configure a global IPv6-only IP pool:
 1. From your gateway configuration (**Network > GlobalProtect > Gateways > <gateway-config>**), select **Agent > Client IP Pool**.
 2. In the IP Pool area, **Add** an IPv6 subnet or address range. To ensure proper routing back to the gateway, you must use a different range of IP addresses from those assigned to the endpoints that are physically connected to your LAN.

GlobalProtect Gateway Configuration

General Authentication Agent Satellite

Tunnel Settings Client Settings Client IP Pool Network Services Connection Settings Video Traffic HIP Notification

IP Pool

☒ 2001:aa::1-2001:aa::10

+ Add - Delete Move Up Move Down

These IPs will be added to the firewall's routing table

OK Cancel

STEP 4 | Save your gateway configuration.

1. Click **OK**.
2. **Commit** the changes.

Management Features

- > Enforcement of Rule Description, Tag, and Audit Comment
- > Rule Changes Archive
- > Tag Based Rule Groups
- > Policy Match and Connectivity Tests from the Web Interface
- > Rule Usage Filtering
- > Objects Capacity Improvements on the PA-5220 and PA-3200 Series Firewalls
- > API Key Lifetime
- > PAN-OS REST API for a Simplified Integration Experience
- > Universally Unique Identifiers for Policy Rules
- > Temporary Master Key Expiration Extension
- > Real-Time Enforcement and Expanded Capacities for Dynamic Address Groups

Enforcement of Rule Description, Tag, and Audit Comment

When you periodically review your [policy rules](#), you need to know what the rule is intended to secure, what the change history for the rule is, how to tag rules so that you can organize your policy rule base, and how to locate a specific rule or set of rules. With the [Enforcement of Rule Description, Tag and Audit Comment](#), you can require a description, audit comment, or tag when creating or editing a rule in the policy rule base for auditing, grouping and change tracking for rules in your policy rule base. For uniformity, you can set specific requirements for what the audit comment can include.

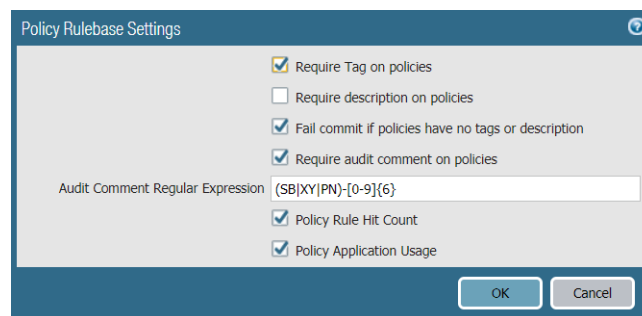
The description, tag, and audit comment are not required by default, and you can select whether a description, tag, audit comment, or any combination of the three is required to successfully add or modify a rule. View the [Rule Changes Archive](#) to view the audit comment history for a selected rule.

STEP 1 | [Log in to the firewall web interface](#).

STEP 2 | Select **Device > Setup > Management** and edit the Policy Rule Base Settings.

STEP 3 | Configure the settings you want to enforce.

STEP 4 | Click **OK** to apply the new policy rulebase settings.



STEP 5 | **Commit** the changes.

STEP 6 | Verify that the new policy rulebase settings are being enforced.

1. Select **Policies** and **Add** a new rule.
2. Confirm that you must add a tag and enter an audit comment to click **OK**.

Security Policy Rule

General Source User Destination Application Service/URL Category Actions

Name test-security-rule

Rule Type universal (default)

Description

Tags

Group Rules By Tag None

Audit Comment

Regex: (SB)XY(PN)-[0-9]{6}

Audit Comment Archive

OK Cancel

Rule Changes Archive

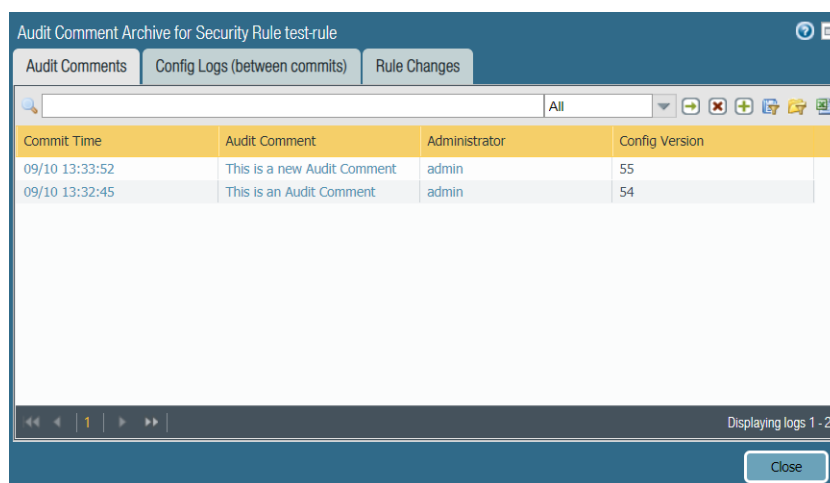
As your rulebase evolves, changes and audit information get lost over time unless they are archived at the time the rule was created or modified. The Rule Changes Archive allows you to [view policy rule usage](#), which contains the audit comment history, configuration log history and enables you to compare rule configuration versions for the selected policy rule. Additionally, the Rule Changes Archive is complimented by [Enforcement of Rule Description, Tag, and Audit Comment](#) by requiring audit comments to be entered when creating or modifying a policy rule.

STEP 1 | Log in to the firewall web interface.

STEP 2 | Select **Policies**, and then select the policy rule to view the **Audit Comment Archive**.

STEP 3 | View the audit history of the selected rule.

1. View the **Audit Comments** to learn which administrator changed what and when, the time the audit comment was committed, the audit comment description, the administrator who added the audit comment, and the configuration version of the policy rule.



Audit Comment Archive for Security Rule test-rule

Tab: Audit Comments

Commit Time	Audit Comment	Administrator	Config Version
09/10 13:33:52	This is a new Audit Comment	admin	55
09/10 13:32:45	This is an Audit Comment	admin	54

Displaying logs 1 - 2

Close

2. View the **Config Logs (between commits)** to display the configuration logs generated by firewalls when the rule is created or modified.



Audit Comment Archive for Security Rule test-rule

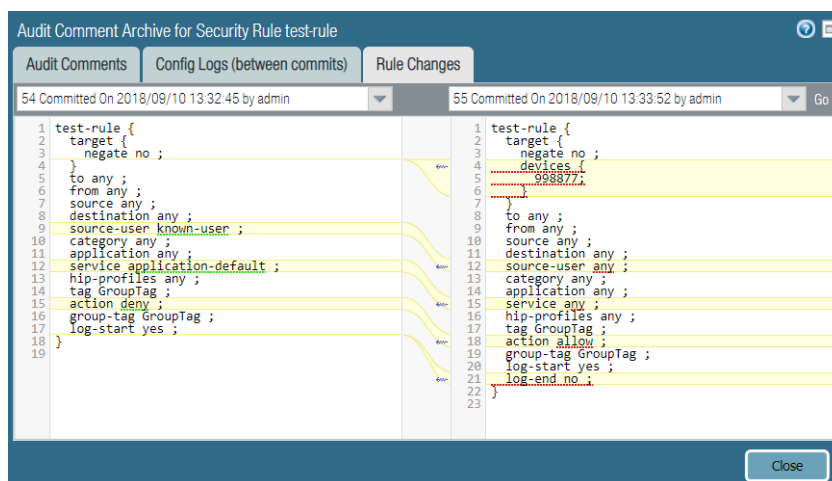
Tab: Config Logs (between commits)

Time	Administrator	Command	Before Change	After Change	Device Name
09/10 13:33:40	admin	edit	test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b10 { source-user [k	test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b10 { target { device	Panorama
09/10 13:32:34	admin	edit	test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b10 { }	test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b10 { log-start yes;	Panorama
09/10 13:22:28	admin	edit	test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b10 { source-user [a	test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b10 { source-user [k	Panorama
07/24 15:35:05	admin	set		security { rules { test-rule 4ceaa5e7-58a3-4071-ba9f-d8ebde721b1	Panorama

Displaying logs 1 - 4

Close

3. View the **Rule Changes** and select the configuration versions for which you want to compare the rule configuration changes. For example, compare two rules to determine when and which administrator modified a security policy rule that allowed previously denied network traffic.



Tag Based Rule Groups

Tags allow you to identify the purpose or function of a rule, and help you better organize your rulebase. PAN-OS 9.0 replaces the tag browser with the Tag Based Rule Groups, and introduces the ability to assign group tags to rules. After your rules are assigned to a tag group, you can view the rulebase as tag groups to visually group rules based on the tagging structure you created. When viewing the rulebase as tag groups, you can perform operational procedures such as adding, deleting or moving the rules in the selected tag group more easily. Viewing the rulebase as tag groups maintains the rule evaluation order. A single tag may appear multiple times throughout the rulebase in order to visually preserve the rule hierarchy.

In order to assign a group tag to a rule, you must first create the tag and assign it to a policy rule on upgrade to PAN-OS 9.0. Policy rules that are already tagged have the first tag automatically assigned as the Group tag. Before upgrading to PAN-OS 9.0, review the tagged rules in your rulebase to ensure rules are correctly grouped upon upgrade. You must manually edit each tag rule and configure the correct Group tag if your rules are grouped incorrectly once you upgrade to PAN-OS 9.0.

STEP 1 | Log in to the firewall web interface.

STEP 2 | Create the tags you want to use for grouping rules.

STEP 3 | Assign a policy rule to a tag group.

1. Create a policy rule. Refer to [Policy](#) in the PAN-OS Admin Guide for more information on creating policy rules.
2. In the **Group Rules by Tag** field, select the tag from the drop-down and click **OK**.
3. **Commit** the changes.

STEP 4 | View your policy rulebase as groups.

1. (**Panorama only**) From the **Device Group** drop-down, select the device group rulebase to view, or view all Shared rules.
2. Click **Policies** and select the rulebase where you created the rules in Step 3.
3. Check the **View Rulebase as Groups** box at the bottom.



Rules not assigned a tag group display as None.

STEP 5 | Perform Group operations as needed.

1. Click **Group** to perform group operations for rules in the selected tag group.
 - (**Panorama only**) **Move rules in group to a different rulebase or device group**—Move all policy rules in the selected tag group to the Pre-Rulebase or Post-Rulebase, or to a different device group.
 - **Change group of all rules**—Move all rules in the selected tag group to a different tag group.
 - **Delete all rules in group**—Delete all rules in the selected tag group.
 - **Clone all rules in group**—Clone all rules in the selected tag group.
2. **Commit** the changes.

Policy Match and Connectivity Tests from the Web Interface

In PAN-OS 9.0, you can perform [policy match and connectivity tests](#) for firewalls from the web interface rather than the CLI. You can easily test the running configuration of your firewalls, and verify traffic and connectivity to ensure policy are matching policy rules as expected to allow or deny traffic, and that firewalls can connect to network resources and external services such as WildFire, Log Collectors, or the Update Server.

STEP 1 | [Log in to the firewall web interface.](#)

STEP 2 | Select **Device > Troubleshooting** to perform a policy match or connectivity test.

STEP 3 | Enter the required information to perform the policy match test.

STEP 4 | **Execute** the policy match test.

STEP 5 | Click the policy rule Test Result in order to view the Result Details for the policy rule that match the test criteria.

Rule Usage Filtering

Over-provisioned access on the firewall can be exploited by attacks, and administrators need to periodically check for outdated and unused rules. [View the policy rule usage](#) to simplify your rule lifecycle management to find unused rules and delete them to maintain an up to date rulebase and improve your security posture. In PAN-OS 9.0, Rule Usage Filtering enables you to quickly filter the selected rulebase based on the rule usage data, as well as additional rule data such as the Created and Modified dates, within a customizable timeframe.

Additionally, use the Rule Usage Filter to [Migrate Port-Based to App-ID Based Security Policy Rules](#). By migrating to app-based rules, administrators can reduce the attack surface and gain visibility into, inspect, and safely enable applications on your network.

STEP 1 | [Log in to the firewall web interface](#).

STEP 2 | Select **Device > Setup > Management**, and navigate to the Policy Rulebase Settings to verify that **Policy Rule Hit Count** is enabled.

STEP 3 | Select **Policies** and then select the policy rulebase to filter.

STEP 4 | In the Policy Optimizer window, click **Rule Usage** to view the rule usage filter.

STEP 5 | Filter rules in the selected rulebase.

1. Select the **Timeframe** you want to filter from the drop-down, or specify a **Custom** timeframe.
2. Select the rule **Usage** to filter.
3. **(Optional)** If you have reset the rule usage data for any rules, check the **Exclude rules reset during the last _ days**, and within how many days the rules were reset in order to be excluded. Rules that were reset before the specified number of days are included in the filtered results.
4. **(Optional)** Specify search filters based on additional rule data, other than the rule usage.
 1. Hover your mouse over the column header, and from the drop-down select **Columns**.
 2. Add any additional columns to want to filter with or to display.
 3. Hover your mouse over the column data that you would like to filter, and select **Filter** from the drop-down. For data that contain dates, select whether to filter using **This date**, **This date or earlier**, or **This date or later**.
 4. Click **Apply Filter**.

Objects Capacity Improvements on the PA-5220 and PA-3200 Series Firewalls

On the PA-5220 and the PA-3200 Series firewalls, the object capacities have been enhanced for the following management objects:

Capacity for	PA-5220			PA-3260			PA-3250			PA-3220		
	New	Old	Change	New	Old	Change	New	Old	Change	New	Old	Change
Security Rule	30,000	20,000	10,000	10,000	5,000	5,000	10,000	5,000	5,000	10,000	2,500	7,500
SSL Rule	3,500	2,000	1,500	1,500	500	1,000	1,500	500	1,000	1,500	250	1,250
App Override Rule	3,500	2,000	1,500	1,500	500	1,000	1,500	500	1,000	1,500	250	1,250
Tunnel Inspection Rule	2,500	2,000	500	1,000	500	500	1,000	500	500	1,000	500	500
Policy Based Forwarding	2,000	2,000	500	1,000	500	500	1,000	500	500	1,000	500	500
Captive Portal	2,000	2,000	0	2,000	1,000	1,000	2,000	1,000	1,000	2,000	1,000	1,000
Max. Security Zones	4,000	2,500	1,500	200	60	140	200	60	140	200	60	140
Max. Address Objects	80,000	40,000	40,000	30,000	10,000	20,000	30,000	10,000	20,000	30,000	5,000	25,000
Max. Address Groups	40,000	4,000	36,000	15,000	1,500	13,500	15,000	1,500	13,500	15,000	1,500	13,500
Max. Services Entries	8,000	2,000	6,000	4,000	1,000	3,000	4,000	1,000	3,000	4,000	1,000	3,000

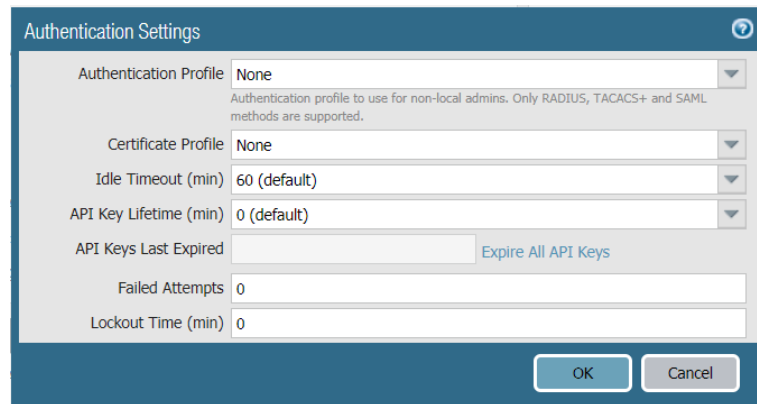
Capacity for	PA-5220			PA-3260			PA-3250			PA-3220		
	New	Old	Change	New	Old	Change	New	Old	Change	New	Old	Change
Max. Services Groups	4000	250	3750	2000	375	1625	2000	375	1625	2000	375	1625
Max. members per Service Group	2500	500	2000	1000	1000	0	1000	1000	0	1000	1000	0
Total IP addresses across Dynamic Address Groups	100,000	100,000	0	10,000	5000	5000	10,000	5000	5000	10,000	5000	5000

API Key Lifetime

To use the API on the firewall and Panorama, you need to [generate an API key](#) that authenticates API calls to the XML API and new REST API. Starting with PAN-OS 9.0, you can now specify an [API key lifetime](#) to enforce key rotation and have the ability to [revoke all](#) currently valid API keys, in the event one or more keys are compromised. When you generate a new API key, after upgrading to PAN-OS 9.0, each key size is larger and each key is unique because it includes the key creation timestamp. These new capabilities help you protect your keys and meet the audit and compliance requirements for your enterprise.

STEP 1 | Select **Device > Setup > Management**.

STEP 2 | Edit Authentication Settings to specify the **API Key Lifetime (min)**.



The screenshot shows the 'Authentication Settings' dialog box. It has a title bar with a question mark icon. The settings are as follows:

Field	Value
Authentication Profile	None
Certificate Profile	None
Idle Timeout (min)	60 (default)
API Key Lifetime (min)	0 (default)
API Keys Last Expired	[Empty field] Expire All API Keys
Failed Attempts	0
Lockout Time (min)	0

At the bottom right are 'OK' and 'Cancel' buttons.

Set the API key lifetime to protect against compromise and to reduce the effects of an accidental exposure. By default, the API key lifetime is set to 0, which means that the keys will never expire. To ensure that your keys are frequently rotated and each key is unique when regenerated, you must specify a validity period that ranges between 1–525600 minutes. Refer to the audit and compliance policies for your enterprise to determine how you should specify the lifetime for which your API keys are valid.

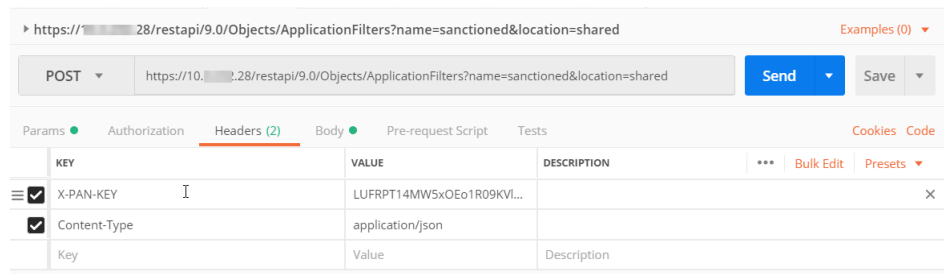
STEP 3 | **Commit** the changes.

PAN-OS REST API for a Simplified Integration Experience

The new PAN-OS REST API allows you to access the Policy and Network resources on the firewall as top-level URIs. You can use these APIs to create, update, and delete these resources directly on the firewall or from Panorama.

STEP 1 | Generate the API key.

When you make your API calls, as an alternative to providing the URL encoded API key in the request URL, you can now use the new custom X-PAN-KEY: <key> parameter to add the key as a name value pair in the HTTP header.



The screenshot shows a REST client interface with a POST request to `https://10.10.10.28/restapi/9.0/Objects/ApplicationFilters?name=sanctioned&location=shared`. The 'Headers' tab is active, displaying a table with the following headers: KEY, VALUE, and DESCRIPTION. Two headers are defined: 'X-PAN-KEY' with a long alphanumeric value and 'Content-Type' with the value 'application/json'. There are also links for 'Bulk Edit' and 'Presets'.

KEY	VALUE	DESCRIPTION
X-PAN-KEY	LUFRPT14MW5xOEo1R09KVI...	
Content-Type	application/json	

or if using Curl, **`curl -H "X-PAN-KEY: LUFRPT02T25Yc0hKUs2Z1FtZWfyWXJOSTdk1234565clhaUFptUT0=" -k 'https://firewall_IP/api/?type=status'`**

STEP 2 | Use the REST API in-product help at https://firewall_IP/restapi-doc.

Universally Unique Identifiers for Policy Rules

Universally unique identifiers (UUIDs) for policy rules are permanent attributes that you can use to track the history of changes to a rule, such as when it was last modified and who made the most recent change to the rule, so that if you change the rule's name or delete it, you can still [track the rule](#) across multiple rulebases. Using the UUID to search for a rule enables you to highlight the specific rule you want to find among thousands of rules, which may have similar or identical names. UUIDs also simplify automation and integration for rules in third-party systems (such as ticketing or orchestration) that do not support names.

Rule UUIDs standardize tracking for policy modifications, making it easier to demonstrate compliance with regulatory requirements. For example, you can include the UUIDs when you [export](#) the rulebase to a PDF or CSV file for internal reviews or audits. Including the UUID in [reports](#) makes it easier to track a rule, even after you change the name of the rule. You can also use the UUID to query the rule in the logs, which helps to create an audit trail.

[Filtering](#) by the rule UUID makes it easier to pinpoint the specific rule you want to locate, even among many similarly-named rules. If your ruleset is very large and contains many rules, using the rule UUID as a filter highlights the particular rule you need to find without having to navigate through pages of results.

STEP 1 | Upgrade existing policy rules to include UUIDs.

- For standalone firewalls, [upgrade to a PAN-OS 9.0 release](#) to automatically generate UUIDs for all existing policy rules.
- For firewalls managed by Panorama, you must [upgrade Panorama to PAN-OS 9.0](#) to automatically generate the UUIDs on Panorama and then [push the policy rulebases](#) with the UUIDs to the managed firewalls before you upgrade the firewalls. If you do not push the policy rulebases with the UUIDs to the managed firewalls before you upgrade them, the upgrade will not proceed.



In Panorama, because the UUIDs are generated on a per-rule basis, all firewalls in the policy target receive a set of centralized rules from Panorama that are synced across HA firewalls. As a result, rules pushed from Panorama and all target devices for the policy rule will have the same UUID; however, if you create a rule locally on the firewall after you push the rules from Panorama to the firewalls, the rule you created locally will have its own UUID.

STEP 2 | Display the UUIDs.

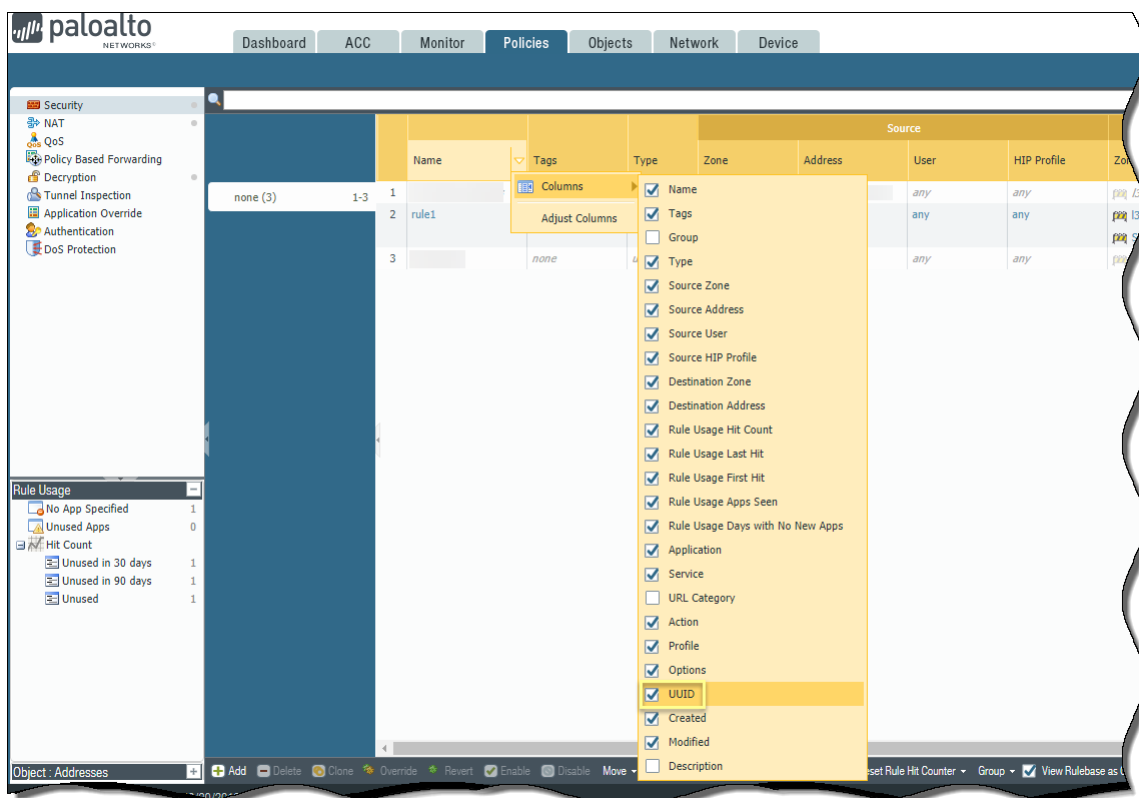
You can use UUIDs to identify applicable rules for the following log types: Traffic, Threat, URL Filtering, WildFire Submission, Data Filtering, GTP, SCTP, Tunnel Inspection, Configuration, and Unified.

- To display the UUID in logs:
 1. Select **Monitor**, then expand the column header (🔍).
 2. Select **Columns**.
 3. Select **Rule UUID**.



- To display UUIDs on the policy rulebase:
 1. Select **Policies**, then expand the column header (▼).
 2. Select **Columns**.
 3. Select **UUID**.

UUIDs are available for all policy rulebases.

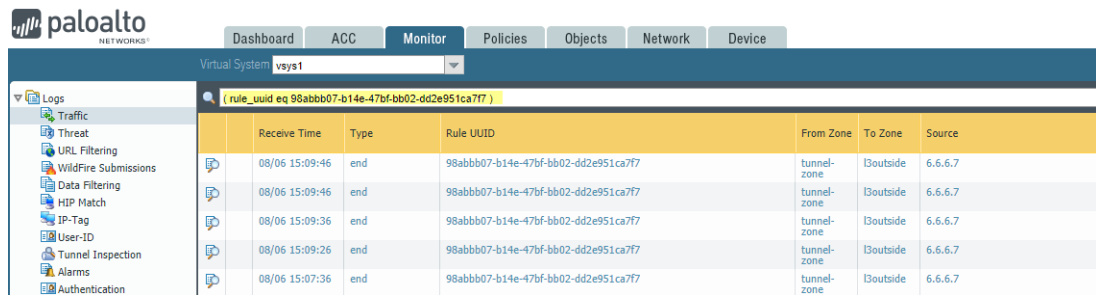


You can now view the UUID associated with the rule, which allows you to match the rule UUID with policies and logs.

STEP 3 | (Optional) Monitor activity for the rule in the ACC.

To apply the UUID as a filter in the ACC, you must copy and paste the UUID.

1. Select the **Monitor** tab to view the UUIDs for the rule that allows or denies the traffic that generated the log.



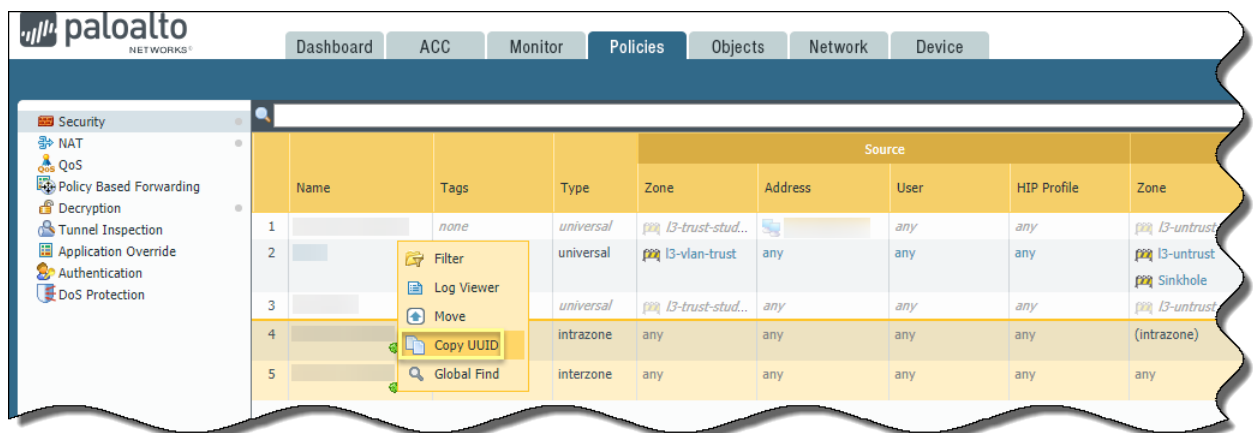
2. Copy the UUID for the rule that allowed or denied the traffic on the firewall.
 1. Select the ellipses that display when you move your cursor over the entry in the **Rule UUID** column.

	Receive Time	Type	Rule UUID
	08/06 15:07:36	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7 ...
	08/06 15:07:26	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7
	08/06 15:07:16	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7
	08/06 15:05:48	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7

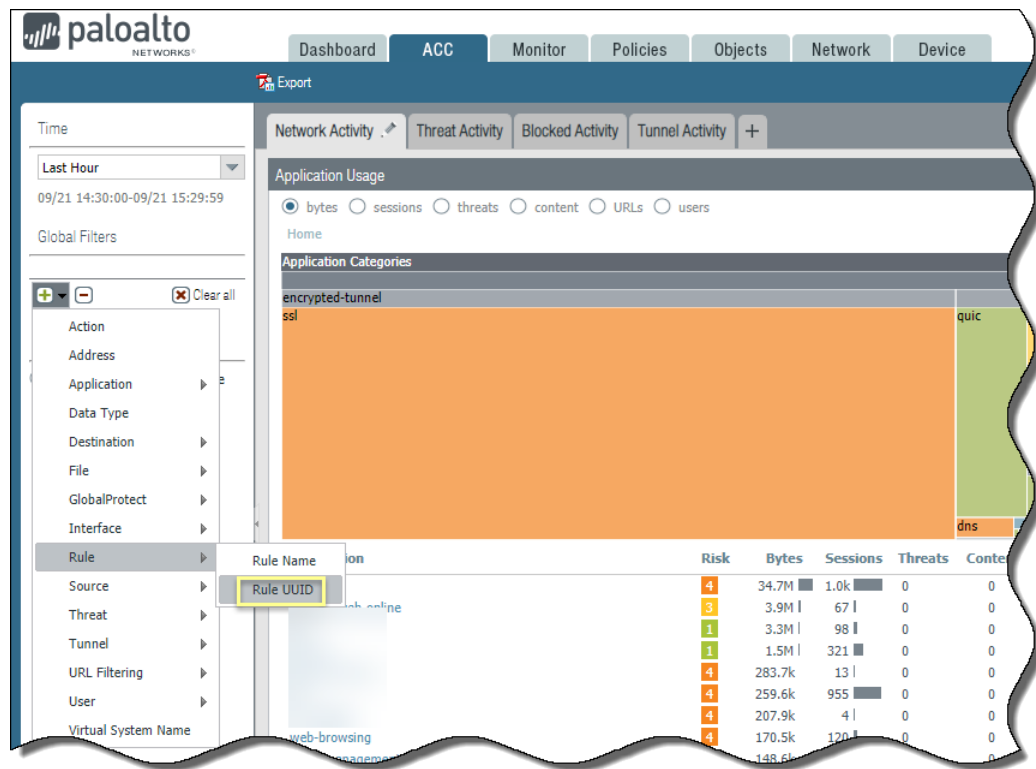
2. Copy the UUID from the pop-up.

	Receive Time	Type	Rule UUID
	08/06 15:07:36	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7
	08/06 15:07:26	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7
	08/06 15:07:16	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7
	08/06 15:05:48	end	98abb07-b14e-47bf-bb02-dd2e951ca7f7

Alternatively, you can go to the **Policies** tab, expand the rule name, and **Copy UUID**.



3. Add a **Rule UUID** global filter to the Application Command Center (ACC) for the rule.
 1. Select the **ACC** tab.
 2. Add (+) a filter to the list of **Global Filters**.
 3. Select **Rule** > **Rule UUID**.



4. Paste the UUID to filter your results.

You can now see activity for the rule UUID in the ACC, making it easier to monitor events related to that rule.

Temporary Master Key Expiration Extension

Each firewall and Panorama management server has a default master key that encrypts all private keys and passwords. To more closely control your private key and password encryption, you can create your own [master key](#) (**Device > Master Key and Diagnostics**) and configure the lifetime of the key.

In PAN-OS 9.0 you can configure the master key to automatically renew the configured master key for a specified number of days after the lifetime of the master key expires. The Temporary Master Key Expiration Extension allows you to extend the lifetime of the master key if you cannot update it across all managed devices and the Panorama management server at the time of expiration.

To deploy a new master key to firewalls, Log Collectors, and WF-500 appliances, see [Master Key Deployment from Panorama](#).

STEP 1 | [Log in to the firewall web interface](#).

STEP 2 | Select **Device > Master Key and Diagnostics** and edit the **Master Key**.

STEP 3 | Enable **Auto Renew Master Key**, and configure the firewall to **Auto Renew with Same Master Key** for a specified number of days and hours.



Consider the number of days until your next available maintenance window when configuring the master key to automatically renew after the lifetime of the key expires.

STEP 4 | Click **OK** to apply the auto-renew setting.

Real-Time Enforcement and Expanded Capacities for Dynamic Address Groups

Virtualization, cloud computing, and IoT have increased the frequency and amount of dynamic changes in the network. To ensure that the network is protected, the firewall can now update the registered IP addresses in a dynamic address group-based (DAG) policy in real time. For example, if you have a containerized environment for software delivery, where workloads can scale up or down and start sending business-critical traffic in a matter of seconds, you can use dynamic address groups in policy to secure such workloads as soon as they begin passing traffic. As soon as the firewall receives a tag on container's source IP address, it can compile the associated DAGs and allow or block traffic based on security policy rules in real time. Similarly, if an IoT device or user device joins the network, the firewall can update DAGs and enforce policy in real time to secure the traffic from the device. And to support the large number of IP addresses generated by IoT devices, virtual machines, and containers, select firewall models now support a higher capacity for registering IP addresses. See [Use Dynamic Address Groups in Policy](#) for the registered IP address capacity of each firewall model.

- [IP-Tag Log](#)
- [IP-Tag Timeout](#)

IP-Tag Log

It is now easier to view the IP address-to-tag mapping with the addition of the IP-tag log on the firewall web interface. This log displays the time when a source IP address is registered or unregistered with the firewall and what tags are associated with that IP address, and the source from which the firewall learned the IP address-to-tag mapping information.

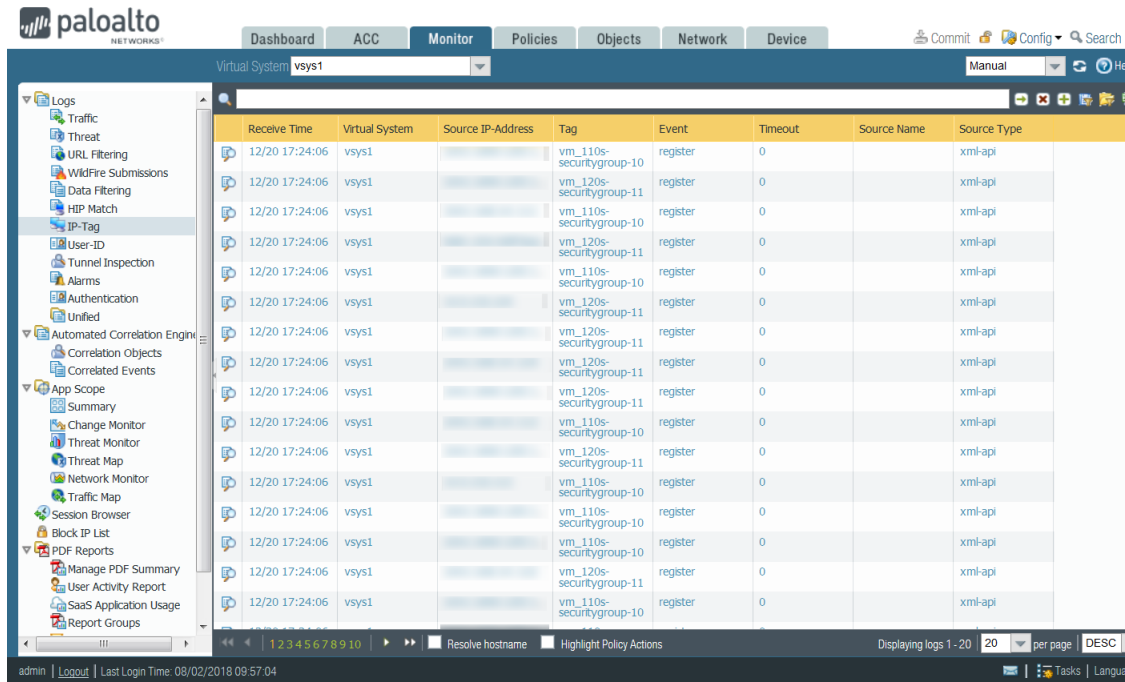
Additionally, you can [generate custom reports](#) based on IP-tag logs or forward IP-tag logs to [Panorama and Log Collectors](#) and [external service](#).



Due to the large number of IP-tag logs generated by the firewall, forwarding the logs using email or SNMP to an external service is not recommended.

Column	Description
Receive Time	The time that the event was logged with the firewall.
Virtual System	The virtual system (vsys) to which the tag is registered.
Source IP-Address	The IP address on which a tag applied or removed.
Tag	Displays the tag that was applied or removed.
Event	The type of event that occurred. Possible values are register and unregister.
Timeout	The amount of time, in minutes, that elapses before the tag is unregistered automatically.

Column	Description
Source Name	The source of the IP address-to-tag mapping information. Possible source names are XML API, AGENT, and HA. See Register IP Addresses and Tags Dynamically for more information about the IP-to-tag mapping sources.
Source Type	The type of source that provided the IP address-to-tag mapping information. Possible source types are unknown, xml-api, ha, and vm-monitor.



The screenshot shows the Palo Alto Networks management console. The 'Monitor' tab is selected, and the 'IP-Tag' log is displayed. The table below represents the data shown in the logs.

Receive Time	Virtual System	Source IP-Address	Tag	Event	Timeout	Source Name	Source Type
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api
12/20 17:24:06	vsys1		vm_120s-securitygroup-11	register	0		xml-api
12/20 17:24:06	vsys1		vm_110s-securitygroup-10	register	0		xml-api

IP-Tag Timeout

Auto-tagging allows the firewall to tag the source or destination IP address when a log is generated on the firewall and establish IP address-to-tag mapping. The firewall can now automatically remove a tag associated with an IP address, so you no longer need to make an explicit action to remove a tag. You can configure a timeout as part of a built-in action for a log forwarding profile or as part of log forwarding settings (**Device > Log Settings**). Configure the timeout, in minutes, from zero (0) minutes to 30 days (43,200 minutes). If you set the timeout to zero (0), the IP address to tag mapping does not timeout and must be removed with an explicit action.

STEP 1 | Log in to the firewall web interface.

STEP 2 | Select **Objects > Log Forwarding**.

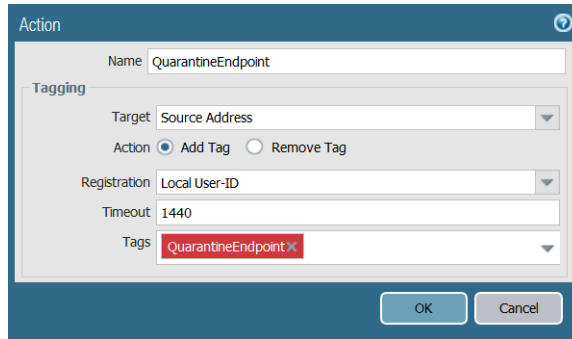
STEP 3 | Select an existing **Log Forwarding Profile** or click **Add** to create a new one.

STEP 4 | Click **Add**.

STEP 5 | Under Built-in Actions, click **Add**.

STEP 6 | Configure an Action.

1. Enter a descriptive Name.
2. Select **Source Address** or **Destination Address** from the **Target** drop-down.
3. Select **Add Tag** as the **Action**. IP-tag timeout does not work with the Remove Tag action.
4. (New in PAN-OS 9.0) Select whether to register the IP address-to-tag mapping to the **Local User-ID** agent on the firewall or Panorama or to a **Remote User-ID** agent.
5. Set the **Timeout** in minutes.
6. Select the **Tags** apply or remove from the target IP address.



The screenshot shows the 'Action' configuration window. The 'Name' field is set to 'QuarantineEndpoint'. Under the 'Tagging' section, the 'Target' is 'Source Address', the 'Action' is 'Add Tag' (selected), and the 'Registration' is 'Local User-ID'. The 'Timeout' is set to '1440' minutes. The 'Tags' field shows 'QuarantineEndpoint' with a red 'X' icon. 'OK' and 'Cancel' buttons are at the bottom right.

Field	Value
Name	QuarantineEndpoint
Target	Source Address
Action	Add Tag
Registration	Local User-ID
Timeout	1440
Tags	QuarantineEndpoint X

Networking Features

- > Security Group Tag (SGT) Ethertype Support
- > FQDN Refresh Enhancement
- > GRE Tunneling Support
- > Wildcard Address Support in Security Policy Rules
- > Hostname Option Support for DHCP Clients
- > FQDN Support for Static Route Next Hop, PBF Next Hop, and BGP Peer
- > Dynamic DNS Support for Firewall Interfaces
- > HA1 SSH Key Refresh
- > Advanced Session Distribution Algorithms for Destination NAT
- > VXLAN Tunnel Content Inspection

Security Group Tag (SGT) Ethertype Support

If you're using Security Group Tags (SGTs) to control user and device access in a Cisco Trustsec network, inline firewalls in Layer 2 or Virtual Wire mode can now inspect and provide threat prevention for the tagged traffic. Before PAN-OS 9.0, a firewall in Layer 2 or virtual wire mode could allow SGT traffic but did not process it. Now, processing of SGT traffic works by default and without any configuration changes.

It's important to note that the firewall does not use SGTs as match criteria for security policy enforcement—you should continue to define SGT-based policy in the same way you do today.

Best practices for deploying Palo Alto Networks firewalls in a Cisco Trustsec network include:

- ❑ Deploy firewalls that you expect to process SGT packets in either [Layer 2](#) or [virtual wire](#) mode.
- ❑ It's not recommended to deploy firewalls that might process SGT packets in Layer 3 mode. However, if you need to use a [Layer 3](#) firewall in a Cisco Trustsec network:
 - Deploy the Layer 3 firewall between two SGT exchange protocol (SXP) peers.
 - Configure the firewall to allow the traffic between the SXP peers.

FQDN Refresh Enhancement

A DNS record of an FQDN includes a time-to-live (TTL) value and, by default, the firewall now refreshes each FQDN in its cache based on that individual TTL provided by the DNS server—as long as the TTL is greater than or equal to the minimum FQDN refresh setting you configure on the firewall (or greater than or equal to the default setting of 30 seconds if you don't configure a minimum FQDN refresh setting). Refreshing an FQDN based on its TTL value results in more accurate FQDN resolutions. This is especially helpful for securing access to cloud platform services, which often require frequent FQDN refreshes to ensure that their services are available. For example, cloud environments that support autoscaling depend on FQDN resolutions for dynamically scaling services up and down; fast resolutions of FQDNs are critical in such time-sensitive environments.

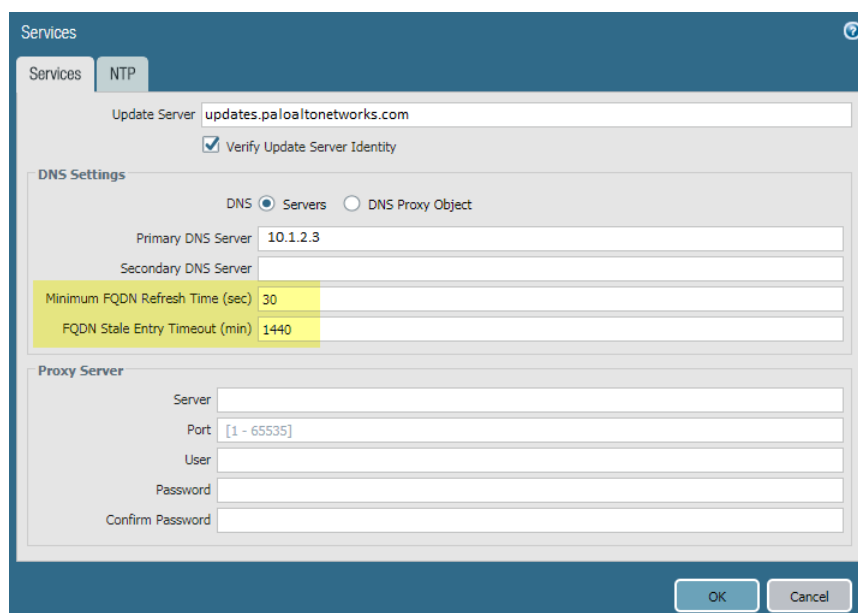
You can configure the firewall with a [Minimum FQDN Refresh Time](#) to limit how small a TTL value the firewall honors. If your IP addresses don't change very often, you can set a higher Minimum FQDN Refresh Time so that the firewall doesn't refresh entries more often than necessary. The firewall uses the higher of the DNS TTL time and the configured Minimum FQDN Refresh Time.

Additionally, you can set a stale-entry timeout to configure how long the firewall continues to use stale (expired) FQDN resolutions in the event of an unreachable DNS Server.

STEP 1 | Select **Device > Setup > Services > Global** (omit Global on a firewall without multiple virtual system capability) and edit.

STEP 2 | Configure the FQDN timers for the firewall:

1. Select **DNS Servers** or **DNS Proxy Object**.
2. Enter the **Minimum FQDN Refresh Time (sec)** in seconds to limit how frequently the firewall will refresh the FQDN cache entries (range is 0 to 14,400; default is 30). A setting of 0 means the firewall will refresh the FQDN based on the TTL value in the DNS record; the firewall doesn't enforce a minimum FQDN refresh time.
3. Enter the **FQDN Stale Entry Timeout (min)** in minutes, which is the length of time that the firewall continues to use stale FQDN resolutions in the event of an unreachable DNS server (range is 0 to 10,080; default is 1,440). A value of 0 means the firewall does not use a stale FQDN entry.
4. Click **OK**.



The screenshot shows the 'Services' configuration window with the 'NTP' tab selected. The 'Update Server' field is set to 'updates.paloaltonetworks.com' and 'Verify Update Server Identity' is checked. Under 'DNS Settings', the 'DNS Servers' radio button is selected. The 'Primary DNS Server' is '10.1.2.3'. The 'Minimum FQDN Refresh Time (sec)' is set to 30, and the 'FQDN Stale Entry Timeout (min)' is set to 1440. The 'Proxy Server' section is empty. The 'OK' and 'Cancel' buttons are at the bottom right.

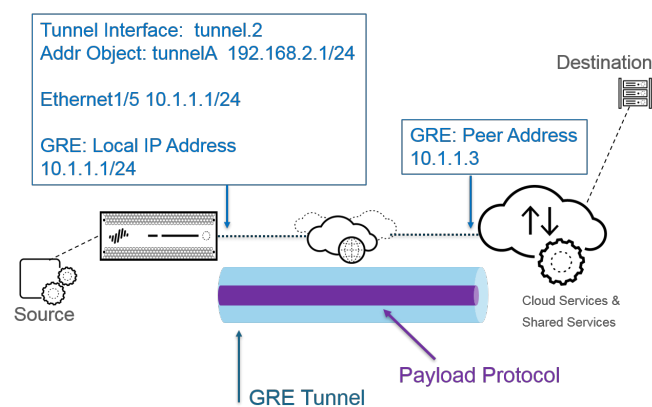
STEP 3 | **Commit** your changes.

GRE Tunneling Support

Palo Alto Networks next-generation firewalls can now terminate GRE tunnels; you can route or forward packets to a GRE tunnel. The [GRE tunnel](#) connects two endpoints in a point-to-point, logical link between the firewall and another device. GRE tunnels are simple to use and often the tunneling protocol of choice for point-to-point connectivity, especially to services in the cloud or to partner networks.

Create a GRE tunnel when you want to direct packets that are destined for an IP address to take a certain point-to-point path, for example to a cloud-based proxy or to a partner network. The packets travel in the GRE tunnel to the cloud service while on their way to the destination address. Thus the cloud service can enforce its services or policies on the packets.

The following figure is an example of a GRE tunnel connecting the firewall across the internet to a cloud service.



STEP 1 | Create a tunnel interface.

1. Select **Network > Interfaces > Tunnel**.
2. Enter the tunnel **Interface Name** followed by a period and a number in the range 1 to 9,999; for example, tunnel.1.
3. Assign the tunnel interface to a **Security Zone**.
4. Assign an IP address to the tunnel interface.

STEP 2 | Create a GRE tunnel to have packets take a specific point-to-point path.

1. Select **Network > GRE Tunnels** and **Add** a tunnel.
2. Select the **Interface** to use as the local GRE tunnel endpoint (source interface), which is an Ethernet interface or subinterface, AE, loopback, or VLAN interface.
3. Select the **Local IP Address** of that interface.
4. Enter the **Peer Address**, which is the IP address of the opposite endpoint of the GRE tunnel.
5. Select the **Tunnel Interface** that you created in Step 1.

STEP 3 | (Best Practice) Enable the Keep Alive function for the GRE tunnel. Optionally change the Keep Alive settings.

STEP 4 | Configure a routing protocol or static route to route packets to the GRE tunnel. For example, [configure a static route](#) to the destination server.

STEP 5 | Commit your changes.

STEP 6 | Configure the opposite end of the tunnel.

STEP 7 | Verify that the firewall can communicate with the tunnel peer over the GRE tunnel.

Wildcard Address Support in Security Policy Rules

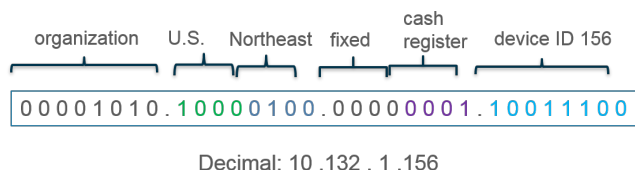
When you define private IPv4 addresses to internal devices, you may use an IP addressing structure that assigns meaning to certain bits in the IP address. For example, the first three bits in the third octet of an IP address signify the device type. This structure helps you easily identify device type, location, and so on, based on the device's IP address.

You can now use this same address structure in Security policy rules on the firewall for easier deployment. You create an address object that uses a wildcard address (IP address and wildcard mask separated by a slash, such as 10.1.2.3/0.127.248.0). A wildcard address can identify many source or destination addresses in a single Security policy rule, which is especially helpful for data center firewalls serving many devices. You won't have to manage an unnecessarily large number of address objects to cover all the matching IP addresses, or use less restrictive Security policy rules than you need due to IP address capacity constraints.

For example, suppose you use the IPv4 addressing scheme shown in the following figure, where the first octet represents your organization (bits 00001010 are fixed). In the second octet, the first four bits designate the country where the network device is located (1000 indicates the U.S.); the last four bits indicate the region (0100 indicates the northeast). In the third octet, the first four bits are zeros and the last four bits indicate device type (0001 indicates cash register; 0011 indicates printer). The last octet indicates the ID number of the networking device.



Based on that structure, the IP address of cash register number 156 in the northeastern U.S. would be 10.132.1.156:



You can use an address object of type **IP Wildcard Mask** to support such an addressing structure in a Security policy rule. You apply a wildcard mask to an IPv4 source or destination address to specify which addresses are subject to the rule. In a Palo Alto Networks wildcard mask, a zero bit indicates that the bit being compared must match the bit in the IP address that is covered by the zero. A one bit in the mask is a wildcard or “don’t care” bit, meaning the bit being compared need not match the bit in the IP address. For example, the following snippets of an IP address and wildcard mask illustrate how they yield four matches:

The diagram shows a binary snippet and a wildcard mask:

```
0011  binary snippet
1010  wildcard mask
-----
0001  yields four matches
0011
1001
1011
```



Not all vendors use a one as a wildcard bit and a zero as a matching bit.

In the example, cash registers have an IPv4 address with the third octet 00000001 and printers have an IPv4 address with the third octet 00000011. Suppose you want to apply a Security policy rule to all cash registers and printers having any ID number from 0 to 255. To get that result, you need a wildcard mask; the third octet of the wildcard mask must be 2, and the device ID (the fourth octet) must be 255. The address object to specify all cash registers and printers in the northeastern U.S. would use wildcard address 10.132.1.2/0.0.2.255:

```
0000 1010.1000 0100.0000 0001.0000 0010 (IP address 10.132.1.2)
0000 0000.0000 0000.0000 0010.1111 1111 (wildcard mask 0.0.2.255)

yields these matches:
0000 1010.1000 0100.0000 0001.0000 0000
0000 1010.1000 0100.0000 0001.0000 0001
0000 1010.1000 0100.0000 0001.0000 0010
0000 1010.1000 0100.0000 0001.0000 0011
... and so on (fourth octet yields every number from 0 to 255)
and
0000 1010.1000 0100.0000 0011.0000 0000
0000 1010.1000 0100.0000 0011.0000 0001
0000 1010.1000 0100.0000 0011.0000 0010
0000 1010.1000 0100.0000 0011.0000 0011
... and so on (fourth octet yields every number from 0 to 255)
```

Thus, a single Security policy rule that uses an address object with wildcard address 10.132.1.2/0.0.2.255 as the destination address matches the addresses of 512 devices (256 cash registers + 256 printers), which is an efficient way to apply a rule to many devices.

Consider the following when you use an address object of type **IP Wildcard Mask** in a Security policy rule:

- A source or destination address that uses an address object of type **IP Wildcard Mask** doesn't support the **Negate** option.
- The firewall doesn't consider wildcard addresses when doing shadow matching, which means you won't be warned if a Security policy rule using an address object of type **IP Wildcard Mask** overlaps a subsequent rule or is overlapped by a rule higher on the list.
- If an address matches rules that have overlapping wildcard masks, the firewall chooses the match to the longest prefix in the wildcard mask, as shown in the following figure:

Rule 1

11.128.0.1/0.127.248.0

0000 1011 . 1000 0000 . 0000 0000 . 0000 0001
0000 0000 . 0111 1111 . 1111 1000 . 0000 0000

9 digits

Rule 2

11.128.0.1/0.15.248.0

0000 1011 . 1000 0000 . 0000 0000 . 0000 0001
0000 0000 . 0000 1111 . 1111 1000 . 0000 0000

12 digits

Address being matched

11.128.80.1

0000 1011 . 1000 0000 . 0101 0000 . 0000 0001

Two wildcard masks in Rule 1 and Rule 2 overlap. Address matches Rule 1 and Rule 2; firewall uses Rule 2 because it is the longest prefix match (12 digits) of wildcard.

STEP 1 | Create an address object that uses a wildcard address.

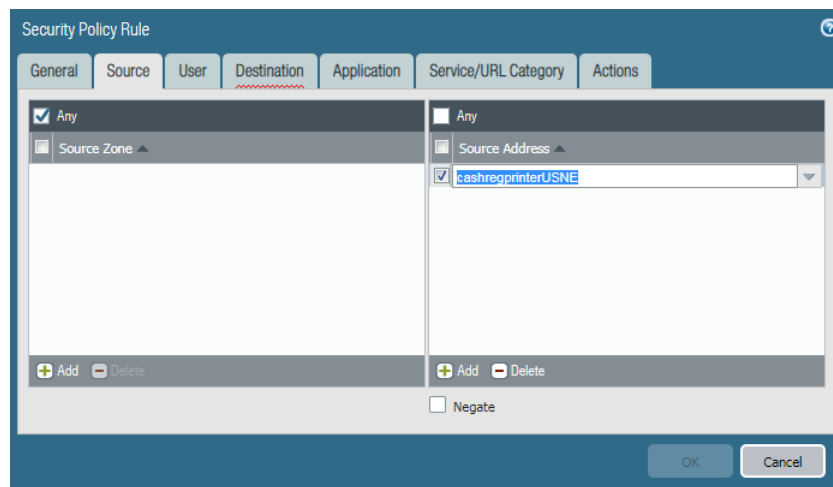
1. Select **Objects > Addresses** and **Add** an address object.
2. For **Type**, select **IP Wildcard Mask** and enter the IPv4 address and wildcard mask, separated by a slash (/). The mask must begin with at least one zero (0); for example, 10.132.1.2/0.0.2.255.



The firewall performs Security policy matching from the top down (starting with the first rule), so place Security policy rules that use more specific wildcards closer to the top of the list of rules.

3. Click **OK**.

STEP 2 | Create a Security policy rule and Add the Address object you created for the source or destination address.



STEP 3 | Commit your changes.

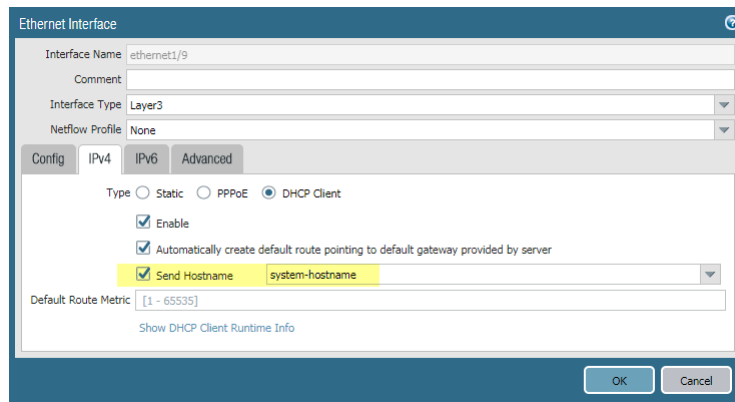
STEP 4 | View logs, custom reports, or network activity in the ACC filtered by the address object you created.

Hostname Option Support for DHCP Clients

When a firewall interface is a DHCP client that is assigned a dynamic IPv4 address by a DHCP server, the changing IP address makes it difficult for external hosts to identify the interface. You can now assign a hostname to a DHCP client interface on the firewall and send that hostname (Option 12) to a DHCP server, which can register the hostname with the DNS server. The DNS server can automatically manage hostname-to-dynamic IP address resolutions.

STEP 1 | [Configure an Interface as a DHCP Client.](#)

STEP 2 | Select **Send Hostname** and accept the firewall hostname (the default) or enter a unique hostname for the interface.



The screenshot shows the 'Ethernet Interface' configuration window. The 'Interface Name' is 'ethernet1/9'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Config' tab is selected, and the 'DHCP Client' radio button is chosen. The 'Enable' checkbox is checked. The checkbox 'Automatically create default route pointing to default gateway provided by server' is also checked. The 'Send Hostname' checkbox is checked, and the dropdown menu next to it shows 'system-hostname'. The 'Default Route Metric' is set to '[1 - 65535]'. There is a link 'Show DHCP Client Runtime Info' below the metric field. At the bottom right, there are 'OK' and 'Cancel' buttons.

FQDN Support for Static Route Next Hop, PBF Next Hop, and BGP Peer

In dynamic environments, network endpoints have dynamic addresses and often use FQDNs to represent the addresses in routing and forwarding. The firewall now supports an FQDN in three additional networking functions: a static route next hop, a policy-based forwarding (PBF) next hop, and a BGP peer address. Using FQDNs reduces configuration and management overhead.

Also, in order to simplify provisioning, you can use an FQDN (instead of statically assigning an IP address to a static IP next hop, PBF next hop, or BGP peer) and the FQDN resolution can change from location to location. Service providers often tend to map the FQDN to an IP address based on the location and deployment requirements. For example, if you are a service provider, you can provide FQDNs for accessing cloud services and resolve these to the IP address of the closest server for the client (based on the client's geo-location), so that the same FQDN can be used globally for the connection to the cloud service.

- Create an address object that uses an FQDN (unless you prefer to directly specify the FQDN when you configure the next hop or BGP peer).
 1. Select **Objects > Addresses** and **Add** a new address object by **Name**.
 2. Select **FQDN** as the object **Type** and enter the FQDN.
 3. Click **OK**.
- [Configure a static route](#) and use an FQDN or the FQDN address object as the next hop.
- [Create a policy-based forwarding rule](#) and use an FQDN or the FQDN address object as the next hop to which the firewall forwards the matching packets.
- [Configure a BGP peer](#) and use an FQDN or the FQDN address object as the BGP peer address.

Dynamic DNS Support for Firewall Interfaces

When you have services hosted behind the firewall and use destination NAT policies on the firewall to access the services, or when you need to provide remote access to the firewall, you can register the interface's IPv4 address changes (dynamic or static address) and IPv6 address changes (static address only) with a dynamic DNS (DDNS) service provider. The DDNS service automatically updates the domain name-to-IP address mappings, so that it can provide accurate IP addresses to DNS clients, which in turn can access the firewall and services behind the firewall. DDNS is often used in branch deployments that are hosting services. Without DDNS support for firewall interfaces, you would need external components to provide accurate IP addresses to clients.

The firewall currently supports the following DDNS service providers: DuckDNS, DynDNS, FreeDNS, Afraid.org Dynamic API, FreeDNS Afraid.org, and No-IP. The individual DDNS service provider determines the services it provides, such as how many IP addresses it supports for a hostname, whether it supports IPv6 addresses, and other factors. Palo Alto Networks uses content updates to add new DDNS service providers and to make service provider updates available to you.

STEP 1 | Before configuring DDNS, determine the hostname that you registered with your DDNS provider.

STEP 2 | Obtain the public SSL certificate from your DDNS provider and import it into the firewall.

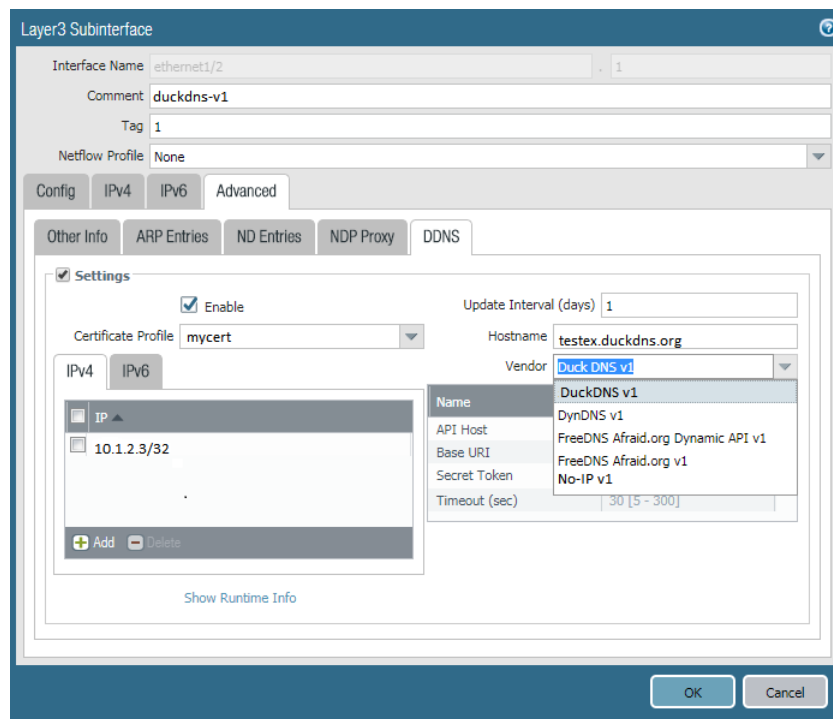
STEP 3 | **Configure DDNS** for a Layer 3 interface.

1. **Enable DDNS** for an Ethernet or VLAN interface or subinterface and enter the **Hostname** for the interface, which exactly matches the hostname you registered with the DDNS service.
2. Select one or more IPv4 or IPv6 addresses assigned to the interface.
3. [Create a certificate profile](#) or select a certificate profile to verify the SSL certificate of the DDNS service when the firewall first connects to a DDNS service to register an IP address and at every update.
4. Select the **Vendor** (and version number) you are using for DDNS service.



Palo Alto Networks uses content updates to add new DDNS service providers and to provide updates to their services.

5. Configure the Value fields, such as a password that the DDNS service provides to you, and a timeout that the firewall uses if it doesn't receive an update from the DDNS service.



STEP 4 | View DDNS information for the interface, such as the result of the last FQDN update, and the last time the DDNS service received an FQDN update.

HA1 SSH Key Refresh

When you configure [Active/Passive HA](#) or [Active/Active HA](#), you can enable encryption for the HA1 (control link) connection between HA firewalls. HA peers use public and private Secure Shell (SSH) host keys to authenticate each other. When you enable encryption and generate a new pair of host keys or configure other HA1 encryption settings, you can now enable the new host keys and other settings without restarting the HA firewalls, thus avoiding the firewalls going offline. The firewall re-establishes HA1 sessions with its peer and generates system logs (subtype is ha) for re-establishing HA1 and HA1-backup sessions.

[Set and display various SSH settings](#) for the HA1 link after you [Access the CLI](#).

- (Optional) Set the HA1 link to use a specific key type (known as the default host key type). The HA1 link uses only the default host key type to authenticate the HA peers (before an encrypted session is established between them). The choices are ECDSA 256, 384, or 521, or RSA 2048, 3072, or 4096. By default, the default host key type is RSA 2048.
- Establish when automatic rekeying of the session keys occurs for the HA1 link by setting data, time, and/or packet count parameters. After any one rekeying parameter reaches its configured value, SSH uses the new session encryption keys.
- (Optional) Set the SSH server to use the specified encryption ciphers for the HA1 sessions. HA1 SSH allows all [supported ciphers](#) by default. When you set one or more ciphers, the SSH server advertises only those ciphers while connecting, and if the client (the HA peer) tries to connect using a different cipher, the server terminates the connection.
- (Optional) Delete a cipher from the set of ciphers you selected for the HA1 link.
- (Optional) Set the session key exchange algorithm for HA1 SSH. By default the server advertises all the key exchange algorithms to the client.
- (Optional) Set the message authentication code (MAC) for HA1 SSH. By default the server advertises all the MAC algorithms to the client.
- Regenerate ECDSA or RSA host keys for HA1 SSH to replace the existing keys. Do this at the frequency you determine necessary for security purposes.

Advanced Session Distribution Algorithms for Destination NAT

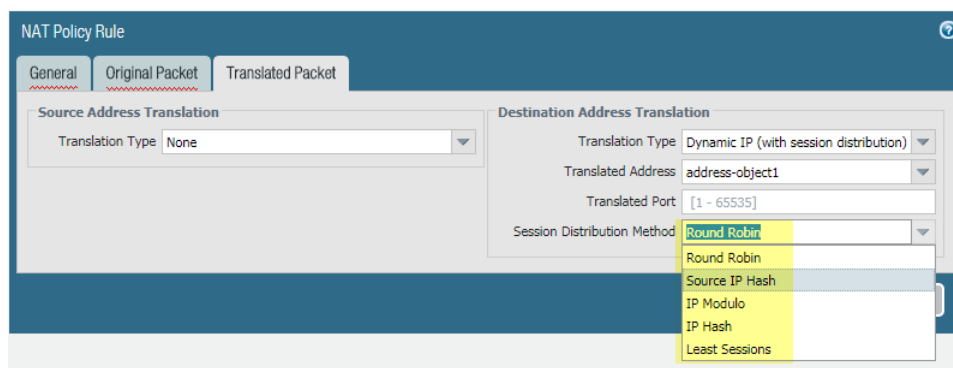
In a destination NAT policy rule, when the destination address type is **Dynamic IP (with session distribution)** (which supports IPv4 addresses only), the translated address can be an address group or address object that uses an IP netmask, IP range, or FQDN, any of which can return multiple addresses from DNS. The firewall distributes incoming NAT sessions among the multiple addresses based on the **Round Robin** method or one of several new methods: **Source IP Hash**, **IP Modulo**, **IP Hash**, and **Least Sessions**.

STEP 1 | Create an address object.

1. Select **Objects > Addresses** and **Add** an address object by **Name**.
2. For **Type**, select one of the following and enter the required information:
 - **IP Netmask**—Enter an IPv4 address, optionally followed by a slash and prefix length.
 - **IP Range**—Enter two IPv4 addresses separated by a hyphen (-).
 - **FQDN**—Enter the FQDN.
3. Click **OK**.

STEP 2 | Configure destination NAT using a dynamic IP address.

1. On the **Translated Packet** tab, in the Destination Address Translation section, select **Dynamic IP (with session distribution)** as the **Translation Type**.
2. For **Translated Address**, select the address object you configured.
3. In case the dynamically-assigned, translated address results in more than one address, select the **Session Distribution Method** the firewall uses to distribute new NAT sessions among those addresses:
 - **Round Robin**—(default) Assigns new sessions to IP addresses in rotating order. Unless you have a reason to change the distribution method, Round Robin distribution is likely suitable.
 - **Source IP Hash**—Assigns new sessions based on hash of source IP address. If you have traffic coming from a single source IP address, then select a method *other than* Source IP Hash.
 - **IP Modulo**—The firewall takes into consideration the source and destination IP address from the incoming packet; the firewall performs an XOR operation and a modulo operation; the result determines to which IP address the firewall assigns new sessions.
 - **IP Hash**—Assigns new sessions based on hash of source and destination IP addresses.
 - **Least Sessions**—Assigns new sessions to the IP address with the fewest concurrent sessions. If you have many short-lived sessions, Least Sessions will provide you with more balanced distribution of sessions.



4. Click **OK**.

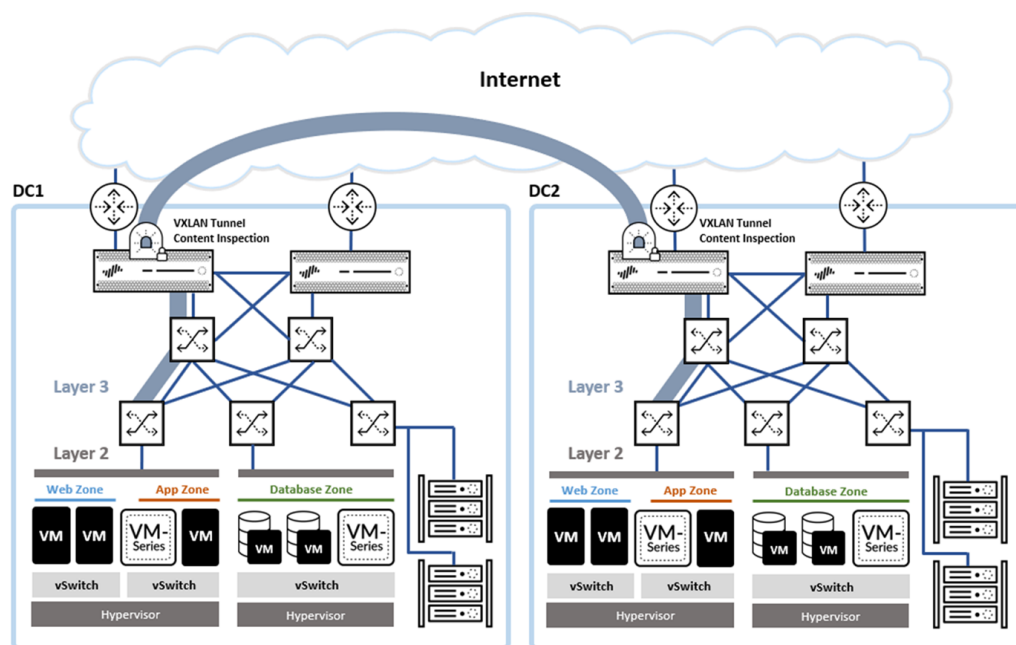
STEP 3 | **Commit** your changes.

VXLAN Tunnel Content Inspection

Tunnel Content Inspection (TCI) now supports the VXLAN inspection protocol. Without terminating the VXLAN tunnel, you can natively scan individual flows within the tunnel, and control them using security policy rules. You can create a tunnel inspection rule using the VXLAN protocol and specify the VXLAN IDs for the flow(s) you want to inspect. The Tunnel ID is a VXLAN Network Identifier (VNI) within the VXLAN packet.

VXLAN TCI is supported for physical and virtual firewalls in VXLAN overlay networks, which can include public or private clouds, and containers.

VXLAN is widely used to encapsulate traffic going over Layer 3 to and from the firewall. For example, you can use VXLAN as a transport overlay to tunnel between geographically dispersed data centers, as shown below.



The following procedure highlights VXLAN elements for tunnel content inspection configuration.

STEP 1 | Create a **Security policy rule** to allow VXLAN traffic for a specific application to travel from the source zone to the tunnel destination zone.

STEP 2 | Create a **tunnel inspection policy rule**.

1. Select **General** and **Add** a policy rule, entering the **Name**, and the **Source** and **Destination** zones and IP addresses.
2. Select **Inspection** > **Add** and select the VXLAN tunnel protocol and other protocols that apply (GRE, GTP-U, or Non-encrypted IPSec). With the VXLAN protocol, the firewall inspects a VXLAN payload to find the encapsulated content or applications within the tunnel. Inspection only occurs on the outer tunnel.
 - Select **Inspect Options**.
 - Set the **Maximum Tunnel Inspection Levels** value to **One Level** (the default, and the only valid choice for VXLAN).

- Choose the condition under which the firewall drops a packet, and if appropriate, choose to return it to the original source.

Optional—When traffic is redirected to the firewall, VXLAN encapsulates the packet. Enable **Return scanned VXLAN tunnel to source** to return the encapsulated packet to the originating VXLAN tunnel endpoint (VTEP). This option is only supported on Layer 3, Layer 3 subinterface, aggregate interface Layer 3, and VLAN.

- Enter a **Monitor Tag (number)** to group similar traffic together for logging and reporting (range is 1 to 16,777,215). The tag number is globally defined.

The **Monitor Tag** field does not apply to the VXLAN protocol. VXLAN logs automatically use the VNI from the VXLAN header.

- (Optional) To inspect all VNIs, skip this step. To limit the VNIs you inspect, you can assign VXLAN IDs. Select **Tunnel ID** and add a name and assign VXLAN (VNI) value(s).

- Assign a **Name**. The **name** is a convenience, and is not a factor in logging, monitoring, or reporting.
- In the **VXLAN ID (VNI)** column, enter a single VNI, a comma-separated list of VNIs, a range of up to 16 million VNIs (with a hyphen as the separator), or a combination of these. For example: 1-54,1024,1677011-1677038,94

The maximum VXLAN IDs per policy is 4,096. To preserve configuration memory, use ranges where possible.

Name	VXLAN ID (VNI)
Tenant_1	1
Tenant_2_to_10	2-10
Tenant_11_13_15	11,13,15
Tenant_Premium_95051	1677702,1677710-1677720,1024

- Click **OK**.

STEP 3 | Manage tunnel inspection policy rules as described in [Configure Tunnel Content Inspection](#) (delete, clone, enable, etcetera).

STEP 4 | **Commit** your changes.

STEP 5 | View tunnel inspection [logs](#). During VXLAN logging, the tunnel ID is the VXLAN ID (VNI) extracted from the VXLAN packet. The tunnel inspection rule match determines whether a Tunnel Inspection log or a Traffic log is produced.

If the VXLAN traffic matches the tunnel inspection rule, the VNI session is logged in the Tunnel Inspection log, and inner sessions are logged in Traffic logs. In the inner session, the Tunnel Inspected flag indicates a VNI session traffic log. The Parent Session is the session that was active when the inner session was created, so the ID might not match the current Session ID. If the VXLAN traffic does not match the tunnel inspection rule, VNI sessions are logged in Traffic logs.

User-ID Features

- > WinRM Support for Server Monitoring
- > Shared User-ID Mappings Across Virtual Systems
- > User-ID Support for Large Numbers of Terminal Servers

WinRM Support for Server Monitoring

To map usernames from login/logout events to IP addresses, the PAN-OS integrated User-ID agent can now use the lightweight Windows Remote Management (WinRM) protocol to monitor Active Directory Windows Servers 2008 or Microsoft Exchange Servers 2008 or later.

Using the WinRM protocol greatly improves the speed, efficiency, and security when monitoring server events to map usernames to IP addresses.

There are three ways to configure server monitoring using WinRM:

- [Configure WinRM over HTTPS with Basic Authentication](#)—The firewall authenticates to the monitored server using the username and password of the service account for the User-ID agent, and the firewall authenticates the monitored server using the User-ID certificate profile.
- [Configure WinRM over HTTP with Kerberos](#)—The firewall and the monitored servers use Kerberos for mutual authentication, and the monitored server encrypts the communication with the firewall using a negotiated Kerberos session key.
- [Configure WinRM over HTTPS with Kerberos](#)—The firewall and the monitored server use HTTPS to communicate and use Kerberos for mutual authentication.



The account you use to configure WinRM on the server you want to monitor must have administrator privileges.

STEP 1 | Configure the [service account](#) with Remote Management User and CIMV2 privileges.

STEP 2 | [Enable WinRM](#) on the Windows server.



WinRM with Kerberos supports the `aes128-cts-hmac-sha1-96` and `aes256-cts-hmac-sha1-96` ciphers. If you want to authenticate using Kerberos and the server you want to monitor uses RC4, you must download the Windows [update](#) and [disable](#) RC4 for Kerberos in the registry settings of the server you want to monitor.

1. To open the ports on the Windows server for WinRM connections, enter the following command:
winrm quickconfig, then enter **y** to confirm the changes and confirm the output displays WinRM service started.

If WinRM is enabled, the output displays `WinRM service is already running on this machine`. You will be prompted to confirm any additional required configuration changes.

2. Verify that WinRM is communicating using the correct protocol by entering the following command:
winrm enumerate winrm/config/listener.
 - For HTTP, confirm that the output displays `Transport = HTTP`.
 - For HTTPS, confirm that the output displays `Transport = HTTPS`.

STEP 3 | ([HTTPS only](#)) Configure the server thumbprint to authenticate the server with the firewall.

1. Verify the certificate is installed in the Local Computer certificate store (**Certificates (Local Computer) > Personal > Certificates**).
2. Open the certificate and select **General > Details > Show: <All>**, select the **Thumbprint** and copy it.
3. From the Windows server command prompt, enter the following command:
winrm create winrm/config/Listener?Address=*&Transport=HTTPS @{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"} ,
hostname is the hostname of the monitored server and *Certificate Thumbprint* is the value you copied from the certificate.

Make sure to remove any spaces in the Certificate Thumbprint to ensure that WinRM will be able to validate the certificate.

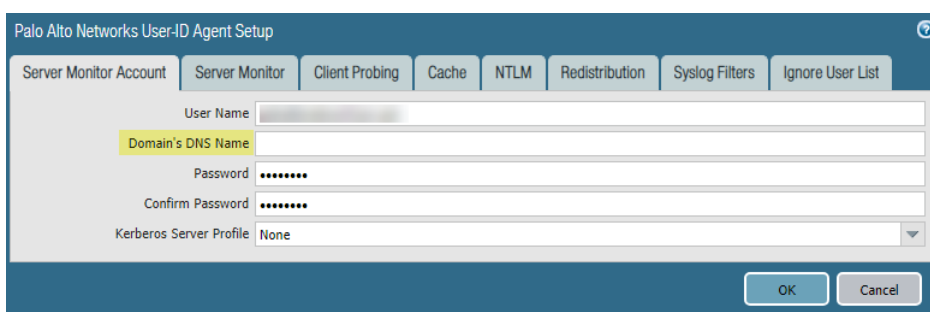
4. Specify the authentication type and verify successful authentication between the server and the firewall.
 - For HTTPS with basic authentication, from the Windows server command prompt, enter the following command: `c:\> winrm set winrm/config/client/auth @{Basic="true"}`, then enter `winrm get winrm/config/service/Auth` and confirm that `Basic = true`.
 - For HTTPS with Kerberos authentication, from the Windows server command prompt, enter the following command: `winrm get winrm/config/service/Auth` and confirm that `Basic = false` and `Kerberos = true`.

STEP 4 | Enable authentication between the PAN-OS integrated User-ID agent and the Windows servers you plan to monitor using WinRM.

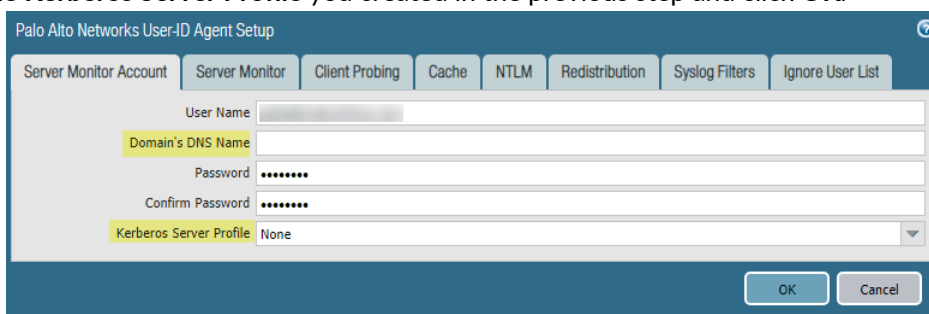
1. From the firewall web interface, select **Device > User Identification > User Mapping > Palo Alto Networks User-ID Agent Setup > Server Monitor Account**.
2. In `domain\username` format, enter the **User Name** for the service account that the User-ID agent will use to monitor servers.
3. Enter the **Domain's DNS Name** of the server monitor account.

If you are authenticating using Kerberos, Kerberos uses the domain name to locate the service account.

4. Enter the **Password** and **Confirm Password** for the service account, then click **OK**.



5. (**Kerberos only**) Configure the firewall to authenticate with the Windows server using Kerberos.
 1. If you did not do so during the [initial configuration](#), make sure you have configured date and time (NTP) settings to ensure successful Kerberos negotiation.
 2. [Configure a Kerberos server profile](#) on the firewall to authenticate with the server to monitor the security logs and session information.
 3. Select the **Kerberos Server Profile** you created in the previous step and click **OK**.



STEP 5 | Configure the PAN-OS integrated User-ID agent to use a WinRM transport protocol to monitor Windows servers.

1. Select the Microsoft server **Type (Microsoft Active Directory or Microsoft Exchange)**.
2. Select the WinRM **Transport Protocol**.
 - **WinRM-HTTP**—Use WinRM over HTTP to monitor the server's security logs and session information. If you select this option, you must configure authentication using [Kerberos](#).
 - **WinRM-HTTPS**—Use WinRM over HTTPS to monitor the server's security logs and session information. If you select this option, you must configure either basic authentication or authentication using [Kerberos](#).
3. Enter the IP address or FQDN **Network Address** of the server.



If you are using Kerberos, the network address must be a fully qualified domain name (FQDN).

STEP 6 | (HTTPS only) Import the certificate that the server uses for WinRM onto the firewall and associate it with the User-ID Certificate Profile.

The firewall uses the same certificate to authenticate with all monitored servers.

1. Select **Device > User Identification > Connection Security** and click **Edit**.
2. Select the Windows server certificate to use for the **User-ID Certificate Profile**, then click **OK**.

STEP 7 | Commit your changes.

STEP 8 | To verify the configuration, verify that the status of each server configured for server monitoring is **Connected** on the **Device > User Identification > User Mapping** tab in the web interface.

Shared User-ID Mappings Across Virtual Systems

To simplify User-ID source configuration if you have multiple virtual systems, you can now share user mappings across virtual systems. To [share User-ID](#) IP address-to-username mappings, choose a virtual system to use as a *User-ID hub* and consolidate all of the [server monitoring](#) configurations that you want to share on the hub.

The User-ID hub then collects the IP address-to-username mappings from the sources you configure and stores them in a centralized mapping table that is accessible to all other virtual systems on the firewall. If you have user information from specific monitored servers that you do not want to share across virtual systems, retain the server monitoring configuration on the individual virtual system instead of moving it to the hub.

When the firewall needs to identify the user to either enforce user-based policy or to include the username in a log or report, it first looks in the mapping table on the local virtual system. If it doesn't find the mapping, it then checks the mapping table on the User-ID hub.

After you assign a virtual system as a User-ID hub and commit, all other virtual systems will have instantaneous access to the mappings on the User-ID hub. After you configure the User-ID hub, when a virtual system needs to identify a user for user-based policy enforcement or to display the user in a log or report, the virtual system can use the mapping table on the User-ID hub.



On the hub, you can configure any User-ID sources that are currently configured on a virtual system. However, IP-address-and-port-to-username mapping information from Terminal Server agents and group mappings are not shared between the User-ID hub and the connected virtual systems.

STEP 1 | Assign the [virtual system](#) as a User-ID hub.

1. Select **Device > Virtual Systems**, then either select an existing virtual system or **Add** a virtual system.
2. On the **Resource** tab, select **Make this vsys a User-ID data hub**.

3. Click **Yes** to confirm, then click **OK**.

STEP 2 | For any existing virtual systems, transfer the configuration for the User-ID sources you want to share (such as monitored servers and User-ID agents) to the hub and then remove the duplicate sources from the existing virtual systems.

This consolidates the User-ID configuration for operational simplicity. By configuring the hub to monitor servers and connect to agents that were previously monitored by other virtual systems, the hub can now collect the user mapping information instead of having each virtual system collect it independently. If there are any mappings that you don't want to share across virtual systems, leave the sources on a virtual system that will not be used as the hub.

STEP 3 | **Commit** the changes to enable the User-ID hub and begin collecting mappings for the consolidated sources.

STEP 4 | Confirm the User-ID hub is mapping the users by entering the following commands:

- **show user ip-user-mapping all**—The output displays the IP-address-to-username-mappings and which virtual system provided the mappings.

```
admin@PA-5260> show user ip-user-mapping all
```

IP	Vsys	From	User
IdleTimeout(s)	MaxTimeout(s)		
192.0.2.0	vsys2 (User-ID Hub)	UIA	api-panorama\wrah51
Never			Never
192.0.2.255	vsys1	UIA	api-panorama\pvdi4d
Never			Never
198.51.100.0	vsys2 (User-ID Hub)	UIA	api-panorama\bvxfgz
Never			Never
198.51.100.255	vsys1	UIA	api-panorama\e8r3k4
Never			Never
203.0.113.0	vsys1	UIA	api-panorama\4zr0l3
Never			Never
203.0.113.255	vsys1	UIA	api-panorama\cff4br
Never			Never
...			

- **show user user-id-agent state all**—The output displays which virtual system is serving as the User-ID hub.

```
admin@PA-5260> show user user-id-agent state all...Agent: UIA-Win2012-
panwqa-org(vsys:
vsys2(User-ID Hub)) Host: 203.0.113.255...
```

User-ID Support for Large Numbers of Terminal Servers

The number of [terminal servers](#) that you can secure with User-ID has been increased for many firewall models, providing user-based policy enforcement and visibility for more terminal server users. Previously, enabling User-ID for over 1,000 terminal servers required a network redesign, which included configuring additional firewalls to segment users and routing the traffic to the terminal servers communicating with those firewalls. Now, you can configure more Terminal Services agents to secure users who access applications on terminal servers without changing your network infrastructure.



For optimal configuration, update the TS agent to the latest version.

The following table shows the number of TS agents supported for each hardware-based and VM-Series firewall model with increased TS agent capacity. All other hardware-based and VM-Series firewall models not listed below retain their existing capacities.

Firewall Model	Previous Capacity	New Capacity
PA-5200 series, VM-700	1000	2500
PA-7080, PA-7050	1000	2000
PA-7050 SMC-B	not applicable	2500
PA-3260, PA-3250, PA-3220	400	2000
PA-800 series	400	1000

In addition, you can now specify a hostname as an alternative IP address. The hostname must resolve to a static IP address. If the hostname resolves to multiple IP addresses, the TS agent uses the first IP address in the list. To view the alternate IP addresses, use **show user ip-port-user-mapping** command.

WildFire Features

- > Increased WildFire File Forwarding Capacity
- > WildFire Appliance Archive Support

Increased WildFire File Forwarding Capacity

The maximum and default WildFire file forwarding sizes and rates are increased in PAN-OS® 9.0 to provide optimal visibility and detection. Based on Palo Alto Network's data analytics, the new default capacities protect against the majority of threats, and is a best practice to use the new default values.



The forwarding capacities for Traps, Aperture, and Magnifier have not changed. For additional information about the file forwarding capacity of these products and other public/API integrations, refer to [the product documentation](#).

File Type	PAN-OS 9.0 Default File Forwarding Sizes	PAN-OS 9.0 Size Limits
pe	16MB	1-50MB
apk	10MB	1-50MB
pdf	3,072KB	100-51,200KB
ms-office	16,384KB	200-51,200KB
jar	5MB	1-20MB
flash	5MB	1-10MB
MacOSX	10MB	1-50MB
archive	50MB	1-50MB
linux	50MB	1-50MB



The default forwarding values might change over time based on the current version of PAN-OS or the content release version. To view the file size ranges and defaults:

- *Web Interface—From the Device > Setup > WildFire > General Settings window, select and clear a Size Limit field, and then press enter to update the field.*
- *CLI—From a terminal emulator, connect to the firewall CLI and issue the following command: `show wildfire file-size-limits`.*

STEP 1 | Log in to the firewall and verify the WildFirefile forwarding size limits.

General Settings

WildFire Public Cloud: wildfire.paloaltonetworks.com

WildFire Private Cloud:

☐ Use Proxy Settings for Private Cloud

File Type	Size Limit
pe (MB)	16
apk (MB)	10
pdf (KB)	3000
ms-office (KB)	16000
jar (MB)	5
flash (MB)	5
MacOSX (MB)	10
archive (MB)	50
linux (MB)	50

☒ Report Benign Files

☒ Report Grayware Files

OK Cancel

Size limits shown here do not necessarily reflect current defaults



As a WildFire best practice, Palo Alto Networks recommends using the default file forwarding sizes. These values are designed to include the vast majority of malware that are likely to be encountered in real-world scenarios. Very large files that are beyond the size limits are excluded.

STEP 2 | Commit your configuration updates.

STEP 3 | Verify that the firewall is forwarding filesto the WildFire public cloud.

WildFire Appliance Archive Support

The WildFire appliance can now analyze and classify archive (RAR and 7-Zip) files with malicious, benign, or grayware verdicts. Previously this feature was only present in the WildFire cloud. This analysis capability has now been expanded to include WildFire appliances running PAN-OS 9.0 and later.



- When any file contained within an archive is determined to be malicious, the archive file is considered malicious by WildFire.
- Archive files that are multi-part or password protected cannot be analyzed.

The WildFire appliance is capable of analyzing the following archive file types:

- RAR—Supports Roshal Archive (.rar) files.
- 7-Zip—Supports (.7z) files.

To forward archive files for analysis, the **WildFire Analysis Profile** on the firewall must be configured to forward the **archive** file type or **Any** unknown files to the WildFire private cloud.

1. Enable file type forwarding.
 1. Select **Objects > Security Profiles > WildFire Analysis** and **Add** or modify a profile to define traffic to forward for WildFire analysis.
 2. Add or modify a profile rule, select **file type**, and set the rule to forward the new **Any** file type. You can also specify the **archive** file type if you want to forward only archives.



Profile rules with the file type set to Any forward all file types for WildFire analysis.

3. Select Destination and set the profile rule to forward the files to the **private-cloud**.
 4. Click **OK** to save the new or modified WildFire Analysis profile.
2. Attach the WildFire Analysis profile to a security policy rule—traffic matched to the policy rule is forwarded for WildFire Analysis.
 1. Select **Policies > Security** and **Add** or modify a security policy rule.
 2. Select **Actions** and set the **Profile Type** to **Profiles**.
 3. Select the newly-created **WildFire Analysis** profile.
 4. Click **OK** to save the security policy rule.



For detailed steps to configure a WildFire Analysis profile and to attach the profile to a security policy rule, see [Forward Files for WildFire Analysis](#).

3. Select **Monitor > WildFire Submissions** to find WildFire verdicts and analysis reports for archive files that have been submitted by the firewall.

