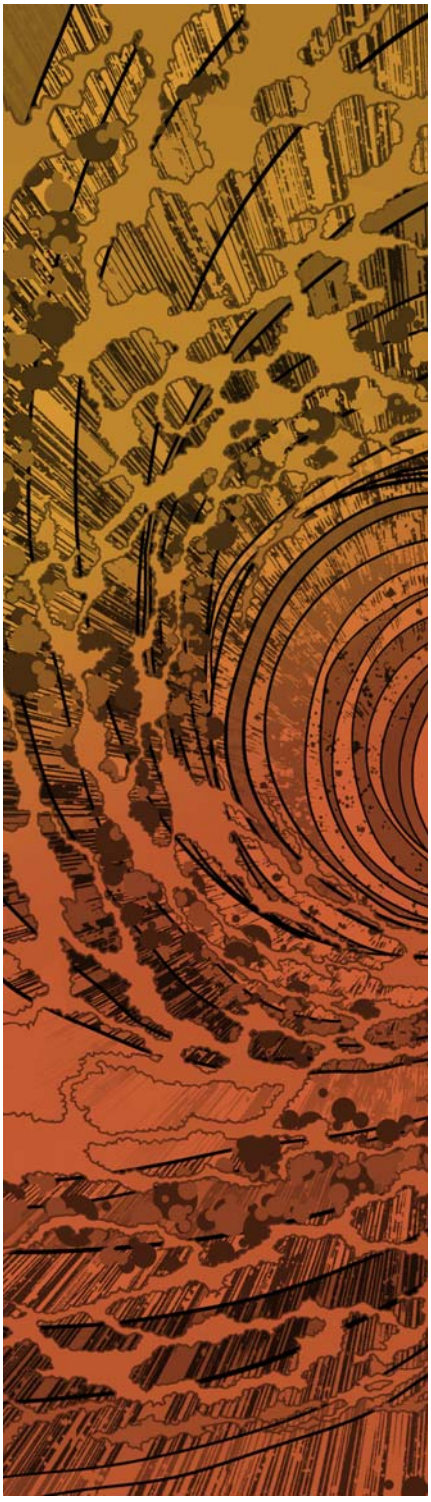


paloalto NETWORKS®

PAN-OS® New Features Guide

Version 7.1

Contact Information

Corporate Headquarters:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About this Guide

This guide describes how to use the new features introduced in PAN-OS 7.1. For additional information, refer to the following resources:

- For information on the additional capabilities and for instructions on configuring the features on the firewall, refer to https://www.paloaltonetworks.com/documentation.
- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/support/tabs/overview.html.
- For the most current PAN-OS and Panorama 7.1 release notes, go to https://www.paloaltonetworks.com/documentation/71/pan-os/pan-os-release-notes.html.

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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Revision Date: May 11, 2017

Table of Contents

Upgrade to PAN-OS 7.1 7
Upgrade/Downgrade Considerations 8
Upgrade the Firewall to PAN-OS 7.1 12
Upgrade Firewalls Using Panorama 12
Upgrade a Firewall to PAN-OS 7.1 15
Upgrade an HA Firewall Pair to PAN-OS 7.1 16
Downgrade from PAN-OS 7.1 20
Downgrade to a Previous Maintenance Release 21
Downgrade to a Previous Feature Release 22
Downgrade While Maintaining Enhanced Capacities on PA-3050 & PA-3020 Firewalls . 23

Management Features 25
Commit Queues 26
Extended SNMP Support 28
Banners and Message of the Day 29
Support for 4,096-bit RSA Certificates 30
Bootstrapping Firewalls for Rapid Deployment 31
Bootstrap a Hardware-Based Firewall 32
Bootstrap a VM-Series Firewall 32
Administrator Login Activity Indicators 33
PAN-OS XML API Request for Version 34
PAN-OS Log Integration with AutoFocus 35
Unified Logs 36

App-ID Features 39
PDF Report for Visibility into SaaS Applications 40

Virtualization Features 43
Support for ELB on the VM-Series Firewalls in AWS 44
VM-Series Firewall and Amazon ELB 44
Use the AWS Management Console to Swap the Management Interface 44
Configure ELB Health Checks 46
Support for Multi-Tenancy & Multiple Sets of Policy Rules: VM-Series NSX Edition Firewall 47
VM-Series for Microsoft Hyper-V 49
Support for VMware Tools on Panorama and VM-Series on ESXi 50
Support for Device Group Hierarchy in the VM-Series NSX edition firewall 51
VM-Series Firewall in Microsoft Azure 52
Support for Bootstrapping VM-Series Firewalls 53

WildFire Features 55
WildFire EU Cloud 56
Submit Samples to the WildFire EU Cloud 56
Mac OS X File Analysis 58
Manually or Programmatically Submit Mac OS X Files 58
Enable the Firewall to Forward Mac OS X Files 58
Five Minute WildFire Updates 60
New WildFire API Features 61

Content Inspection Features 63
Support for Custom Domains in an External Dynamic List 64
Support for URLs in an External Dynamic List 65
Enhanced Security for URL Category and Application-Based Policy 66

GlobalProtect Features 67
GlobalProtect App for Chrome OS 68
Prerequisites for the GlobalProtect App for Chrome OS 68
Configure the GlobalProtect App for Chrome OS 68
Deploy the GlobalProtect App for Chrome OS 72
GlobalProtect App for Windows Phone 73
GlobalProtect App for Windows 10 UWP Feature Support 73
Prerequisites for GlobalProtect App for Windows 10 UWP 74
Configure the GlobalProtect App for Windows 10 UWP 74
Obtain the GlobalProtect App for Windows 10 UWP 77
Set Up the GlobalProtect App for Windows 10 UWP 77
Use the GlobalProtect App for Windows 10 UWP 78
Simplified GlobalProtect Agent User Interface for Windows and Mac OS 80
Dynamic GlobalProtect App Customization 81
GlobalProtect App Display Options 81
GlobalProtect App User Behavior Options 82
GlobalProtect App Behavior Options 83
Enhanced Two-Factor Authentication 85
Dynamic Certificate Distribution Using SCEP 85
Secure Encrypted Cookies for Simplified Authentication 85
Client Authentication Configuration by Operating System or Browser 87
Kerberos for Internal Gateway for Windows 89
Customizable Password Expiry Notification Message 92
Enhanced Authentication Challenge Support for Android and iOS Devices 93
Block Access from Lost or Stolen and Unknown Devices 94
Block Device Access from an Unknown Device 94
Block Access from a Lost or Stolen Device 94
Certificate Selection by OID 95
Save Username Only Option 96
Use Address Objects in a GlobalProtect Gateway Client Configuration 97

Maximum Internal Gateway Connection Retry Attempts 99
GlobalProtect Notification Suppression on Windows. 100
Disable GlobalProtect Without Comment 100
Pre-logon then On-Demand Connect Method. 101
Enforce GlobalProtect for Network Access 104
Connection Behavior on Smart Card Removal 106

User-ID Features 107
User-ID Redistribution Enhancement 108
Ignore User List Configurable in Web Interface. 110
User Group Capacity Increase. 111

Networking Features 113
Failure Detection with BFD 114
LACP and LLDP Pre-Negotiation on an HA Passive Firewall. 115
LACP and LLDP Pre-Negotiation Support 115
Enable LACP and LLDP Pre-Negotiation on an HA Passive Firewall 116
Binding a Floating IP Address to an HA Active-Primary Firewall 117
Multicast Route Setup Buffering 118
Per-VLAN Spanning Tree (PVST+) BPDU Rewrite 119
Configurable MSS Adjustment Size 122
DHCP Client Support on Management Interface 123
PA-3000 Series and PA-500 Firewall Capacity Increases 124
SSL/SSH Session End Reasons 125
Diagnose SSL/SSH Session Terminations 125
Monitor SSL/SSH Session Termination Events. 126
Fast Identification and Mitigation of Sessions That Overutilize the Packet Buffer 127
Identify Sessions That Use an Excessive Percentage of the Packet Buffer 127
Discard a Session Without a Commit 129

Decryption Features 131
Transparent Certificate Distribution for SSL Forward Proxy. 132
Perfect Forward Secrecy (PFS) Support 133

VPN Features 135
DES Support for Crypto Profiles. 136

Panorama Features. 139
Role Privileges for Commit Types. 140
Increased (8TB) Disk Support on the Panorama Virtual Appliance. 142

Upgrade to PAN-OS 7.1

- Upgrade/Downgrade Considerations
- Upgrade the Firewall to PAN-OS 7.1
- Downgrade from PAN-OS 7.1

Upgrade/Downgrade Considerations

Table: PAN-OS 7.1 Upgrade/Downgrade Considerations lists the new features that have upgrade or downgrade impacts. Make sure you understand all potential changes before you upgrade to or downgrade from PAN-OS 7.1. For additional information about this release, refer to the PAN-OS 7.1 Release Notes.

Table: PAN-OS 7.1 Upgrade/Downgrade Considerations

Feature	Upgrade Considerations	Downgrade Considerations
Role Privileges for Commit Types		If the permission for any commit type is disabled in a Panorama Admin Role profile, the permissions for all commit types are disabled for that profile after a downgrade.
User Group Capacity Increase		Before downgrading a PA-5060 or PA-7000 Series firewall that has the multiple virtual systems capability disabled and that uses more than 640 distinct user groups in policies, you must reduce the number of groups to 640 or less.
User-ID WMI Client Probing	In PAN-OS 7.0 and earlier releases, client probing that uses Windows Management Instrumentation (WMI) includes all public and private IPv4 and IPv6 addresses by default. However, after you upgrade to PAN-OS 7.1, the default for WMI probing is to exclude public IPv4 addresses. (Public IPv4 addresses are those outside the scope of RFC 1918 and RFC 3927). To use WMI probing for public IPv4 addresses after the upgrade, you must add their subnetworks to the User-ID agent Include Networks list.	
8TB Disk Support on the Panorama Virtual Appliance	After you upgrade to Panorama 7.1, the Panorama virtual appliance will continue using only 2TB of any existing virtual disk that exceeds that capacity. After upgrading, you must manually add a virtual disk of up to 8TB before Panorama can use more than the 2TB limit.	If you added a virtual disk of more than 2TB to the Panorama virtual appliance, you must remove the disk before you can downgrade to a release earlier than Panorama 7.1.

Feature	Upgrade Considerations	Downgrade Considerations
Federal Information Processing Standard (FIPS) Mode	If your firewall is running a PAN-OS 6.1 or earlier release and is in FIPS mode, you must Enable FIPS and Common Criteria Support using **Set CCEAL4 Mode** before you upgrade to PAN-OS 7.0.1 or a later release. If you do not change to CCEAL4 mode before you upgrade, the firewall will enter maintenance mode because FIPS mode is not supported as of PAN-OS 7.0.1.  After you change from FIPS mode to CCEAL4 mode, you will need to import the saved configuration backup that you created prior to the mode change. If the configuration contains IKE and IPSec crypto profiles that use 3DES, you will need to delete the profiles and create new profiles using AES because 3DES is not supported in CCEAL4 mode.	
DES Support for Crypto Profiles		When downgrading to an earlier PAN-OS version, the following actions occur: • DES is removed from the crypto profile. If DES was the only encryption type in the crypto profile, then DES is converted to 3DES. • If DES was used in an IPSec tunnel configuration that used a manual key, the IPSec tunnel entry is removed from the configuration. After a reboot, any such IPSec tunnels no longer exist in the running configuration.
Custom Application Signatures		Before downgrading to a release earlier than PAN-OS 7.0, you must remove any custom application signatures that have the following settings: • **Operator** set to **Greater Than** or **Less Than** • **Operator** set to **Equal To** and a **Context** set to any value besides **unknown-req-tcp**, **unknown-rsp-tcp**, **unknown-req-udp**, or **unknown-rsp-udp**
Sinkholing of DNS Signatures	After you upgrade, all Palo Alto Networks DNS signatures are enabled by default. The default action for the DNS Signatures is sinkhole, and the sinkhole IP address is a Palo Alto Networks server (71.15.192.112). This IP address is not static and can change because it is pushed using Palo Alto Networks content updates.	

Feature	Upgrade Considerations	Downgrade Considerations
Support for Multi-Tenancy and Multiple Policy Sets on the VM-Series NSX Edition Firewall	If you configured the VMware Service Manager on Panorama, note the following changes that occur after you upgrade to Panorama 7.1: • The VMware Service Manager configuration that is required for enabling communication between Panorama and the NSX Manager is separated from the Service Definition. • A new Service Definition named `Palo Alto Networks NGFW` is created. This service definition includes the configuration for deploying VM-Series firewalls. It also includes a template, device group, link to the OVA for the PAN-OS version, and the auth codes you configured on the VMware service manager in the earlier version. If you did not create a template in the earlier version, then a default template called NSX_TPL is created for you. • A zone called Palo Alto Networks profile 1 is auto-generated within the template. On a Template and Device Group Commit, the VM-Series firewalls will generate a pair of virtual wire subinterfaces (ethernet1/1.2 and ethernet1/2.2) and bind the pair to this new zone. • All existing policy rules are retained with source and destination zone set to 'any'. These rules are functional and you do not need to modify the rules.	
External Dynamic List for IP Addresses	After you upgrade, Dynamic Block List for IP addresses are renamed to **External Dynamic List** of **Type** IP Address. The earlier maximum limit 10 Dynamic Block Lists for IP addresses has changed in PAN-OS 7.1. On each firewall platform, you can now configure a maximum of 30 unique sources for External Dynamic Lists of type IP address, URL or Domain. The firewall does not impose a limit on the number of lists of a specific type. The PA-5000 Series and the PA-7000 Series firewalls support a maximum of 150,000 total IP addresses; all other platforms support a maximum of 50,000 total IP addresses. No limits are enforced for the number of IP addresses per list. When the maximum supported IP address limit is reached on the firewall, the firewall generates a syslog message.	

Feature	Upgrade Considerations	Downgrade Considerations
PA-3000 Series and PA-500 Firewall Capacity Increases	When you upgrade to PAN-OS 7.1, the ARP table capacity automatically increases. To avoid a mismatch when upgrading a pair of HA firewalls, you should upgrade both HA peers within a short period of time. You should also clear the ARP cache (`clear arp`) on both HA peers before you upgrade.	
Save User Credentials	The **Allow user to save password** option, which was available in PAN-OS 7.0, is superseded by the **Save User Credentials** setting in PAN-OS 7.1. After you upgrade the firewall or Panorama to PAN-OS 7.1, the setting is discarded. Because the default behavior—which allows GlobalProtect to save user credentials—is the same for both options, no additional configuration is required to retain this behavior. However, to enforce behavior other than the default—for example, to prevent GlobalProtect from saving credentials altogether or from saving the password only—you must manually configure the **Save User Credentials** option after upgrading to PAN-OS 7.1.	
Authentication with Secure Encrypted Cookies	The **Authentication Modifier** option, which was available in PAN-OS 7.0, is superseded by the **Authentication Override** options in PAN-OS 7.1. After you upgrade the firewall or Panorama to PAN-OS 7.1, any authentication modifier settings are discarded. Because the new **Authentication Override** options are disabled by default, to configure GlobalProtect portals and gateways to accept secure encrypted cookies, you must manually configure the new **Authentication Override** options in PAN-OS 7.1.	
Gateway Configuration with Tunnel Mode		When tunnel mode is enabled in a GlobalProtect gateway configuration, the gateway configuration is discarded after a downgrade to an earlier major release unless you use the automatically generated saved configuration prior to upgrading.
GlobalProtect portals and gateways		Loading a configuration other than running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release removes authentication profiles from GlobalProtect portals and gateways, which causes an auto-commit failure. To prevent this issue, select running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release.

Upgrade the Firewall to PAN-OS 7.1

How you upgrade to PAN-OS 7.1 depends on whether you have standalone firewalls or firewalls in a high availability (HA) configuration and, for either scenario, whether Panorama manages your firewalls. Review the PAN-OS 7.1 Release Notes and then follow the procedure specific to your configuration:

- Upgrade Firewalls Using Panorama
- Upgrade a Firewall to PAN-OS 7.1
- Upgrade an HA Firewall Pair to PAN-OS 7.1

When upgrading firewalls that you manage with Panorama or firewalls that are configured to forward content to a WF-500 appliance, you must first upgrade Panorama and its Log Collectors and upgrade the WF-500 appliance, before upgrading the firewalls.

Upgrade Firewalls Using Panorama

Review the PAN-OS 7.1 Release Notes and then use the following procedure to upgrade firewalls that Panorama manages. This procedure applies to standalone firewalls and firewalls deployed in a high availability (HA) configuration.

When upgrading firewalls that you manage with Panorama, you must upgrade Panorama and its Log Collectors before you upgrade the firewalls.

Upgrade Firewalls Using Panorama		
Step 1	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. Log in to Panorama, select **Panorama > Setup > Operations**, and **Export Panorama and devices config bundle** to generate and export the latest configuration backup of Panorama and of each managed device. 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 2	Install the content updates.  Make sure the firewalls you plan to upgrade are running content release version 564 or later.	1. Select **Panorama > Device Deployment > Dynamic Updates**. 2. **Check Now** (located in the lower left-hand corner of the window) to check for the latest updates. If an update is available, the Action column displays a **Download** link. 3. **Download** the desired version. After a successful download, the link in the Action column changes from **Download** to **Install**. 4. Click **Install**, select the devices on which you want to install the update, and click **OK**.

Upgrade Firewalls Using Panorama (Continued)		
Step 3	Determine the software upgrade path. You cannot skip installation of any major release versions in the path to your target PAN-OS release. For example, if you intend to upgrade from PAN-OS 6.0.13 to PAN-OS 7.1.1, you must: • Download and install PAN-OS 6.1.0 and reboot. • Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0). • Download PAN-OS 7.1.0 (you do not need to install it). • Download and install PAN-OS 7.1.1 and reboot.	1. To access the web interface of the firewall you intend to upgrade, use the **Context** drop-down in Panorama or log in to the firewall directly. 2. Select **Device > Software**. 3. Check which version has a check mark in the Currently Installed column and proceed as follows: • If PAN-OS 7.0.1 or later is currently installed, continue to Step 4. • If a version earlier than PAN-OS 7.0.1 is currently installed, follow the upgrade path to 7.0.1 before you upgrade to 7.1. Refer to the Release Notes for your currently installed PAN-OS version for upgrade instructions.
Step 4	Download the software updates.	1. On Panorama, select **Panorama > Device Deployment > Software** and **Check Now** for the latest updates. If an update is available, the Action column displays a **Download** link. 2. **Download** the file or files that correspond to the Platform of the firewalls to which you are upgrading and the version to which you need to upgrade (including any intermediate major release versions). You must download a separate installation file for each platform you intend to upgrade. For example, to upgrade your PA-3050 firewalls and PA-5060 firewalls to 7.1.0, download the images that have filename PanOS_3000-7.1.0 and PanOS_5000-7.1.0. After a successful download, the Action column changes to **Install** for that image.

Upgrade Firewalls Using Panorama (Continued)	
Step 5 Install the software updates on the firewalls.  To avoid downtime when updating the software on firewalls in an HA configuration, update one peer at a time. For firewalls in an active/active configuration, it doesn't matter which HA peer you update first. For an active/passive configuration, you must update the passive peer first, suspend the active peer (fail over), update the active peer, and then return the active peer to a functional state (fail back).	Perform the steps that apply to your firewall deployment: **Non-HA Firewalls** Click **Install** in the Action column for the appropriate update, select all firewalls you intend to update, **Reboot device after install**, and click **OK**. **Active/Active HA Firewalls** 1. Click **Install**, clear **Group HA Peers**, select either of the HA peers, **Reboot device after install**, and click **OK**. Wait for the firewall to finish rebooting before you proceed. 2. Click **Install**, clear **Group HA Peers**, select the HA peer that you didn't update in the previous step, **Reboot device after install**, and click **OK**. **Active/Passive HA Firewalls** In this example, the active firewall is named fw1 and the passive firewall is named fw2: 1. Click **Install** in the Action column for the appropriate update, clear **Group HA Peers**, select fw2, **Reboot device after install**, and click **OK**. Wait for fw2 to finish rebooting before you proceed. 2. Access fw1, select **Device > High Availability > Operational Commands**, and **Suspend local device**. 3. Access fw2 and, on the **Dashboard** High Availability widget, verify that the **Local** firewall state is **active** and the **Peer** firewall is **suspended**. 4. Access Panorama, select **Panorama > Device Deployment > Software**, click **Install** in the Action column for the appropriate update, clear **Group HA Peers**, select fw1, **Reboot device after install**, and click **OK**. Wait for fw1 to finish rebooting before you proceed. 5. Access fw1, select **Device > High Availability > Operational Commands**, and click **Make local device functional**. Wait two minutes before you proceed. 6. On fw1, select the **Dashboard** tab and, in the High Availability widget, verify that the **Local** firewall state is **active** and the **Peer** firewall is **passive**.
Step 6 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.

Upgrade a Firewall to PAN-OS 7.1

Review the PAN-OS 7.1 Release Notes and then use the following procedure to upgrade a firewall not in an HA configuration to PAN-OS 7.1.

When upgrading firewalls configured to forward content to a WF-500 appliance, you must first upgrade the WF-500 appliance to PAN-OS 7.1 before upgrading the connected firewalls.

Ensure the devices are connected to a reliable power source. A loss of power during an upgrade can make the devices unusable.

Upgrade PAN-OS		
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 **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	Make sure the firewall is running content release version 564 or later.	1. Select **Device > Dynamic Updates**. 2. Check the **Applications and Threats** or **Applications** section to determine what update is currently running. 3. If the firewall is not running the minimum required update, **Check Now** to retrieve a list of available updates. 4. Locate and **Download** the appropriate update. 5. After the download completes, **Install** the update.
Step 3	Determine the upgrade path. You cannot skip installation of any major releases in the path to your target PAN-OS version. Therefore, if you intend to upgrade to a version that is more than one major release away, you must still download, install, and reboot the firewall for each intermediate major release along the upgrade path. For example, if you want to upgrade from PAN-OS 6.0.13 to PAN-OS 7.1.1, you must: • Download and install PAN-OS 6.1.0 and reboot. • Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release, not 7.0.0). • Download PAN-OS 7.1.0 (you do not need to install it). • Download and install PAN-OS 7.1.1 and reboot.	1. Select **Device > Software**. 2. Check which version has a check mark in the Currently Installed column and proceed as follows: • If PAN-OS 7.0.1 or a later release is currently installed, continue to Step 4. • If a version of PAN-OS prior to 7.0.1 is currently installed, you must follow the upgrade path to 7.0.1 before you can upgrade to 7.1. Refer to the Release Notes for your currently installed PAN-OS version for upgrade instructions.

Upgrade PAN-OS (Continued)		
Step 4	Install PAN-OS 7.1. 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** for latest updates. 2. Locate and **Download** the version to which you intend to upgrade. 3. After the download completes, **Install** the update. 4. After the installation successfully completes, 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** (Device Operations section).
Step 5	Verify that the firewall is passing traffic.	Select **Monitor > Session Browser**.

Upgrade an HA Firewall Pair to PAN-OS 7.1

Review the PAN-OS 7.1 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.

When upgrading peers in an HA configuration, you must upgrade each firewall separately. Consequently, there is a period of time when PAN-OS versions differ on the individual firewalls in the HA pair. If you have session synchronization enabled, this will continue to function during the upgrade process as long as you are upgrading from one feature release to the next consecutive feature release, PAN-OS 7.0.x to PAN-OS 7.1 in this case. If you are upgrading the pair from an older feature release of PAN-OS, session syncing between the firewalls will not work and, if a failover occurs before both firewalls are running the same version of PAN-OS, session forwarding could be impacted. In this case, if session continuity is required, you must temporarily permit non-syn-tcp while the session table is rebuilt as describe in the following procedure.

Ensure the devices are connected to a reliable power source. A loss of power during an upgrade can make the devices unusable.

When you upgrade to PAN-OS 7.1, the ARP table capacity automatically increases. To avoid a mismatch, you should upgrade both peers within a short period of time. You should also clear the ARP cache (`clear arp`) on both peers before you upgrade.

Upgrade PAN-OS		
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 **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.

Upgrade PAN-OS (Continued)		
Step 2	Make sure each device is running content release version 564 or later.	1. Select **Device > Dynamic Updates**. 2. Check the **Applications and Threats** or **Applications** section to determine what update is currently running. 3. If the firewall is not running the minimum required update, **Check Now** to retrieve a list of available updates. 4. Locate and **Download** the content release version you intend to install. 5. After the download completes, **Install** the update.
Step 3	Determine the upgrade path. You cannot skip installation of any major releases in the path to your desired PAN-OS version. Therefore, if you intend to upgrade to a version that is more than one major release away, you must download, install, and reboot the firewall for each intermediate major PAN-OS releases along the upgrade path. For example, if you want to upgrade from PAN-OS 6.0.13 to PAN-OS 7.1.1, you must: • Download and install PAN-OS 6.1.0 and reboot. • Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0). • Download PAN-OS 7.1.0 (you do not need to install it). • Download and install PAN-OS 7.1.1 and reboot.	1. Select **Device > Software**. 2. Check which version has a check mark in the Currently Installed column and proceed as follows: • If PAN-OS 7.0.1 or a later release is currently installed, continue to Step 4. • If a version of PAN-OS prior to 7.0.1 is currently installed, you must follow the upgrade path to 7.0.1 before you can upgrade to 7.1. Refer to the Release Notes for your currently installed PAN-OS version for upgrade instructions.
Step 4	Install PAN-OS 7.1 on the passive device (active/passive) or on the active-secondary device (active/active). 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** for the latest updates. 2. Locate and **Download** the version to which you intend to upgrade. 3. After the download completes, **Install** the update. 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** (Device Operations section). After the reboot, the device will not be functional until the active/active-primary device is suspended.

Upgrade PAN-OS (Continued)		
Step 5	Suspend the active/active-primary firewall.	1. On the active (active-passive) or active-primary (active-active) peer, select **Device > High Availability > Operational Commands**. 2. **Suspend local device**. 3. Select **Dashboard** and verify that the state of the passive device changes to active in the High Availability widget. 4. Verify that the firewall that took over as active (or active-primary) and is passing traffic (**Monitor > Session Browser**). 5. (Optional) If you have session synchronization enabled and you are currently running a PAN-OS version prior to 6.1.0, run the `set session tcp-reject-non-syn no` operational command. This will rebuild the session table so that sessions that started prior to the upgrade will continue.
Step 6	Install PAN-OS 7.1 on the other peer in the pair. 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** for the latest updates. 2. Locate and **Download** the version to which you intend to upgrade. 3. After the download completes, **Install** the update. 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** in the Device Operations section. After the reboot, the device will not be functional until the active/active-primary device is suspended. 5. (Optional) If you configured the firewall to temporarily allow non-syn-tcp traffic in order to enable the firewall to rebuild the session table in Step 4, revert back by running the `set session tcp-reject-non-syn yes` command. If the preemptive option is configured, the current passive peer will revert to active when state synchronization is complete.

Upgrade PAN-OS (Continued)		

Step 7	Verify that the firewalls are passing traffic as expected.
	In an active/passive deployment, the active peer (only) should be passing traffic while both peers should be passing traffic in an active/active deployment.
		Run the following CLI commands to confirm that the upgrade succeeded:
		• (Active peer(s) 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 show packets transmitted and the passive device will only show packets received.
		   If you have 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 bidirectional 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.

Downgrade from PAN-OS 7.1

The way you downgrade from PAN-OS 7.1 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 7.1 to 7.0 or 6.0 to 5.0) or you are downgrading to a maintenance release within the same feature release version (where the third digit in the release version changes, for example, from 7.1.1 to 7.1.0). When downgrading from one feature release to an earlier feature release, the configuration may be migrated to accommodate new features. Therefore, before downgrading you must restore the configuration for the feature release to which you are downgrading. You can downgrade from one maintenance release to another within the same feature release without having to worry about restoring the configuration:

- Downgrade to a Previous Maintenance Release
- Downgrade to a Previous Feature Release
- Downgrade While Maintaining Enhanced Capacities on PA-3050 Firewalls and PA-3020 Firewalls

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 7.1.1 to 7.0.9), not to downgrades to maintenance releases within the same feature release version (for example, 7.1.1 to 7.1.0).

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 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 7.1.1 to 7.1.0 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.

Downgrade to a Previous Maintenance 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. Select **Device > Setup > Operations** and **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 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. Select **Device > Software** and **Check Now** for available images. 2. Locate the version to which you want to downgrade. If the image is not already downloaded, then **Download** it. (If the image is already downloaded, you can skip this step.) 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, select **Device > Setup > Operations** and **Reboot Device** (Device Operations section).

Downgrade to a Previous Feature Release

This procedure will restore your device to the configuration that was running before you upgraded to a different feature release. Any changes made since the upgrade are lost so it is important to back up your current configuration so you can restore those changes when you return to the newer feature release.

Downgrades from PAN-OS 7.1 to any version earlier than PAN-OS 5.0.5 is not supported because the log management subsystem has been significantly enhanced between PAN-OS 5.0 and PAN-OS 6.0. Because of the changes implemented in the log partitions, a firewall that is downgraded to PAN-OS 5.0.4 and earlier releases cannot accurately estimate the disk capacity available for storing logs and the log partition can reach maximum capacity without a user notification. Such a situation allows the log partition to reach 100% capacity, which results in a loss of logs.

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

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. Select **Device > Setup > Operations** and **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 downgrade.
Step 2	Install the previous feature release image.  Autosave versions are created when you upgrade to a new release beginning with PAN-OS 4.1. If you are downgrading to a release prior to PAN-OS 4.1, you may need to do a factory reset and restore the device.	1. Select **Device > Software** and **Check Now** for available images. 2. Locate the image to which you want to downgrade. If the image is not already downloaded, then **Download** it. (If the image is already downloaded, you can skip this step.) 3. After the download completes, **Install** the image. 4. Select a configuration to load after the device reboots from the **Select a Config File for Downgrading** drop-down. In most cases, you should select the autosaved configuration that was created when you upgraded from the release to which you are now downgrading. For example, if you are running PAN-OS 7.1.1 and want to downgrade to PAN-OS 7.0.3, select autosave-7.0.3. 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, select **Device > Setup > Operations** and **Reboot Device** (Device Operations section).

Downgrade While Maintaining Enhanced Capacities on PA-3050 Firewalls and PA-3020 Firewalls

PA-3000 Series and PA-500 firewalls support larger capacities in PAN-OS 7.1 than in prior PAN-OS releases.

- If you want to downgrade a PA-3000 Series or PA-500 firewall to an older PAN-OS release, perform Step 1 through Step 5 and Step 8 to downgrade successfully.
- If you want to downgrade a PA-3000 Series firewall and preserve the capacity increases gained when upgrading to PAN-OS 7.1 but you have not used the `debug system arp-mac-capacity increase` operational command, then perform all steps in the following procedure.

Use the following procedure to downgrade PA-3000 Series and PA-500 firewalls and preserve PA-3000 Series firewall capacity increases on downgrade.

Downgrade PA-3000 Series and PA-500 Firewalls and Preserve PA-3000 Series Firewall Capacity Increases on Downgrade		
Step 1	Determine the decreased number of ARP entries the older release supports.	Access the Product Selection Tool and find the ARP capacity of the release to which you are downgrading.
Step 2	Determine if you currently have more static ARP entries than the number supported in Step 1.	1. In the CLI, use the `clear arp all` command to delete the dynamic ARP entries. 2. Use the `show arp all` command to display a count of all the ARP entries. Because you just deleted the dynamic ARP entries, only the static ARP entries are counted.
Step 3	Export the running configuration.	1. Select **Device > Setup > Operations > Save named configuration snapshot**, enter a **Name**, and click **OK**. 2. **Export named configuration snapshot**, select the name of the file you created from the drop-down, and click **OK**.
Step 4	If your current static ARP entries (determined by Step 2) exceed the decreased number of ARP entries supported (determined by Step 1), delete enough static ARP entries to get the firewall below the downgraded capacity.	1. Select **Network > Virtual Routers > Static Routes**. 2. Select **IPv4** or **IPv6**. 3. Select a static route and **Delete** it; repeat as necessary. 4. Click **OK** and **Commit**.
Step 5	Downgrade the PAN-OS version to 7.0.1.	Select **Device > Software**, select the 7.0.1 software image that is downloaded, and **Install** it.
Step 6	Enable larger capacities on a PA-3050 or PA-3020 firewall. This command is available only in PAN-OS 6.1.0 and PAN-OS 7.0.1.	In the CLI, use the `debug system arp-mac-capacity increase` operational command.
Step 7	Upgrade the PAN-OS version to 7.1.	Upgrade a Firewall to PAN-OS 7.1
Step 8	Import the saved configuration.	Select **Device > Setup > Operations > Import named configuration snapshot**, select the file you created in Step 3 to import, and click **OK**.
Step 9	Downgrade the PAN-OS version to 7.0.1 again.	Select **Device > Software**, select the 7.0.1 software image that is downloaded, and **Install** it.

Management Features

- Commit Queues
- Extended SNMP Support
- Banners and Message of the Day
- Support for 4,096-bit RSA Certificates
- Bootstrapping Firewalls for Rapid Deployment
- Administrator Login Activity Indicators
- PAN-OS XML API Request for Version
- PAN-OS Log Integration with AutoFocus
- Unified Logs

Commit Queues

The firewall and Panorama now queue commit operations so that you can initiate a new commit while a previous commit is still in progress. This enables you to activate configuration changes without having to coordinate commit times with other administrators. For example, you can initiate a local firewall commit while it is still receiving device group and template settings that a Panorama administrator committed. In Panorama, you can also initiate a single commit to push settings from multiple device groups that target different virtual systems on the same firewall instead of committing from one device group at a time.

The firewall and Panorama perform commits in the order you and other administrators initiate them. However, the firewall and Panorama prioritize automatic commits such as FQDN refreshes. If the queue already has the maximum number of administrator-initiated commits (varies by platform), the firewall or Panorama must begin processing a commit (remove it from the queue) before you can initiate a new commit.

If Panorama pushes configurations to the firewall, you must wait for the associated commit to finish processing before you can add more commits locally to the firewall queue. In the period after the firewall removes the Panorama-initiated commit from the queue but before that commit finishes processing, you cannot edit the firewall settings.

You can perform the following tasks to manage commit operations:

Manage Commit Requests	
• Add a description when initiating a commit. A brief summary of what changed in the configuration is useful to other administrators who want to know what changed without performing a configuration audit.	Click **Commit**, select options (these vary by firewall or Panorama platform), enter a **Description** of up to 512 characters, and click **Commit** again.
• View details about commits. For example, if the firewall takes longer than expected to start processing a commit, you can check which other commits are ahead of it in the commit queue.	1. Click **Tasks** at the bottom right of the web interface. For each commit, the Task Manager displays the Job ID, Status (pending, in progress, completed, or failed), Start Time (when you initiated the commit), End Time, and associated Messages. When the firewall or Panorama removes a commit from the queue to start processing that commit, the status changes from pending to in progress. The dialog displays progress as a completion percentage. The Messages column displays the dequeued time, the queue positions of pending commits, and whether the commit succeeded or failed. If the Messages column says `Too many messages`, click **Commit** in the task Type column to see the messages. 2. (Panorama only) **Show** the tasks for **Panorama** (default) or the firewall for which you want to see commit details. 3. Click **Commit Description** in the Messages column if you want to see the description for a commit.

Manage Commit Requests (Continued)	
• Cancel pending commits. Your administrator role must be Superuser, Superuser read-only, Device administrator (predefined on the firewall), or Panorama administrator (predefined on Panorama) to cancel pending commits; however, regardless of role, you cannot cancel commits that are in progress.	1. Click **Tasks** at the bottom right of the web interface. 2. (Panorama only) **Show** the tasks for **Panorama** (default) or the firewall for which you want to cancel commits. 3. Click **Clear Commit Queue**.

Extended SNMP Support

PAN-OS support for Simple Network Management Protocol (SNMP) now includes the following features. To access the latest MIBs, refer to SNMP MIB Files. For a list of supported traps, use an SNMP manager to view the **PAN-COMMON-MIB.my > panCommonEvents > panCommonEventsEvents > panCommonEventEventsV2** object. To view generated traps, use the PAN-TRAPS.my MIB.

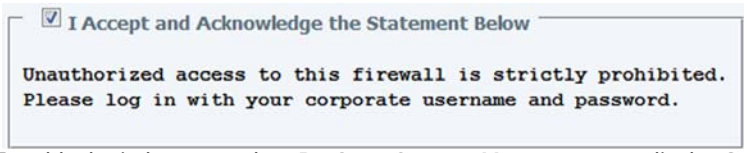
Feature	Description
Synchronization of SNMP Trap and MIB Information	When an event triggers SNMP trap generation (for example, an interface goes down), the firewall, Panorama virtual appliance, M-Series appliance, and WF-500 appliance now respond by updating the corresponding SNMP object (for example, the interfaces MIB) instead of waiting for the periodic update of all objects that occurs every ten seconds. This ensures that your network management system displays the latest information when it polls an object to confirm an event.
Commit Queues	The *panTraps* MIB now has traps that indicate the status of commit requests (added to queue, in progress, completed, or failed) to help you troubleshoot commit issues on the firewall or Panorama.
Failure Detection with BFD	The firewall now supports the BFD-STD-MIB and BFD traps so that you can monitor and receive alerts for communication failures between a firewall and its neighbor or peer.
DHCP Client Support on Management Interface	The firewall now supports DHCP traps for the management (MGT) interface so that you can troubleshoot issues that might occur when the MGT interface tries to receive its IP address from a DHCP server.

Banners and Message of the Day

You can now customize the firewall or Panorama web interface using the following options:

Configure Banners and Message of the Day

- Force administrators to acknowledge the login banner to ensure they see information they need to know before logging in, such as login instructions. The following is an example of a login banner:

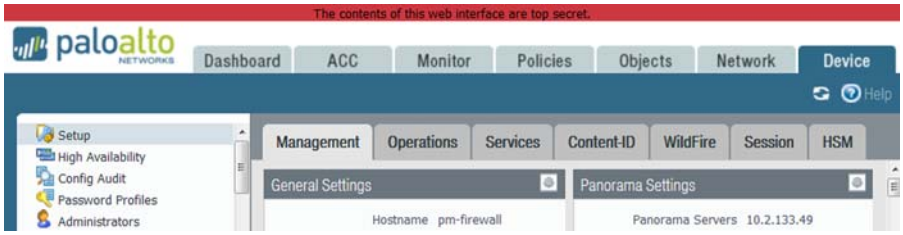


  To add a login banner, select **Device > Setup > Management**, edit the General Settings, configure the login banner, and then click **OK** and **Commit**.

- Add a *message of the day* that displays after administrators log in to ensure they see important information, such as a pending system restart that might affect the tasks they perform. Administrators will also see post-login messages that Palo Alto Networks embeds to highlight important information associated with software or content releases. The following is an example of an administrator-configured message of the day:

  To add a message of the day, select **Device** > **Setup** > **Management**, edit the Banners and Messages settings, enable and configure the **Message of the Day**, and click **OK**. A commit is not required.

- Add colored bands that highlight text across the top (*header banner*) and bottom (*footer banner*) of the web interface to ensure administrators see critical information, such as the classification level for firewall administration. The following is an example of a highlighted header banner indicating that the firewall web interface is classified as top secret:



  To add header and footer banners, select **Device** > **Setup** > **Management**, specify the **Header Banner**, optionally clear **Same Banner Header and Footer** and specify the **Footer Banner**, and then click **OK** and **Commit**.

Support for 4,096-bit RSA Certificates

The firewall and Panorama now support RSA certificates with 4,096-bit keys, which are more secure than smaller keys. You can use these certificates to authenticate clients, servers, users, and devices in multiple applications, including Captive Portal, GlobalProtect, site-to-site IPSec VPN, and web interface access.

The maximum key size is 3,072 bits for certificates that you generate on firewalls in FIPS mode and for certificates that are used in two-factor GlobalProtect authentication.

Generate a 4,096-bit RSA Certificate	
Step 1	Select **Device** > **Certificate Management** > **Certificates** > **Device Certificates** and **Generate** a new certificate.
Step 2	Select **Local** and enter a **Certificate Name**.
Step 3	Specify the **Common Name**—either the FQDN (recommended) or the IP address of the interface on which you will configure the service that will use this certificate.
Step 4	Select **Certificate Authority** (CA) if this is a CA certificate. Otherwise, from the **Signed By** drop-down, select the root CA certificate that will issue this certificate.
Step 5	Set the **Algorithm** to **RSA** (default) and the **Number of Bits** to **4096**.
Step 6	Select the **Digest** algorithm (default is **sha256**).
Step 7	Enter the **Expiration** period, which is the number of days for which the certificate is valid (default is 365).
Step 8	**Generate** the certificate.
Step 9	Click the certificate **Name** in the Device Certificates tab to edit it.
Step 10	Select the usage description(s) that correspond to the intended use of the certificate.
Step 11	Click **OK** and **Commit**.

Bootstrapping Firewalls for Rapid Deployment

Whether you are deploying a VM-Series firewall (on-demand deployment) or a hardware-based Palo Alto Networks next-generation firewall (mass rollout to remote sites), the bootstrapping process provides an agile, consistent, and scalable process for setting up a firewall with or without Internet access. PAN-OS support bootstrapping capability on all hardware-based firewalls and on VM-Series firewalls in the private cloud (ESXi, KVM, and Hyper-V) and public cloud (AWS and Azure). Additionally, starting with PAN-OS 7.1.4, PAN-OS supports bootstrapping in KVM in OpenStack.

Bootstrapping speeds up the process of configuring and licensing the firewall and making it operational on the network. This process allows you to choose whether to configure the firewall with only a basic configuration (init-cfg.txt file) so that it can connect to Panorama and obtain the complete configuration or to fully configure the firewall with the basic configuration and the optional bootstrap.xml file. When you include both files in the bootstrap package, the firewall merges the configurations from both of those files and, if any configuration settings overlap between the two, the firewall uses the settings defined in the init-cfg.txt file.

The following table shows the supported external devices and formats required for bootstrapping the firewall.

External Device for Bootstrapping (Bootstrap Package Format)	Hardware Firewalls	VM-Series Firewalls (Hypervisor Type)						
		ESXi	KVM	Hyper-V	AWS	Azure	KVM in OpenStack	NSX
CD-ROM (.iso)	—	Yes	Yes	Yes	—	—	—	N/A
Disk (.vhd)	—	—	—	—	—	Yes	—	
S3 Bucket	—	—	—	—	Yes	—	—	
USB Flash Drive (tar.gz)	Yes	—	—	—	—	—	—	
Config-Drive	—	—	—	—	—	—	Yes	

Use the following high-level workflows to guide you when bootstrapping:

- Bootstrap a Hardware-Based Firewall
- Bootstrap a VM-Series Firewall

Bootstrap a Hardware-Based Firewall

Bootstrap a Hardware-Based Firewall
• Upgrade the Firewall to PAN-OS 7.1 and Reset the Firewall to Factory Default Settings. For security reasons, you can only bootstrap a firewall when it is a factory default state.  To bootstrap a hardware-based firewall, you must first upgrade the firewall to PAN-OS 7.1 and perform a factory reset or private data reset on it. When firewalls ship with PAN-OS 7.1 preloaded on it, the bootstrap capability will be available out-of-the-box.
• Prepare a USB Flash Drive for Bootstrapping a Firewall.
• Bootstrap a Firewall Using a USB Flash Drive.
• Verify Bootstrap Completion. For details on bootstrapping the hardware-based firewall, refer to Bootstrap the Firewall.

Bootstrap a VM-Series Firewall

Bootstrap a VM-Series Firewall
• For security reasons, you can only bootstrap a firewall when it is in factory default state. If you want to bootstrap a VM-Series firewall that has been previously configured, Reset the Firewall to Factory Default Settings.
• Prepare the Bootstrap Package.

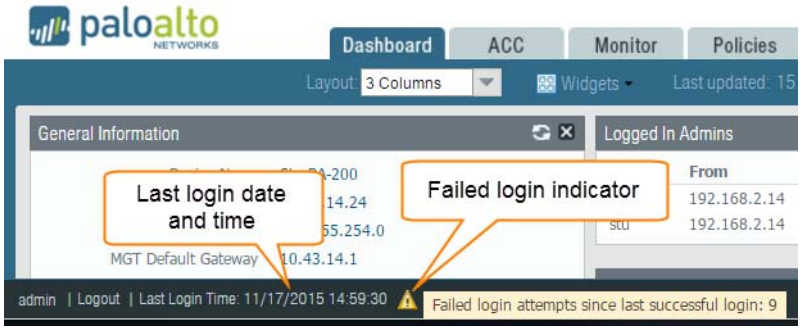
• Place the bootstrap package in the format required by your hypervisor and bootstrap the VM-Series firewall.
  • ESXi
  • Hyper-V
  • KVM
  • AWS
  • Azure
  • KVM in OpenStack

• Verify Bootstrap Completion. For details on bootstrapping the VM-Series firewall, refer to Bootstrap the VM-Series Firewall.

Administrator Login Activity Indicators

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

The Last Login Time information is located to the right of **Logout** at the bottom left of the web interface. If one or more failed login attempts occurred using your account since the last successful login, a caution symbol appears to the right of Last Login Time. Hover over the caution symbol to view the number of failed login attempts or click the symbol to view details about the events.



The PAN-OS Administrator's Guide provides more details on how to Use the Administrator Login Activity Indicators to Detect Account Misuse.

PAN-OS XML API Request for Version

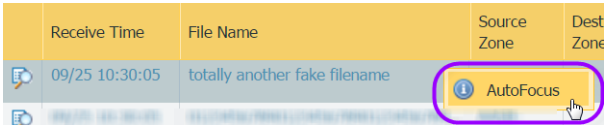
You can now use the PAN-OS XML API to show the PAN-OS version for a firewall or Panorama. In addition to the PAN-OS version, this new API request type (`type=version`) provides a direct way to obtain the serial number and model number.

PAN-OS Log Integration with AutoFocus

AutoFocus threat intelligence data is now integrated with the PAN-OS logs to provide context analysis for firewall events on network, industry, and global scales. On firewalls with an active AutoFocus license, you can now click any IP address, URL, user agent, filename, or hash included in a log entry to open an AutoFocus Threat Intelligence Summary of the latest findings for that artifact. The summary includes (but is not limited to):

- The total number of malware, grayware, and benign samples with which WildFire found the artifact.
- The latest WildFire submissions from your network that included the artifact.
- Passive DNS history for URLs, domains, and IP addresses.
- Threats that include the artifact that Unit 42 has identified as posing a direct security risk.

This immediate access to AutoFocus intelligence within the firewall or Panorama context enables you to quickly assess the pervasiveness and risk of an artifact along with the option to then add the artifact directly to an AutoFocus search.

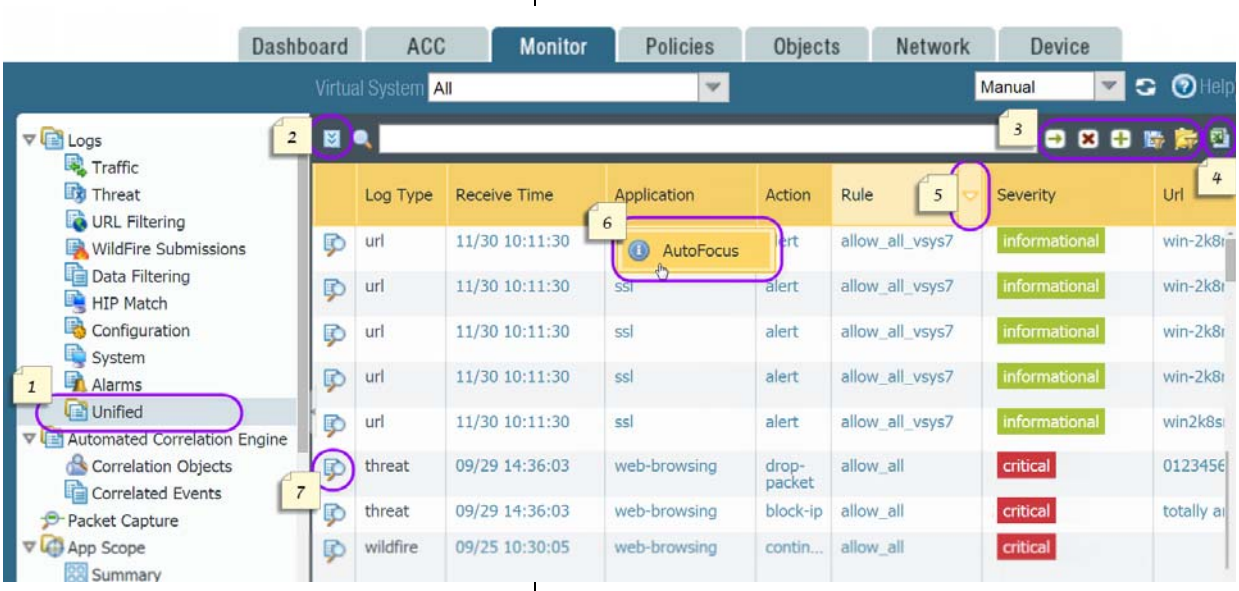
Find AutoFocus Threat Intelligence in PAN-OS Logs		
Step 1	Enable AutoFocus threat intelligence on the firewall.	
Step 2	Find the latest AutoFocus threat intelligence for firewall events.	1. Select **Monitor**. 2. View **Traffic**, **Threat**, **URL Filtering**, **WildFire Submissions**, **Data Filtering**, or **Unified** logs. 3. Hover over any IP Address, URL, User-ID, filename, or hash included in any log entry and click the arrow icon:  4. Click **AutoFocus:** 
Step 3	**Next Steps...** • Review the AutoFocus threat intelligence summary for a log entry artifact. • Explore more ways to use AutoFocus with a Palo Alto Networks firewall.	

Unified Logs

The firewall now provides a single Unified log set that enables you to monitor and filter events regardless of log type. The new unified log set includes Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs in a single view and you can choose to display some or all of these log types.

Additionally, with an active AutoFocus license, you can view AutoFocus threat intelligence for artifacts found in the Unified logs and filter firewall logs based on AutoFocus artifacts.

Unified logs have the same look and feel as other PAN-OS logs but with a few additions.

First Look at Unified Logs		
Step 1	Find unified logs (1).	Select **Monitor** > **Logs** > **Unified**.
		
Step 2	(New) Choose which log types (2) to display.	Select the down arrow to the left of the filter and select one or more of the log types to display: **traffic**, **threat**, **url**, **data**, and **wildfire**.
Step 3	Filter (3) unified logs.	Use the filter to search for specific attributes in log fields. Unified logs include all Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering log entries so you can now search for attributes across these log types with a single filter instead of filtering each log type separately.
Step 4	Export (4) unified logs.	Export the current log set to a comma-separated value (CSV) file.
Step 5	Adjust the log details (5) displayed.	Hover over any column header to adjust the visible columns. The column options for the Unified log view include all fields that are displayable for Traffic, Threat, URL Filtering, WildFire Submissions, and Data Filtering logs.

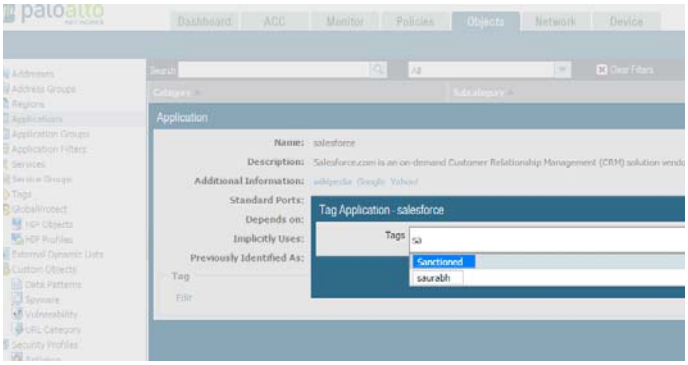
First Look at Unified Logs (Continued)		
Step 6	(With an AutoFocus License) Preview AutoFocus threat intelligence (6) for log entry data.	1. Enable AutoFocus threat intelligence on the firewall. 2. Click an IP address, URL, User-ID, filename, or hash artifact in a log entry to open the AutoFocus Threat Intelligence Summary of the latest findings and risk statistics for that artifact. The AutoFocus threat intelligence summary also allows you to add the artifact from the firewall directly to an AutoFocus search. For details, see View AutoFocus Threat Data for Logs. Explore more ways to use AutoFocus with a Palo Alto Networks firewall.
Step 7	View additional log entry details (7).	Click the spyglass to display a detailed log view for a single entry. Log entry details vary depending on the type of log you are viewing (Traffic, Threat, URL Filtering, Data Filtering, or WildFire Submissions).

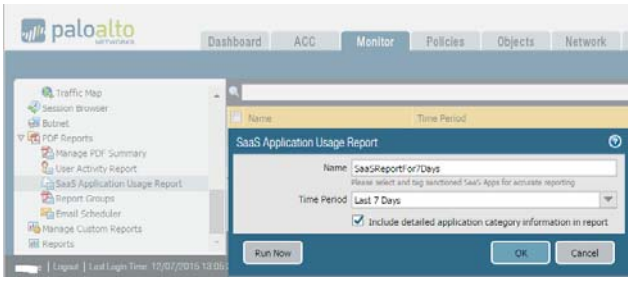
App-ID Features

- PDF Report for Visibility into SaaS Applications

PDF Report for Visibility into SaaS Applications

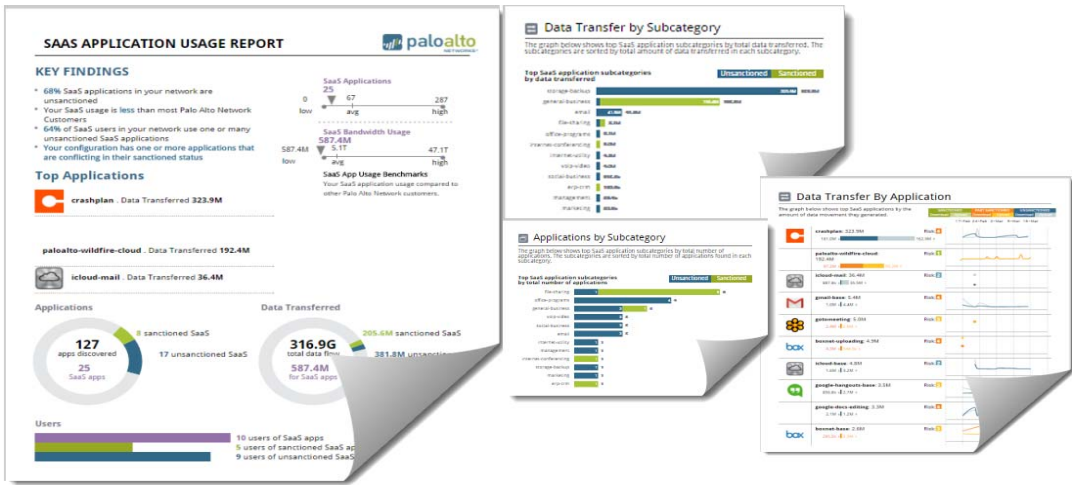
To maintain network security and ensure compliance with corporate policy, you must identify and monitor the use of SaaS applications on your network. To meet this challenge, the firewall includes a new SaaS Application Usage report in PDF format to give you visibility into the SaaS applications that users on your network are accessing. You can generate this report on demand or you can schedule it to run on a daily, weekly, or monthly cadence and then use the findings in this report to consolidate the list of business-critical and approved SaaS applications and to enforce policies for controlling unsanctioned applications that pose an unnecessary risk for malware propagation and data leaks.

Configure and Schedule the SaaS Application Usage Report	
Step 1 Tag applications that you approve for use on your network as Sanctioned. The accuracy of the report depends on whether you have tagged an application as Sanctioned. You can tag both SaaS and non-SaaS applications as Sanctioned; the detailed browsing section of the SaaS Application Usage report displays whether the application is SaaS and whether it is sanctioned.	1. Select **Object** > **Applications.** 2. Click the application **Name** to edit an application and select **Edit** in the Tag section. 3. Select **Sanctioned** from the **Tags** drop-down. You must use the predefined **Sanctioned** tag (with the azure colored background). If you use any other tag to indicate that you sanctioned an application, the firewall will fail to recognize the tag and the report will be inaccurate.  4. Click **OK** and **Close** to exit all open dialogs.

Configure and Schedule the SaaS Application Usage Report (Continued)	
Step 2 Configure the SaaS Application Usage report.	1. Select **Monitor** > **PDF Reports** > **SaaS Application Usage**. 2. **Add** a **Name** and select a **Time Period** for the report (default is **Last 7 Days**). By default, the report includes detailed information on the top SaaS and non-SaaS application subcategories, which can result in a report with a large page count and file size. Disable the **Include detailed application category information in report** option as needed to reduce the file size and restrict the page count to eight pages.  3. **Run Now** to generate the report on demand. Make sure pop-up blocker is disabled on your browser because the report opens in a new tab. Panorama running PAN-OS 7.1 can generate the SaaS Application Usage report for managed firewalls running PAN-OS 6.1 and later releases except for PA-7000 Series firewalls. Because logs are stored locally on PA-7000 Series firewalls and are not forwarded to Panorama, these firewalls must be running PAN-OS 7.1 to include information on SaaS application usage. 4. Click **OK** to save your changes.
Step 3 Schedule the report for email delivery.	On the PA-200, PA-500, and PA-2000 Series firewalls, the SaaS Application Usage report is not sent as a PDF attachment in the email. Instead, the email includes a link you use to open the report in a web browser.

Configure and Schedule the SaaS Application Usage Report (Continued)

Step 4 Use the informative PDF report to learn about SaaS application usage on your network.



Virtualization Features

The following are new virtualization features for the firewall and Panorama:

- Support for ELB on the VM-Series Firewalls in AWS
- Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall
- VM-Series for Microsoft Hyper-V
- Support for VMware Tools on Panorama and VM-Series on ESXi
- Support for Device Group Hierarchy in the VM-Series NSX edition firewall
- VM-Series Firewall in Microsoft Azure
- Support for Bootstrapping VM-Series Firewalls

Support for ELB on the VM-Series Firewalls in AWS

Elastic Load Balancing (ELB) is an Amazon web service that helps you improve the availability and scalability of your applications by routing traffic across multiple Elastic Compute Cloud (EC2) instances. ELB detects unhealthy EC2 instances and reroutes traffic to healthy instances until the unhealthy instances are restored. ELB can send traffic only to the primary interface of the next-hop, load-balanced EC2 instance. Therefore, to use ELB with a VM-Series firewall in AWS, the firewall must be able to use the primary interface (eth0) for dataplane traffic instead of management traffic.

- VM-Series Firewall and Amazon ELB
- Use the AWS Management Console to Swap the Management Interface
- Configure ELB Health Checks

VM-Series Firewall and Amazon ELB

Beginning with PAN-OS 7.1, you can configure the firewall to receive dataplane traffic on the primary interface in scenarios where the VM-Series firewall is behind the Amazon ELB. Before PAN-OS 7.1, the VM-Series firewall could not integrate with ELB because ELB could forward traffic only to the primary (eth0) elastic network interface (ENI) of an EC2 instance. You now have the ability to enable the primary interface on the VM-Series firewall to function as a dataplane interface, instead of functioning as the management interface, so that ELB can forward traffic to the firewall.

You cannot configure the firewall to send and receive dataplane traffic on eth0 when the firewall is in front of ELB. The VM-Series firewall must be placed behind the Amazon ELB to leverage this capability.

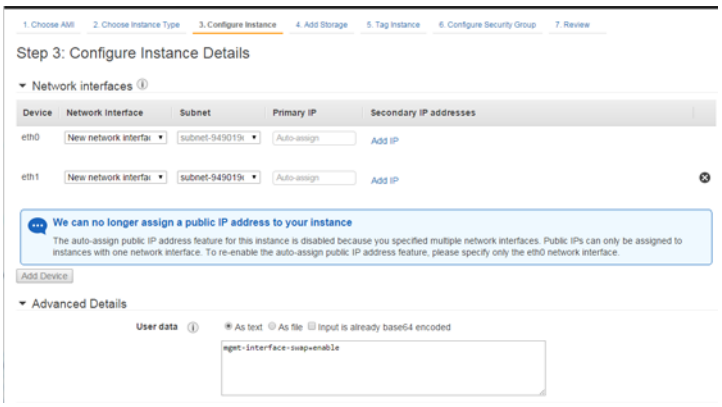
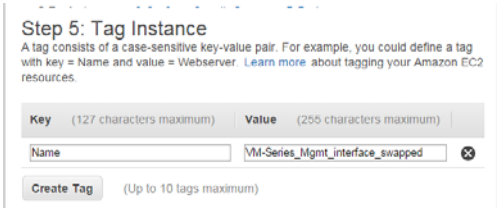
If you want to deploy a load balancer sandwich topology, you must use the CFT, see Auto Scale VM-Series Firewalls with the Amazon ELB.

To learn about specific scenarios and about how to use management interface mapping changes for use with Amazon ELB, see VM-Series Firewall in AWS.

Use the AWS Management Console to Swap the Management Interface

Use these instructions when you are launching the firewall to perform a swap so that Elastic Network Interface (ENI) eth0 maps to ethernet1/1 and ENI eth1 maps to the MGT interface on the firewall.

Management Interface Swap on the VM-Series Firewall Using the AWS Management Console	
Step 1	On the EC2 Dashboard, click **Launch Instance**.
Step 2	Select the VM-Series Amazon Machine Image (AMI). To get the AMI, see Obtain the AMI.
Step 3	Choose the **EC2 instance type** for allocating the resources required for the firewall and click **Next**. See EC2 instance types for a list of supported types.
Step 4	Select the Amazon Virtual Private Cloud (VPC) and the subnet to which the VM-Series management interface will attach.

Management Interface Swap on the VM-Series Firewall Using the AWS Management Console (Continued)	
Step 5	Select **Launch as an EBS-optimized instance** to leverage Amazon Elastic Block Store (EBS) benefits.
Step 6	Expand the Network Interfaces section and click **Add Device** to add another network interface. Swapping interfaces requires a minimum of two ENIs (eth0 and eth1). Make sure that your VPC has more than one subnet so that you can add additional ENIs at launch. If you launch the firewall with only one ENI, the interface swap command will cause the firewall to boot into maintenance mode.
Step 7	Expand the Advanced Details section and set **User data** to `mgmt-interface-swap=enable` **As text** to perform the interface swap during launch. 
Step 8	Accept the default **Storage** settings.
Step 9	Add one or more tags to create your own metadata to identify the VM-Series firewall. For example, add a **Name** tag with a **Value** that helps you remember that the ENI interfaces have been swapped on this VM-Series firewall. 
Step 10	Select an existing **Security Group** or create a new one. This security group is for restricting access to the management interface of the firewall. At a minimum, consider enabling HTTPS and SSH access for the management interface (eth1).
Step 11	If prompted, select an appropriate **SSD** option for your setup.
Step 12	Select **Review and Launch** to ensure your selections are accurate and then click **Launch**. Select an existing key pair or create a new one and acknowledge the key disclaimer.
Step 13	Download and save the private key to a safe location; the file extension is .pem. You cannot regenerate this key if lost.

Management Interface Swap on the VM-Series Firewall Using the AWS Management Console (Continued)	
Step 14	View the progress of the installation on the EC2 Dashboard. It can take five minutes or longer to launch the VM-Series firewall. When the process is complete, the VM-Series firewall will display on the **Instances** page of the EC2 Dashboard.
Step 15	Assign an EIP to eth1 and then use the EIP address to open an SSH session to the CLI of the VM-Series firewall and configure the administrative password.

Step 16	Verify that the interfaces have been swapped. Use the following command to verify:
	debug show vm-series interfaces all
	`Phoenix_interface Base-OS_port Base-OS_MAC PCI-ID Driver`
	`mgt(interface-swap) eth0 0e:53:96:91:ef:29 0000:00:04.0 ixgbevf`
	`Ethernet1/1 eth1 0e:4d:84:5f:7f:4d 0000:00:03.0 ixgbevf`

If you want to swap the management interface on a VM-Series firewall that you have already deployed, use the VM-Series Firewall CLI.

Configure ELB Health Checks

ELB periodically checks the health of the EC2 instance using pings or by sending requests to test the availability of the firewall. On the Amazon EC2 console, configure the health check to use port 80 or 443 of the web server behind the firewall. This allows you to compute the health using the total path of the HTTP request and includes routing on the firewall, NAT, and availability of the web server itself. For instructions on configuring health checks, refer to the AWS documentation.

Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall

Beginning with PAN-OS 7.1, the VM-Series NSX edition firewall includes support for multi-tenancy, which means that you can use the VM-Series firewall to secure traffic from multiple tenants (or sub-tenants) hosted in the vSphere environment. The VM-Series NSX edition firewall allows you to create up to 32 service definitions, each with a unique device group and template. The device group allows you to create and manage policy rules for a tenant (or sub-tenant) and the template allows you to define one or more zones so that you can isolate traffic for each tenant or sub-tenant. Each tenant (or sub-tenant) is mapped to a specific zone on Panorama, and the zone becomes available as a service profile on the NSX Manager; the NSX security administrator can select the appropriate service profile to logically isolate traffic and redirect it to the VM-Series firewall.

In previous releases, the VM-Series NSX edition firewalls were all assigned to one service definition with a single template (with one default zone and, hence, a single service profile for redirecting traffic) and a single device group (one set of security policies). With the support for multiple service definitions in PAN-OS 7.1, whether you have a shared compute infrastructure and need shared security policies, or you have a dedicated compute infrastructure and need dedicated security policies, or you have shared compute infrastructure and need dedicated security policies (multiple instances of the VM-Series firewall per host in an ESXi cluster), you can configure the firewall for your needs.

For details on multi-tenant deployment options, see What is Multi-Tenant Support on the VM-Series NSX Edition Firewall?

High-Level Workflow for Deploying the VM-Series NSX Edition Firewall for Multi-Tenancy
❑ Register the VM-Series firewall as a service on the NSX Manager. To enable communication between the NSX Manager and Panorama and to deploy the firewall as a service on the NSX Manager, you must provide the IP address or hostname along with the credentials of the NSX Manager on the VMware service manager configuration on Panorama. The registration also allows the NSX Manager to update Panorama with dynamic changes to the software-defined data center (SDDC).
❑ On the NSX Manager, use the NSX service composer to create security groups. The NSX security group allows you to define which objects—DVS port-group, logical switch (VXLAN), or virtual machines—are included or excluded from the group. When you create a security group in NSX, the information is transmitted to Panorama. On Panorama, the security administrator can then use NSX security groups as match criteria or tags within dynamic address groups and then use dynamic address groups in security policy rules and push the rules to the VM-Series firewalls.
❑ On Panorama, create the building blocks for redirecting traffic to the VM-Series firewall for policy enforcement. • Create the template(s) and device group(s). On each template, create one or more zones (NSX service profile zone) for each tenant or sub-tenant from which you want to redirect traffic to the firewall. The firewall automatically creates a pair of virtual wire subinterfaces for each zone. • Create dynamic address groups and use them in security policy rules. You can now use an NSX service profile zone name as the source and destination zone (must be the same zone) in a security policy rule. Using dynamic address groups in policy allows you to secure virtual machines as they are dynamically added or removed from your vSphere environment.
❑ Create the service definition(s) on Panorama. The service definition includes the template and device group to which a VM-Series firewall belongs. When the firewall connects to Panorama, it receives its configuration settings, including the zone(s) for each tenant or department that the firewall will secure and its policy settings from the device group specified in the service definition.

High-Level Workflow for Deploying the VM-Series NSX Edition Firewall for Multi-Tenancy (Continued)
❑ On the NSX Manager, create security policies to granularly define which traffic flows to redirect to the VM-Series firewall for inspection and enforcement. NSX security policies allow you to assign security services, such as the VM-Series firewall for network introspection of traffic, for the objects that belong to NSX security groups. After you deploy the firewalls, the traffic redirection rules allow you to steer traffic to the appropriate Service Profile. The NSX Manager receives these Service Profile(s) from Panorama and each profile maps to the NSX service profile zone you created in the Panorama template. Make sure to select the correct service and profile when defining NSX security policies. To create policies, see Create Policies. Traffic allowed by the VM-Series firewall is then returned to the NSX virtual switch for delivery to the final destination (guest virtual machine or physical device).
❑ Deploy the VM-Series firewalls. For instructions, see Deploy the VM-Series Firewalls. On the NSX Manager, make sure to select the appropriately defined service to ensure that you properly secure the ESXi cluster.

VM-Series for Microsoft Hyper-V

The VM-Series firewall can now be deployed on Hyper-V Server 2012 R2 (standalone edition) and on Windows Server 2012 R2 (standard and datacenter editions) with the Hyper-V role that lets you create and manage virtual machines. You can deploy the firewall using the Hyper-V Manager (guided user interface) or Windows PowerShell (command line interface).

The VM-Series firewall on Hyper-V supports the following:

- Tap, virtual wire, Layer 2, and Layer 3 interface deployments. See Supported Deployments on Hyper-V.
- All capacity model licenses—VM-100, VM-200, VM-300, and VM-1000-HV.
- Active/active and active/passive high availability (HA) configurations.

The VM-Series firewall on Hyper-V is bundled with the Linux Integration Services package to improve integration between the host and the virtual machine. This bundle allows you to:

- Use the Hyper-V Manager to view the IP address assigned to the management interface on the firewall.
- Synchronize time and heartbeat between the host and the firewall to ensure that firewall is operating properly.
- Gracefully shutdown the firewall from the Hyper-V Manager.

Support for VMware Tools on Panorama and VM-Series on ESXi

VMware Tools is now supported on the VM-Series firewall and Panorama virtual machine deployed on VMware ESXi. The tool is bundled with the software image and is automatically enabled when you launch the VM-Series firewall and the Panorama virtual machine. Because VMware Tools is bundled with the software image for the firewall and Panorama, any updates will be made available with a new OVF image; you cannot upgrade VMware Tools using the vCenter server.

VMware Tools gives you the following capabilities for managing the VM-Series firewall and Panorama from the VMware infrastructure:

- Displays the IP address of the management interface and the PAN-OS version running on the firewall or Panorama.
- Provides resource utilization metrics on the hard disk, memory, and CPU. You can use these metrics to enable alarms or actions on the vCenter server.
- Graceful shutdown and restart of the firewall and Panorama using the power off function in vCenter.
- Enables a heartbeat mechanism between the vCenter server and the firewall or Panorama to verify whether it is functioning or rebooting. If the firewall goes into maintenance mode, heartbeats are disabled so that the vCenter server does not shut down the firewall. Disabling heartbeats allows the firewall to stay operational in maintenance mode when it cannot send heartbeats to the vCenter server.

The current version of the implementation uses Open VMware Tools version 9.4.6.

Support for Device Group Hierarchy in the VM-Series NSX edition firewall

When deploying the VM-Series NSX edition firewall, you can now use a template stack and a device group hierarchy in the VMware Service Manager configuration on Panorama. Both template stacks and device group hierarchy (introduced in PAN-OS 7.0) allow you to organize devices based on some common criteria in order to minimize redundant configuration.

- A template stack allows you to push all the necessary settings to the set of firewalls assigned to a stack without the redundancy of adding every setting to every template.
- A device group hierarchy allows you to nest device groups in a tree hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) from higher-level groups.

To create context awareness between the virtual and security environments for Dynamic Address Groups referenced in policy, you can also select one or more device groups in a hierarchy for notification when virtual machines are provisioned or removed from the network. The firewalls use this update to determine the most current list of members that constitute Dynamic Address Groups referenced in policy.

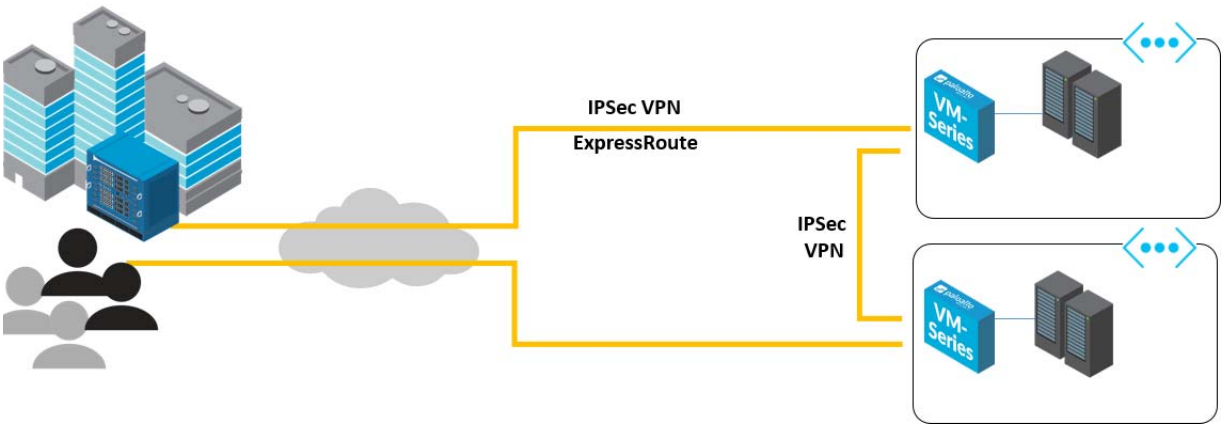
For configuration details, see Create Template(s) and Device Group(s) on Panorama. For additional new features on the VM-Series NSX edition firewall, see Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall.

VM-Series Firewall in Microsoft Azure

Microsoft Azure allows you to deploy a virtual network in the cloud so that you can deploy a private cloud solution or you can extend the on-premises IT infrastructure to create a hybrid or cross-premises solution. The VM-Series firewall in Azure must be deployed in a virtual network (VNet) using the Azure Resource Manager (ARM) deployment mode only; the classic mode (Service Management-based deployments) is not supported. The VM-Series firewall in Azure must be of the Standard tier and any of the following types—A4, D3, D3_v2, D4 and D4_v2—that meet the minimum system requirements. Because the Azure VNet is a Layer 3 network, the VM-Series firewall in Azure supports only Layer 3 interfaces. The VM-Series firewall in Azure supports the Bring Your Own License (BYOL) model and the usage-based licensing (PAYG) model.

The VM-Series firewall (PAN-OS 7.1.1) is available on Azure Government, and the Azure Government Marketplace offers the BYOL option only. To deploy the VM-Series firewall on Azure Government, you will follow the same steps for BYOL deployments that are outlined in the documentation.

You can deploy a VM-Series firewall in Azure to function as a VNet gateway that secures traffic destined to the servers in the VNet, as a VPN termination point to securely extend your physical data center to the Azure private cloud into Azure, or to set up an IPSec tunnel for traffic between two Azure VNets. You can also deploy the VM-Series firewall to function as a GlobalProtect gateway and portal to safely enable your mobile users with consistent security policy when they are not on the corporate network.



To deploy the VM-Series firewall, Palo Alto Networks provides an solution template in the Azure Marketplace and a customizable ARM template in the Palo Alto Networks GitHub repository. The ARM template includes two JSON files (a Template File and a Parameters File) to help you deploy the firewall. For more information, see the VM-Series Deployment Guide.

The VM-Series firewall in Azure does not support native VM Monitoring capabilities for virtual machines that are hosted in Azure. VM-Series high availability configuration is not supported either; use the integration with Azure Gateway and Load balancer to address availability requirements for web facing applications.

Support for Bootstrapping VM-Series Firewalls

See Bootstrapping Firewalls for Rapid Deployment.

WildFire Features

- WildFire EU Cloud
- Mac OS X File Analysis
- Five Minute WildFire Updates
- New WildFire API Features

The WF-500 appliance is not supported with PAN-OS 7.1.1. However, a WF-500 appliance that is running PAN-OS 7.1.0 (or 7.1.2 and later releases) is compatible with firewalls running any PAN-OS 7.1 release version (including PAN-OS 7.1.1).

WildFire EU Cloud

A new WildFire regional cloud is now available in Europe. The WildFire EU cloud is hosted in The Netherlands, and is designed to adhere to European Union (EU) data privacy regulations. Samples submitted to the WildFire EU cloud remain within EU borders, and the WildFire EU cloud analyzes malware and generates signatures independently of the WildFire global cloud.

Any firewall with an active WildFire subscription can start forwarding samples to the WildFire EU cloud, and you can access the WildFire EU portal using your support account credentials. You can learn more about the file types supported for WildFire analysis depending on the cloud to which you are forwarding files—currently, all file types supported for WildFire global cloud analysis are also supported for WildFire EU cloud analysis.

If you have not done so already, get started with WildFire to define the samples that you want a firewall to forward for analysis—you can then begin to Submit Samples to the WildFire EU Cloud.

Submit Samples to the WildFire EU Cloud

You can submit samples to the WildFire EU cloud from the firewall, from a WF-500 appliance, using the WildFire EU portal, and using the WildFire API.

Submit Samples to the WildFire Regional Cloud in Europe	
• **Firewall:**	Enable a firewall with an active WildFire subscription to forward samples to the WildFire EU cloud: 1. Log in to the firewall and select **Device > Setup > WildFire** and edit General Settings. 2. Enter the URL for the **WildFire Public Cloud** hosted in Europe: `eu.wildfire.paloaltonetworks.com`. 3. Click **OK** to save the updated WildFire analysis location. Use the `show wildfire status` command in the CLI to verify that the firewall is connected to the WildFire EU cloud. Find verdicts and analysis reports for samples: Select **Monitor > WildFire Submissions** or log in to the WildFire EU cloud portal to view the WildFire verdict and analysis details for samples submitted to the WildFire EU cloud. WildFire Submissions logs might not be displayed for samples submitted up to seven minutes before and two minutes after you update the WildFire public cloud field on the firewall. • To view verdicts and analysis reports for samples submitted before the update, go to the WildFire global cloud portal. • To view verdicts and analysis reports for samples submitted after the update, go to the WildFire EU cloud portal.

Submit Samples to the WildFire Regional Cloud in Europe (Continued)	

• **WF-500 Appliance:**	Enable a WF-500 appliance to submit locally-discovered malware or sample reports to the WildFire EU cloud for additional analysis and signature distribution:
	1. To connect the WF-500 appliance to the WildFire EU cloud, enter the following command from the WF-500 appliance CLI:
	`set deviceconfig setting cloud-server eu.wildfire.paloaltonetworks.com`
	2. If you have not done so already, enter the following command from the WF-500 appliance CLI to start submitting malware to the WildFire EU cloud:
	`set deviceconfig setting wildfire cloud-intelligence submit-sample yes`

• **WildFire EU Portal:**	You can manually submit samples to the WildFire EU cloud using the WildFire EU portal: https://eu.wildfire.paloaltonetworks.com. After uploading files or URLs to the WildFire EU portal, you can also view the WildFire analysis verdict and report for the sample.

• **WildFire API:**	Use the following resources to submit samples through the WildFire API to the WildFire EU cloud:
	• Submit a file:
	`https://eu.wildfire.paloaltonetworks.com/publicapi/submit/file`
	• Submit a file through a URL:
	`https://eu.wildfire.paloaltonetworks.com/publicapi/submit/url`
	• Submit a URL:
	`https://eu.wildfire.paloaltonetworks.com/publicapi/submit/link`
	• Submit multiple URLs:
	`https://eu.wildfire.paloaltonetworks.com/publicapi/submit/links`
	  To get information on submissions to the WildFire EU Cloud, you must also use the same base URI that corresponds to the WildFire EU cloud. Example:
	`https://eu.wildfire.paloaltonetworks.com/publicapi/get/verdict`

Mac OS X File Analysis

The WildFire public cloud can now analyze and classify Mac OS X file types as malicious, grayware, or benign. For malicious Mac OS X files, the WildFire public cloud distributes a signature to Palo Alto Networks firewalls to allow the firewalls to detect and block future instances of the file.

The following Mac OS X file types are supported for WildFire public cloud analysis:

- **Mach-O**—With Mac OS X, Mach-O file format is used for native executable, library, and object files. Possible file extensions include .o, .dylib, and .bundle.
- **DMG**—.dmg is the file extension for Universal Disk Image Format (UDIF) files and is the native disk image format for Mac OS X.
- **PKG**—Mac OS X installer files used for Apple software packages.
- **Application Bundles**—With Mac OS X, application bundles are used to deliver software and can hold executable code and related resources.

While you can manually or programmatically submit all Mac OS X supported file types to the WildFire public cloud for analysis; the firewall supports automatic forwarding only for Mach-O, DMG, and PKG files.

▲ Manually or Programmatically Submit Mac OS X Files

▲ Enable the Firewall to Forward Mac OS X Files

The WF-500 appliance does not support Mac OS X file analysis.

Manually or Programmatically Submit Mac OS X Files

Submit Mac OS X file types directly to the WildFire public cloud for analysis. With a WildFire subscription, you can manually and programmatically submit a daily total of 1000 files.

Submit MAC OS X Files Directly to the WildFire Public Cloud
❑ Manually submit Mac OS X files to the WildFire public cloud for analysis. You can then view the WildFire sample analysis report and verdict (malicious, grayware or benign) on the WildFire portal.
❑ Use the WildFire API to submit Mac OS X files to the WildFire public cloud. You can continue to use the WildFire API to retrieve verdicts and analysis reports for Mac OS X files. You can also specify Mac OS X as the target analysis environment when you retrieve a packet capture through the WildFire API.

Enable the Firewall to Forward Mac OS X Files

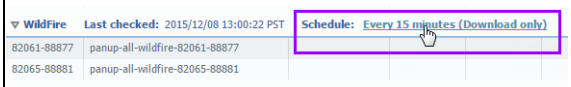
To forward Mach-O, DMG, and PKG files for WildFire public cloud analysis, the firewall must be running PAN-OS 7.1 with content version 599 installed. Firewalls already configured to forward **Any** unknown files to the WildFire public cloud automatically begin forwarding Mac OS X file types when content version 599 is installed.

Enable the Firewall to Automatically Forward Mac OS X Files to the WildFire Public Cloud		
Step 1	Download and install content version 599.	
Step 2	Upgrade the firewall to PAN-OS 7.1.	
Step 3	Enable Mac OS X file type forwarding.	1. Select **Objects** > **Security Profiles** > **WildFire Analysis** and **Add** or modify a profile to define traffic to forward for WildFire analysis. a. Add or modify a profile rule, select **file type**, and set the rule to forward the new **MacOSX** file type. Profile rules with the file type set to **Any** forward all file types for WildFire analysis, including **MacOSX** files. b. Select Destination and set the profile rule to forward Mac OS X files to the **public-cloud**. c. 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. a. Select **Policies** > **Security** and **Add** or modify a security policy rule. b. Select **Actions** and set the **Profile Type** to **Profiles**. c. Select the newly-created **WildFire Analysis** profile. d. 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.
Step 4	Select **Monitor** > **WildFire Submissions** to find WildFire verdicts and analysis reports for Mac OS X files the firewall submits.	

Five Minute WildFire Updates

The WildFire public cloud now makes virus and DNS signatures available every five minutes to Palo Alto Networks firewalls. This more frequent distribution enables firewalls with a WildFire subscription to detect and block threats within minutes of discovery. With earlier PAN-OS releases, WildFire updates are made available only every fifteen minutes.

Take the following steps to enable the firewall to retrieve the very latest signatures from WildFire.

Modify the WildFire Updates Schedule		
Step 1	Confirm that the WildFire subscription is active on the firewall.	• If you have not already done so, activate the WildFire subscription on the firewall. • To verify an active WildFire subscription, select **Device** > **Licenses** and check that the WildFire license is valid.
Step 2	Check that the firewall is connected to the WildFire public cloud.	Select **Device** > **Setup** > **WildFire** and confirm that **WildFire Public Cloud** is set to `wildfire.paloaltonetworks.com`.
Step 3	Set the schedule for the firewall to check for the latest WildFire updates.	1. Select **Device** > **Dynamic Updates**. 2. Find the **WildFire** updates. 3. Select the existing **Schedule** setting:  4. Use the **Recurrence** field to configure the firewall to check for new WildFire updates **Every Minute**. Because new WildFire signatures are now available every five minutes, it is a best practice to use this setting to ensure the firewall retrieves these signatures within a minute of availability. 5. To get the most of out of WildFire five-minute updates, set the firewall to **Download and Install** these updates as WildFire makes them available. You can also set the firewall to **Download Only** so that you can manually install the updates whenever appropriate after they are downloaded. 6. Click **OK**.

New WildFire API Features

You can now use the WildFire API with the public cloud and WF-500 appliance to submit links for WildFire analysis and to retrieve WildFire verdicts for all supported file types and email links. The WildFire API provides new resources to access these features. You can use the `submit/link` and `submit/links` resources to programmatically submit links to the WildFire and identify potentially malicious websites. With the `/get/verdict` and `/get/verdicts` resources, you can use the WildFire API to automate the retrieval of WildFire verdicts for submitted samples.

Read more about the new `submit/link`, `submit/links`, `/get/verdict`, and `/get/verdicts` resources in the WildFire API Reference.

The WF-500 appliance is supported with PAN-OS 7.1.0, and is not supported with PAN-OS 7.1.1.
To use this feature with the WF-500 appliance, you should upgrade the appliance to PAN-OS 7.1.0 and not PAN-OS 7.1.1.

Content Inspection Features

- Support for Custom Domains in an External Dynamic List
- Support for URLs in an External Dynamic List
- Enhanced Security for URL Category and Application-Based Policy

Support for Custom Domains in an External Dynamic List

Prior to PAN-OS 7.1, you could only use the DNS-based signatures available on the firewall to configure DNS sinkholing. Now, if you subscribe to third-party threat intelligence and want to protect your network from new sources of threat or malware listed in the feed, you can create an *external dynamic list* for domain names to give you the agility to protect your network.

An external dynamic list (formerly called a Dynamic Block List) is a text file that you host on an external web server. In addition to IP addresses and URLs, you can now use this list to import domain names into the firewall so that you can enforce policy—block, alert, sinkhole, or allow—on the domains you include in the list. This enhancement allows you to configure the firewall to create DNS-based spyware signatures for a custom or third-party list of domains so that you can use intelligence from other sources to enable DNS sinkholing of malicious DNS traffic. The firewall dynamically imports the list at the configured interval and enforces policy for the domains included in that list without requiring a configuration change or commit on the firewall. The DNS-based spyware signature that the firewall generates for a custom domain name is of type spyware with medium severity and is named `Custom Malicious DNS Query <domain name>`.

On each firewall platform, you can configure a maximum of 30 unique sources for External dynamic lists; these limits are not applicable to Panorama. When using Panorama to manage a firewall that is enabled for multiple virtual systems, a commit error displays on Panorama if you exceed the limit for the firewall. Each firewall platform supports a maximum of 50,000 domain names combined in one or more external dynamic lists but no maximum limit is enforced for any one list. A source is a URL that includes the IP address or hostname, the path, and the filename for the external dynamic list. The firewall matches the URL (complete string) to determine whether a source is unique.

Use an External Block List in an Anti-Spyware Profile for Sinkholing Custom Domains	
Step 1	Create an external dynamic list and host it on a web server that the firewall can access. Use the formatting guidelines for the list.  The 50,000 domain name limit is for generating signatures for entries in external dynamic lists. Palo Alto Networks DNS signatures do not count towards this limit.
Step 2	Configure the firewall to access the external dynamic list.
Step 3	Use the external dynamic list in an Anti-Spyware profile and enforce policy.

Support for URLs in an External Dynamic List

Instead of statically defining a URL allow list, block list, or custom URL category on a firewall, the external dynamic list (formerly called a Dynamic Block List) is enhanced in PAN-OS 7.1 to include support for URLs, which enhances your agility to protect your network from new sources of threat and malware.

An external dynamic list is a text file that you host on an external web server. In addition to IP addresses and domains, you can now use this list to import URLs into the firewall so that you can enforce policy—block, alert, continue, override, or allow—for the objects you include in the list. The firewall dynamically imports the list at the configured interval and enforces policy for the included URLs without requiring a configuration change or commit on the firewall.

The firewall handles an external dynamic list that includes URLs like a custom URL category and you can use this list in two ways:

- As a match criteria in Security policy rules, Decryption policy rules, and QoS policy rules to allow, deny, decrypt, not decrypt, or allocate bandwidth for the URLs in the custom category.
- In a URL Filtering profile where you can define more granular actions, such as continue, alert, or override, before you attach the profile to a Security policy rule.

On each firewall platform, you can configure a maximum of 30 unique sources for external dynamic lists. Each firewall platform supports a maximum of 50,000 URLs combined in one or more external dynamic lists but no maximum limit is enforced for any one list. A source is a URL that includes the IP address or hostname, the path, and the filename for the external dynamic list. The firewall matches the URL (complete string) to determine whether a source is unique.

Enforce Policy on URLs in an External Dynamic List	
Step 1	Create the external dynamic list and host it on a web server that the firewall can access. Use the formatting guidelines for the list.
Step 2	Configure the firewall to access the external dynamic list.
Step 3	Select one of the following options: • Use an external dynamic list of Type URL as Match Criteria in a Security Policy Rule. • Use an external dynamic list in a URL Filtering profile to enforce policy.

Enhanced Security for URL Category and Application-Based Policy

With PAN-OS 7.1.1, you can enable evasion prevention for policy rules that block or allow traffic based on URL category and/or application. Setting up this evasion prevention feature enables the firewall to check that the hostname or SNI indicated in an initial HTTP or TLS request corresponds to the destination IP address for the connecting client.

This feature is supported only with PAN-OS 7.1.1 and later release versions.

Prevent HTTP Hostname and TLS SNI Evasions		
Step 1	Install the Applications and Threats content version 579 or a later version.  Applications and Threats content updates require an active Threat Prevention license.	1. Select **Device** > **Dynamic Updates**. 2. **Check Now** to get the latest Applications and Threats content update. 3. **Download** and **Install** Applications and Threats content version 579 or a later version.
Step 2	Upgrade the Firewall to PAN-OS 7.1.1.	
Step 3	Enforce traffic matching the evasion signature IDs 14984 and 14978.  The default action for both of these signatures is allow; to enable this feature to work seamlessly, ensure that both signatures are set to any action other than allow or default.	1. Select **Objects** > **Security Profiles** > **Anti-Spyware** and **Add** or modify an Anti-spyware profile. 2. Select **Exceptions** and select **Show all signatures.** 3. Filter signatures based on the keyword `evasion`. 4. For the signatures 14978 and 14984, set the **Action** to any setting other than allow and default (for example, set the Action to alert or block on). 5. Click **OK** to save the updated Anti-spyware profile. 6. Attach the Anti-spyware profile to a security policy rule: a. Select **Policies** > **Security**, select the desired policy to modify and then click the **Actions** tab. b. In **Profile Settings**, click the drop-down next to **Anti-Spyware** and select the anti-spyware profile enabled to enforce the evasion signatures 14978 and 14984.
Step 4	Enable the firewall to act as a DNS proxy.  When DNS proxy is enabled, evasion signatures that detect crafted HTTP or TLS requests can alert to instances where a client connects to a domain other than the domain specified in the original DNS request. If you do not enable DNS proxy along with the evasion signatures (Step 3), the signatures will trigger when a DNS server in a load balancing configuration returns different IP addresses (for servers hosting identical resources) to the firewall and the client in response to the same DNS request.	
Step 5	**Commit** your changes.	

GlobalProtect Features

- GlobalProtect App for Chrome OS
- GlobalProtect App for Windows Phone
- Simplified GlobalProtect Agent User Interface for Windows and Mac OS
- Dynamic GlobalProtect App Customization
- Enhanced Two-Factor Authentication
- Client Authentication Configuration by Operating System or Browser
- Kerberos for Internal Gateway for Windows
- Customizable Password Expiry Notification Message
- Enhanced Authentication Challenge Support for Android and iOS Devices
- Block Access from Lost or Stolen and Unknown Devices
- Certificate Selection by OID
- Save Username Only Option
- Use Address Objects in a GlobalProtect Gateway Client Configuration
- Maximum Internal Gateway Connection Retry Attempts
- GlobalProtect Notification Suppression on Windows
- Disable GlobalProtect Without Comment
- Pre-logon then On-Demand Connect Method
- Enforce GlobalProtect for Network Access
- Connection Behavior on Smart Card Removal

GlobalProtect App for Chrome OS

The new GlobalProtect app for Chrome OS extends the same next-generation firewall-based policies that are enforced within the physical perimeter to Chromebooks. To set up the app for the user automatically, you can optionally use the Google Chromebook Management Console to configure and deploy settings to managed Chrome OS devices.

- Prerequisites for the GlobalProtect App for Chrome OS
- Configure the GlobalProtect App for Chrome OS
- Deploy the GlobalProtect App for Chrome OS

Prerequisites for the GlobalProtect App for Chrome OS

To add support for the GlobalProtect app for Chrome OS, consider the following:

- The GlobalProtect app 3.0 is available for Chromebooks running Chrome OS 45 and later.
- GlobalProtect portals and gateways support the GlobalProtect app for Chrome OS in PAN-OS 6.1 and later releases.
- (Client certificate authentication only) To authenticate using client certificates, upgrade the GlobalProtect gateway to PAN-OS 6.1.8, PAN-OS 7.0.3, PAN-OS 7.1.0, or any subsequent release.
- Because Chrome OS does not allow third-party applications to launch automatically, the GlobalProtect app for Chrome OS must use the on-demand connect method to initiate a VPN connection. For ease of configuration, the GlobalProtect portal automatically uses the on-demand connect method in the client configuration so that you do not need to manually change the connect method.
- The GlobalProtect app for Chrome OS collects HIP data specific to Chrome. Therefore, if you are using HIP-based policy enforcement, consider creating or modifying your existing HIP objects and HIP profiles or creating new ones.

Configure the GlobalProtect App for Chrome OS

- Configure the Gateway to Support the GlobalProtect App for Chrome OS
- Configure the Portal and Customize the GlobalProtect App to Support Chrome OS
- Enforce Policies on the GlobalProtect App for Chrome OS

Configure the Gateway to Support the GlobalProtect App for Chrome OS

The GlobalProtect app for Chrome OS can establish VPN connections with both internal and external gateways. Configuring a gateway that supports the GlobalProtect app for Chrome OS is similar to configuring a gateway that supports mobile devices—you must also install a gateway subscription for each gateway that supports Chromebooks. You can also customize an external gateway configuration to apply it specifically to Chromebooks (see Client Authentication Configuration by Operating System or Browser).

Configure the Portal and Customize the GlobalProtect App to Support Chrome OS

To support the GlobalProtect app for Chrome OS, you must configure one or more gateways to which the app can connect and then configure the portal and app settings. The portal sends configuration information to the app, including information about available gateways and customization settings that define how end users interact with the app.

After receiving the configuration from the GlobalProtect portal, the app auto-discovers the gateways listed in the client configuration and selects the best gateway. Because Chrome OS does not allow third-party applications to launch automatically, the GlobalProtect app for Chrome OS only supports on-demand connections. As a result, the end user has to launch the app and manually initiate a VPN connection to establish a VPN (tunnel) connection.

The following workflow shows how to configure the GlobalProtect portal to support Chrome OS clients.

Configure the Portal and Customize the App		
Step 1	Before You Begin:	Configure one or more gateways to which the app can connect. See Configure the Gateway to Support the GlobalProtect App for Chrome OS.
Step 2	Configure the GlobalProtect portal.	1. Select **Network** > **GlobalProtect** > **Portals** and select the portal configuration for which you want to add a client configuration or **Add** a new one. 2. (New portal configuration only) On the **General** tab, provide a **Name** and **Interface** for the new GlobalProtect portal configuration.
Step 3	Configure the method of authentication a GlobalProtect portal uses to authenticate Chrome OS users.	1. Select the **Authentication** tab. 2. (New portal configuration only) Select an **SSL/TLS Service Profile**. 3. **Add** a new Client Authentication configuration and configure the settings. To create a configuration specific to Chromebooks, specify Chrome as the OS as described in Client Authentication Configuration by Operating System or Browser.
Step 4	Add the trusted root CA certificate the app will use to perform certificate checks when connecting to the GlobalProtect gateway. The portal deploys the specified root CA certificate with the client configuration.  If the certificate is self-signed, the GlobalProtect app for Chrome OS will not use the certificate deployed by the portal. Therefore, to use a self-signed certificate, you must install the root CA in the client's local certificate store. If GlobalProtect does not require the certificate, you must install it in the root CA of the client's local certificate store.	1. Select the **Agent** tab and **Add** the trusted root CA in the Trusted Root CA section. 2. Install the root CA in the local certificate store of the Chromebook: a. From the Chromebook, click the status area and then select **Settings** > **Show advanced settings** > **Manage certificates** > **Authorities** > **Import**. b. Browse to the certificate and then click **Open**. c. When prompted to edit trust settings, select all options and then click **OK**. d. Verify that the Chromebook lists the certificate on **Your Certificates** tab.

Configure the Portal and Customize the App (Continued)	
Step 5 Add a new agent configuration for the app and configure the internal or external gateways to which users with this configuration can connect. The GlobalProtect app for Chrome OS does not support manual gateway configurations.	1. Select **Network** > **GlobalProtect** > **Portals** and reselect the portal configuration you are configuring. 2. From the **Agent** tab, select the agent configuration you want to modify or **Add** a new one. 3. Select **Authentication** and provide a **Name** for the configuration. 4. Select **Gateways** and **Add** one or more internal or external gateway. 5. (External gateways only) Set the **Priority** of the gateway. GlobalProtect excludes any external gateways that have **Manual only** priority.

Configure the Portal and Customize the App (Continued)		
Step 6	Customize how your end users interact with the GlobalProtect app installed on their Chromebooks. The GlobalProtect app for Chrome OS supports only the configuration options listed here.	1. On the **App** tab, configure the **Connect Method** as **On-demand (Manual user initiated connection)**. This setting requires users to manually initiate a VPN connection using the GlobalProtect app. The GlobalProtect app for Chrome OS supports only this connect method and automatically uses this method for all connections even if you do not specify it as the **Connect Method**. 2. Customize the behavior of the app for users that receive this configuration, including any of the following supported options: • **Enable Advanced View**—Select **No** to restrict the user interface on the Chromebook to the basic minimum view. By default, the user can view advanced settings. • **Allow User to Change Portal Address**—Select **No** to disable the **Portal** field on the GlobalProtect app. • **Allow User to Continue with Invalid Portal Server Certificate**—Select **No** to prevent the app from establishing a connection with the portal if the portal certificate is not valid. By default, the app can establish a connection with the portal when the portal certificate is not valid. • **Portal Connection Timeout**—Specify the amount of time, in seconds, after which the app cancels the portal connection (range is 1-600; default is 30). • **TCP Connection Timeout**—Specify the amount of time, in seconds, after which the app cancels a TCP connection request (range is 1-600; default is 5). • **TCP Receive Timeout**—Specify the permitted amount of time, in seconds, in which the app can receive a partial response to a request or read some data. If the response exceeds the timeout, the app cancels the request (range is 1-600; default is 30). • **SCEP Cert Renewal Period**—Specify the number of days after which the app renews the Simple Certificate Enrollment Protocol (SCEP) certificate. A value of 0 means the certificate should not be renewed automatically during a configuration refresh. • **Maximum Internal Gateway Connection Attempts**—Specify the maximum number of times the app tries to establish a connection to an internal gateway. The default is 0, which means the app does not reattempt a connection after an initial failure.
Step 7	Save your configuration changes.	1. Click **OK** twice. 2. **Commit** your changes.
Step 8	Deploy the GlobalProtect app to end users.  The portal does not distribute the GlobalProtect app for Chrome OS.	An end user can download the GlobalProtect app directly from the Chrome Web Store. You can also force-install the app on managed Chromebooks using the Chromebook Management Console. See Configure the GlobalProtect App Using the Chromebook Management Console.

Enforce Policies on the GlobalProtect App for Chrome OS

With the release of the GlobalProtect app for Chrome OS, you can now create HIP objects using **Host Info** that is specific to Chrome OS and use it as match conditions in any HIP profiles. You can then use a HIP profile as a match condition in a policy rule to enforce the corresponding security policy.

The following table defines the criteria that is specific to Chrome OS that you can use when you create a HIP object.

HIP Object Criteria	Value
General > **Host Info** > **OS**	Select **Contains: Google: Chrome** to create a HIP object that looks for information about devices running Chrome OS.
General > **Host Info** > **Client Version**	Select an operator (for example, **Contains**) and then enter the version number of the GlobalProtect app for Chrome OS. For example, enter `3.0` to match endpoints running the GlobalProtect app 3.0. Specifying the client version without specifying the OS or hostname matches all endpoints regardless of OS version.
General > **Host Info** > **Host Name**	Select an operator (for example, **Contains**) and enter `CHROME` to match devices that contain chrome in the host name. GlobalProtect automatically prepends the host name with this prefix when the app submits the host information to the gateway.

Deploy the GlobalProtect App for Chrome OS

Deploy the GlobalProtect app using either of the following methods:

- **Chrome Web Store**—You or your users can install the GlobalProtect app on a Chromebook by downloading the app from the Chrome Web Store.
- **Chromebook Management Console**—Enables management Chromebook settings and apps from a central, web-based location. From the console, you can deploy the GlobalProtect app to Chromebooks and customize VPN settings.

For instructions, see Download and Install the GlobalProtect App for Chrome OS.

GlobalProtect App for Windows Phone

GlobalProtect 3.1.3 now extends its Windows 10 support to include Windows 10 phones. The new GlobalProtect app takes advantage of the Universal Windows Platform (UWP) technology which provides a common platform for apps to run across all Windows devices. The new GlobalProtect app for Windows 10 UWP extends enterprise security protection by enabling enforcement of the same next-generation firewall-based policies that are enforced within the physical perimeter.

The app is ideal for Windows 10 mobile devices but can also be used on laptops or desktops running Windows 10. For a fuller feature set, we recommend using the standard GlobalProtect app.

- GlobalProtect App for Windows 10 UWP Feature Support
- Prerequisites for GlobalProtect App for Windows 10 UWP
- Configure the GlobalProtect App for Windows 10 UWP
- Obtain the GlobalProtect App for Windows 10 UWP
- Use the GlobalProtect App for Windows 10 UWP

GlobalProtect App for Windows 10 UWP Feature Support

The following table lists the features that are supported by the GlobalProtect app for Windows 10 UWP versus the features that are supported by the standard GlobalProtect app for Windows in version 3.1.3. For additional feature support, see What Features Does GlobalProtect Support?. A ✓ indicates the feature is supported; A – indicates the feature is not supported.

Choose the GlobalProtect app that is right for your feature requirements and devices.

Feature	Windows UWP	Windows
Devices		
Windows 10 phones	✓	–
Windows 10 tablets	✓	✓
Windows 10 laptops and desktops	✓	✓
Split Tunneling		
App-level VPN	✓	–
Device-level VPN	✓	✓
Connect Methods		
User-logon (always on)	✓ (Always On configured from third-party endpoint management system)	✓
Pre-logon (always-on)	–	✓
Pre-logon (then on-demand)	–	✓

Feature	Windows UWP	Windows
On-demand	✓	✓
Modes		
Internal mode	–	✓
External mode	✓	✓
Single Sign-On (SSO)		
SSO (Credential Provider)	–	✓
Kerberos SSO	–	✓
Customization		
Enforce GlobalProtect for network access	✓ (VPN Lockdown configured from third-party endpoint management system)	✓
Native Windows 10 user interface	✓	–
Deployment of SSL forward proxy CA certificates in the trust store	–	✓
HIP reports	✓ (Host information only; Notifications not supported)	✓
Script actions that run before and after sessions	–	✓
Certificate selection by OID	–	✓
Allow users to disable GlobalProtect	–	✓
Welcome and help pages	–	✓
Endpoint management system (EDM/MDM) support	✓	–

Prerequisites for GlobalProtect App for Windows 10 UWP

- The GlobalProtect app 3.1.3 is available for devices running Windows 10 UWP or later releases.
- GlobalProtect portals and gateways support the GlobalProtect app for Windows 10 UWP in PAN-OS 6.1 and later releases with content update 612-3527 and later releases.
- The GlobalProtect app for Windows 10 UWP requires a gateway subscription for each gateway that supports Windows 10 UWP devices.

Configure the GlobalProtect App for Windows 10 UWP

- Configure Gateways to Support the GlobalProtect App for Windows 10 UWP
- Configure the Portal to Support the GlobalProtect App for Windows 10 UWP

▲ Enforce Policies on the GlobalProtect App for Windows 10 UWP

Configure Gateways to Support the GlobalProtect App for Windows 10 UWP

Configuring a gateway that supports the GlobalProtect app for Windows 10 UWP is similar to configuring a gateway that supports mobile devices: Each gateway that supports Windows 10 UWP endpoints requires a gateway subscription. In addition, you can optionally configure specific authentication or client settings that only apply to Windows 10 UWP endpoints.

Configure Gateways to Support the GlobalProtect App for Windows 10 UWP		
Step 1	Complete the prerequisite tasks for setting up a GlobalProtect gateway.	Configure GlobalProtect Gateways
Step 2	Install a gateway subscription for each gateway that supports Windows 10 UWP devices.	Activate Licenses
Step 3	(Optional) Tailor a gateway configuration to Windows 10 UWP endpoints. When you configure a gateway you can specify client authentication settings that apply specifically to Windows 10 UWP. For example, you could configure Windows and Mac endpoints to use two-factor authentication and Windows 10 UWP endpoints to use certificate-based authentication. You can also configure client settings—such as specific IP pools, access routes, cookie authentication, or split tunneling—for Windows 10 UWP endpoints.	1. Select **Network > GlobalProtect > Gateways**, and then select or **Add** a gateway configuration. 2. Add a Client Authentication configuration for Windows 10 UWP endpoints: a. Select **Authentication** and **Add** a new Client Authentication configuration. b. Enter a **Name** to identify the Client Authentication configuration, set **OS** to **WindowsUWP**, specify the Authentication Profile to use for authenticating users on this gateway and optionally enter an authentication message to provide users with instructions or additional information. Kerberos and single sign-on are not supported with the GlobalProtect app for Windows 10 UWP. c. Click **OK**. 3. To configure specific client settings that apply to only Windows 10 UWP endpoints, configure a new Client Settings configuration: a. Select **Agent** and **Add** a new Client Settings configuration. b. Configure the Client Authentication settings as desired. c. Select **User/User Group**, **Add** an **OS**, and select **WindowsUWP**. d. Click **OK**. 4. Click **OK**.
Step 4	Save your changes.	**Commit** the configuration.

Configure the Portal to Support the GlobalProtect App for Windows 10 UWP

To support the GlobalProtect app for Windows 10 UWP, you must configure one or more external (auto-discovery) gateways to which the app can connect and then configure the portal and app settings. The portal sends configuration information and information about the available gateways to the app.

After receiving the configuration from the GlobalProtect portal, the app auto-discovers the gateways listed in the client configuration and selects the best gateway.

The following workflow shows how to configure the GlobalProtect portal to support the GlobalProtect app for Windows 10 UWP.

Configure the Portal to Support the GlobalProtect App for Windows 10 UWP		
Step 1	If you have not already done so, complete the prerequisite tasks for setting up a GlobalProtect portal.	Configure the GlobalProtect Portal
Step 2	(Optional) Define client settings for Windows 10 UWP users to authenticate to the portal.	1. Select **Network > GlobalProtect > Portals**, and then select a portal configuration. 2. Configure Client Authentication settings that apply to Windows 10 UWP endpoints when users access the portal: a. Select **Authentication** and then **Add** a new Client Authentication configuration. b. Enter a **Name** to identify the Client Authentication configuration, set **OS** to **WindowsUWP**, specify the Authentication Profile to use for authenticating users on this portal and optionally enter an authentication message to provide users with instructions or additional information. Kerberos and single sign-on are not supported with the GlobalProtect app for Windows 10 UWP.
Step 3	Customize an agent configuration for Windows 10 UWP endpoints. Whether you modify an existing configuration or create a new one depends on your environment. For example, if you use OS-specific gateways or want to collect host information that is specific to Windows 10 UWP endpoints, consider creating a new agent configuration. If you use an existing configuration that contains settings that are not supported, the GlobalProtect app for Windows 10 UWP automatically discards these settings (see GlobalProtect App for Windows 10 UWP Feature Support). For example if you select the **Always On** Connect Method, the app defaults to the **On Demand** Connect Method.	Define a GlobalProtect Agent Configuration: 1. Select **Agent** and select an existing or **Add** a new portal agent configuration. 2. Configure the **Authentication** settings for Windows 10 UWP endpoints including whether to use client certificates, save user credentials, use authentication cookies, or require dynamic passwords. Windows 10 UWP endpoints support two-factor authentication using dynamic passwords on the portal and external gateways (auto-discovery) only. The options to save and clear credentials on Windows 10 UWP endpoints are not supported; however, if you enable the option to save credentials in the agent configuration, Windows automatically saves the users credentials. If you do not enable GlobalProtect to save credentials, users must enter them every time they connect. 3. Select **User/User Group**, **Add** an **OS**, and select **WindowsUWP**. 4. Specify the external gateways to which users with this configuration can connect. Windows 10 UWP endpoints support **External gateways-auto discovery** only. 5. (Optional) Select **App** and customize the portal and TCP timeout settings for the GlobalProtect app for Windows 10 UWP. Configuration of any additional settings that do not apply are discarded. 6. Click **OK** twice.

Configure the Portal to Support the GlobalProtect App for Windows 10 UWP (Continued)	
Step 4 Save your changes.	**Commit** the configuration.

Enforce Policies on the GlobalProtect App for Windows 10 UWP

With the release of the GlobalProtect app for Windows 10 UWP, you can now create HIP objects using Host Info that is specific to Windows 10 UWP endpoints and use it as match conditions in any HIP profiles. You can then use a HIP profile as a match condition in a policy rule to enforce the corresponding security policy.

The following table defines the criteria that is specific to Windows 10 UWP that you can use when you create a HIP object.

HIP Object Criteria	Value
General > Host Info > OS	Select **Contains: Microsoft: Windows UWP Desktop** or **Windows UWP Mobile** to create a HIP object that looks for information about desktop or mobile devices running Windows UWP.
General > Host Info > Client Version	Select an operator (for example, **Contains**) and then enter the version number of the GlobalProtect app for Windows 10 UWP. For example, enter 3.1.3 to match endpoints running the GlobalProtect app 3.1.3. Specifying the client version without specifying the OS or hostname matches all endpoints regardless of OS version.

Obtain the GlobalProtect App for Windows 10 UWP

Obtain the GlobalProtect app for Windows 10 UWP using either of the following methods:

- **Microsoft Store** —You or your users can install the GlobalProtect app on a Windows 10 UWP endpoint by downloading the app from the Microsoft Store.
- **Third-party endpoint management system**—Use a mobile device management system, such as AirWatch, to manage and deploy the GlobalProtect App for Windows 10 UWP from a centralized, web-based location. See Deploy the GlobalProtect App Windows 10 UWP Using AirWatch.

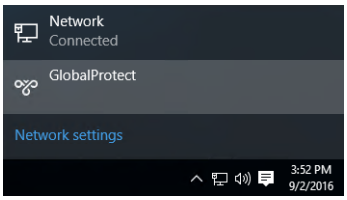
Set Up the GlobalProtect App for Windows 10 UWP

After you install the GlobalProtect app for Windows 10 UWP, configure the connection settings.

Set Up the GlobalProtect App for Windows 10 UWP		
Step 1	Launch the GlobalProtect app.  	From the Windows 10 UWP device, select **Start > All apps > GlobalProtect**.
Step 2	Configure the VPN settings for the GlobalProtect app. After you configure the settings you can return to the **NETWORK & INTERNET > VPN Settings** page at any time to modify the following settings: •Connection name •Portal address	1. Select the **NETWORK & INTERNET VPN Settings** link to jump to Windows 10 settings. 2. Click **Yes** to confirm the switch from the GlobalProtect app to the **Settings** page. 3. Click **Add a VPN connection**. 4. Select **GlobalProtect** as the **VPN provider**. 5. Enter a **Connection name** to identify the GlobalProtect VPN connection. 6. Enter the server name (FQDN) or IP address of the GlobalProtect portal in the **Server name or address** field. 7. Click **Save** to create the connection. Windows 10 adds the connection to the list of VPNs.
Step 3	Test the connection. If the connection is successful, the network settings display the connection name with a status of Connected.	1. Select the GlobalProtect connection (**NETWORK & INTERNET > VPN**) and click **Connect**. 2. Enter your username and password and click **Connect**.

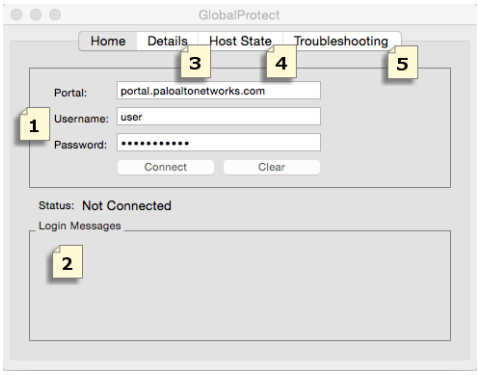
Use the GlobalProtect App for Windows 10 UWP

The GlobalProtect app for Windows 10 UWP provides on-demand connectivity to your network and enables enforcement of security policies on Windows 10 UWP endpoints. To connect to GlobalProtect you must manually initiate a connection.

Use the GlobalProtect App for Windows 10 UWP	
Step 1 If you are not connected to GlobalProtect, connect now. When the VPN is connected, the Network settings displays the status of the connection as **Connected**.	1. Click the Network icon ( ) in the notification area of the Windows 10 UWP endpoint and then select the connection name for your GlobalProtect app.  The **NETWORK & INTERNET > VPNs** settings page opens. 2. Select the connection name and select **Connect**. 3. When prompted, enter your **Username** and **Password** for the portal and click **Next**.
Step 2 (Optional) Use the app to perform any of the following tasks:	
• Disconnect from GlobalProtect.	1. Click the Network icon ( ) in the notification area of the Windows 10 UWP endpoint and then select the connection name for your GlobalProtect app. The **NETWORK & INTERNET > VPNs** settings page opens. 2. Select the connection name and select **Disconnect**.
• Log in with a new password. If your password for accessing your corporate network changes, you will need to disconnect from GlobalProtect to clear your credentials. When you next log in, GlobalProtect prompts you for your new credentials.	1. Disconnect from GlobalProtect as described in the previous step. 2. Click the Network icon ( ) in the notification area of the Windows 10 UWP endpoint. 3. Select the connection name and select **Connect**. 4. When prompted, enter your **Username** and new **Password** and click **Next**.
• Collect any available logs and send them in an email.	Select **Start > All apps > GlobalProtect**, and then **Email Logs**. The app prompts you to select your email application and then attaches the logs to an email which you can send to Support.

Simplified GlobalProtect Agent User Interface for Windows and Mac OS

The GlobalProtect agent 3.0 for Windows and Mac OS now displays a simpler, cleaner user interface. As part of the redesign, a user can now log in to the GlobalProtect portal and view connection status information from the main **Home** tab. The following figure displays the GlobalProtect agent for Mac but the menus and layout of the GlobalProtect agent for Windows are very similar:

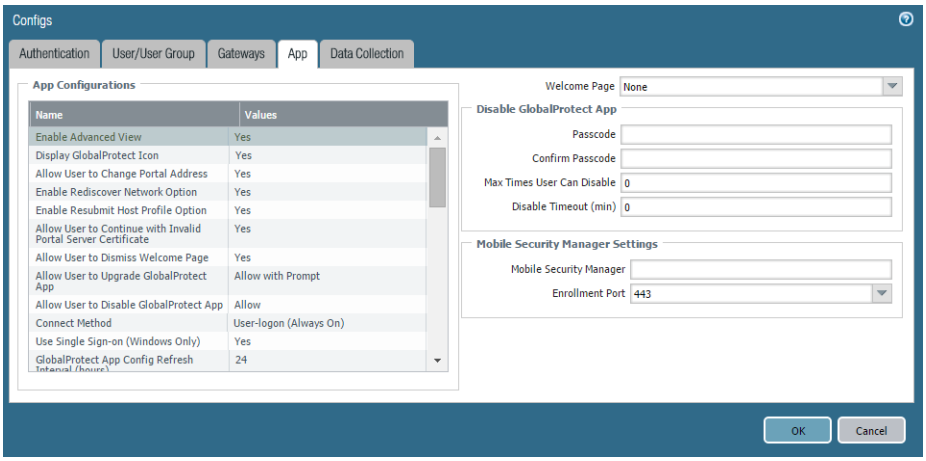


With this update, the menu bar along the top has been removed and has been replaced with the **Home**, **Details**, **Host State**, and **Troubleshooting** tabs. The tab contents are described in more detail in the following table.

Item	Description
1	(New) Users can log in to the GlobalProtect portal from the **Home** tab. At any time, users can also change the portal (unless disabled from the portal agent configuration) and re-enter login credentials from this tab.
2	(New) Users can also view connection status information from the **Home** tab, including any pertinent warning or error messages.
3	The **Details** tab displays information about your connection, including the portal to which users connect, IP address information, and protocol information. This tab also displays connection statistics, such as the number of bytes sent and received, and information about the gateway with which the agent established the VPN connection.
4	The GlobalProtect agent collects information about the security status of your end hosts, such as whether the host has the latest security patches and antivirus definitions installed, whether disk encryption is enabled, and whether the host is running specific software required within your organization (including custom applications). The GlobalProtect agent then displays this information on the **Host State** tab. To drill down into the data, users can collapse or expand categories and select the type of information to view collected data.
5	The **Troubleshooting** tab enables users to view information that can help troubleshoot connection issues. Users can select between **Network Configurations**, **Routing Table**, and **Sockets** to view information for that type. Additionally, selecting the **Logs** option enables users to begin or stop logging of either the GlobalProtect agent or service.

Dynamic GlobalProtect App Customization

You can now view all agent customization options and configure them from the new **App** tab in a GlobalProtect portal agent configuration. You can create separate agent configurations to customize the GlobalProtect app for different groups of users or types of endpoints.



Additionally, future options will be available with content releases that allow you to take advantage of new app configuration features without waiting for the next PAN-OS release.

Included in the new customization options are settings that, in earlier releases, required you to define their values in the Windows registry or Mac global property list (plist). Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows registry or Mac plist.

The following topics describe the available customization options:

- GlobalProtect App Display Options
- GlobalProtect App User Behavior Options
- GlobalProtect App Behavior Options

GlobalProtect App Display Options

By configuring GlobalProtect app display options in a GlobalProtect portal agent configuration, you can customize which options are available for different sets of users.

Some options allow you to hide notifications or menu options from view while other options only let you gray out the feature in menus but this still prevents users from selecting the option.

Option	Details
Enable Advanced View	Select **No** to restrict the user interface on the client side to the basic minimum view. By default, the advanced view setting is enabled.

Option	Details
Display GlobalProtect Icon	Select **No** to hide the GlobalProtect icon on the client system. When the icon is hidden, users cannot perform other tasks (such as change passwords, rediscover the network, resubmit host information, view troubleshooting information, or trigger an on-demand connection request). However, HIP notification messages, login prompts, and certificate dialogs still display as necessary for interacting with the end user.
Enable Rediscover Network Option	Select **No** to prevent users from performing a manual network rediscovery.
Enable Resubmit Host Profile Option	Select **No** to prevent users from manually triggering resubmission of the latest HIP.
(New) Show System Tray Notifications	Select **No** to hide notifications from users. Select **Yes** (default) to enable the GlobalProtect agent to display notifications about status changes in the notification area (system tray).

GlobalProtect App User Behavior Options

User behavior options enable you to define the way your users can interact with the GlobalProtect app.

Option	Details

Allow User to Change Portal Address	Select **No** to disable the **Portal** field on the **Home** tab of the GlobalProtect agent. Because the user is then unable to specify a portal to which to connect, you must pre-deploy the default portal address by configuring a new key in the Windows registry or Mac plist and supplying the portal address as the value:
	• **Windows registry**—Create a new key named `Portal` in the following registry location:
	`HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup`
	• **Mac plist**—Create a new entry named `Portal` in the following plist location:
	`Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist`

Allow User to Dismiss Welcome Page	Select **No** to force the GlobalProtect agent to display the Welcome Page each time users initiate a connection to prevent them from dismissing important information, such as terms and conditions required by your organization to maintain compliance.
Allow User to Continue with Invalid Portal Server Certificate	Select **No** to prevent the GlobalProtect agent from establishing a connection with the portal if the portal certificate is not valid.
Allow User to Upgrade GlobalProtect App	Select **Disallow**, **Allow Manually**, **Allow with Prompt**, or **Allow Transparently** to specify whether GlobalProtect agent software downloads and upgrades are allowed and, if so, how they occur.
Allow User to Disable GlobalProtect App	Select an override option—**Allow**, **Disallow**, **Allow with Comment**, **Allow with Passcode**, or **Allow with Ticket**—to specify the condition under which users can disable the GlobalProtect agent.

GlobalProtect App Behavior Options

GlobalProtect app behavior options determine how the GlobalProtect agent establishes a connection with GlobalProtect portals and gateways.

Option	Details
Connect Method	Select a connect method—**On-demand (Manual user initiated connection)**, **User-logon (Always On)**, or **Pre-logon (Always On)**—to specify how users connect to the GlobalProtect gateway.
GlobalProtect App Config Refresh Interval (hours)	Specify the interval, in hours, to determine the frequency at which the GlobalProtect agent refreshes the configuration (range is 1-168; default is 24).
(New) Update DNS Settings at Connect (Windows Only)	Select **Yes** to flush the DNS cache and force all adapters to use the DNS settings specified in the configuration. Select **No** (default) to enable the GlobalProtect agent to use the DNS settings of the client.
(New) Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)	Select **No** to prevent the GlobalProtect agent from sending HIP data in response to a change in the Windows Security Center (WSC) status. Select **Yes** (default) to configure GlobalProtect to immediately send HIP data when the WSC status changes.
(New) Detect Proxy for Each Connection (Windows Only)	Select **No** to enable the GlobalProtect agent to automatically detect the proxy for the portal connection and use that proxy for subsequent connections. Select **Yes** (default) to enable the GlobalProtect agent to automatically detect the proxy each time the agent connects.
(New) Clear Single Sign-On Credentials on Logout (Windows Only)	Select **No** to enable the GlobalProtect agent to keep single sign-on (SSO) credentials after users log out. Select **Yes** (default) to clear credentials and force users to enter them when they next log in.
(New) Use Default Authentication on Kerberos Authentication Failure (Windows Only)	Select **No** to force GlobalProtect to authenticate using Kerberos. Select **Yes** (default) to allow the GlobalProtect agent to retry authentication using the default authentication method after a failure to authenticate with Kerberos.
(New) Custom Password Expiration Message (LDAP Authentication Only)	An optional custom message notification that the GlobalProtect agent appends to the standard password expiry message sent to alert users that their password is due to expire. The message text supports up to 200 characters.
(New) Portal Connection Timeout (sec)	The period of time, in seconds, that is required for the portal connection request to time out due to inactivity (range is 1-600; default is 30).
(New) TCP Connection Timeout (sec)	The period of time, in seconds, that is required for the TCP connection request to time out due to inactivity (range is 1-600; default is 5).
(New) TCP Receive Timeout (sec)	The period of time, in seconds, that is required to receive a partial response to a TCP request (range is 1-600; default is 30).
(New) Client Certificate Store Lookup	The store which the agent should use to look up client certificates to use to authenticate and establish the VPN connection with the GlobalProtect gateway. **User** certificates are stored in the Current User certificate store on Windows and in the Personal Keychain on Mac OS. **Machine** certificates are stored in the Local Computer certificate store on Windows and in the System Keychain on Mac OS. By default, the agent looks for **User and machine** certificates in both places.

Option	Details
(New) SCEP Certificate Renewal Period (days)	The frequency, in days, after which the portal should renew the Simple Certificate Enrollment Protocol (SCEP) certificate (default is 7). A value of 0 means the portal does not renew the certificate automatically during a configuration refresh.
(New) Maximum Internal Gateway Connection Attempts	Enter the number of times that GlobalProtect reattempts to connect to the internal gateway after initially failing. A value of 0 indicates that the GlobalProtect agent will not attempt to reconnect if the initial attempt fails.
(New) Extended Key Usage OID for Client Certificate	Enter a certificate object identifier (OID) to specify the type of certificate that GlobalProtect should use for authentication on Windows and Mac clients. When specified, GlobalProtect presents only certificates with that OID and ignores all other certificates.
User Switch Tunnel Rename Timeout (sec)	Specify a grace period, in seconds, to enable the GlobalProtect gateway to reassign a VPN tunnel to a remote user within a specified amount of time. If the remote user fails to authenticate within the configured grace period, the GlobalProtect gateway terminates the original VPN connection. The default value of 0 seconds means the remote user is not permitted to authenticate with the gateway (range is 0-600).

Enhanced Two-Factor Authentication

Two-factor authentication enables strong authentication by using a pre-deployed client certificate or a dynamic password, such as one-time password (OTP), and supports the following two-factor authentication methods:

- Client certificate profile and OTP provided by an authentication service such as RADIUS.
- Client certificate profile and authentication profile such as LDAP.
- OTP and secure-encrypted cookies.

The following enhancements make two-factor authentication even easier to use and deploy.

▲ Dynamic Certificate Distribution Using SCEP

▲ Secure Encrypted Cookies for Simplified Authentication

Dynamic Certificate Distribution Using SCEP

The GlobalProtect portal can now request unique client or server certificates from your enterprise PKI and directly deploy them to GlobalProtect components without exposing your PKI infrastructure to the Internet. GlobalProtect automates the process of requesting and installing client certificates by using the Simple Certificate Enrollment Protocol (SCEP).

Configure Certificate Distribution Using SCEP	
Step 1	Set up a SCEP profile.
Step 2	Assign the SCEP profile to a GlobalProtect portal agent configuration. The GlobalProtect portal can then transparently deliver the certificates to endpoints that receive the configuration, thus simplifying the deployment of certificates. You can also use SCEP to automate the generation of server certificates for GlobalProtect gateways.

Secure Encrypted Cookies for Simplified Authentication

To improve the user experience with two-factor authentication, you can now configure GlobalProtect portals and gateways to generate and accept secure, encrypted cookies to authenticate the user.

This feature supersedes the **Authentication Modifier** option, which was available in PAN-OS 7.0. After you upgrade the firewall or Panorama to PAN-OS 7.1, any Authentication Modifier settings are discarded. Because the new **Authentication Override** options are disabled by default, to configure GlobalProtect portals and gateways to accept secure encrypted cookies, you must manually configure the new **Authentication Override** options in PAN-OS 7.1.

To enable this feature, you configure an authentication override to instruct the portal or gateway to override the default authentication profile requirements while the cookie is active. The user must then log in successfully to receive the new secure encrypted cookie. For each subsequent log in to portals and gateways during the lifetime of that cookie, the GlobalProtect agent presents the cookie instead of prompting for

credentials, which reduces the number of times that users are required to enter their credentials. If the portal or gateway are also configured for client authentication as a second authentication factor, then the GlobalProtect client must also provide a valid certificate to be granted access.

If you need to immediately block access to a device that has a cookie which has not yet expired (for example, if the device is lost or stolen), you can Block Access from Lost or Stolen and Unknown Devices by adding the device to a block list.

Configure the Portal and Gateway to Generate and Accept Cookies	
Step 1	Before you begin: Configure the certificate with the private key to encrypt the cookie. The cookie must be encrypted before sending it to the agent.
Step 2	Select **Network** > **GlobalProtect** > **Gateways** (or **Portals**) and select the configuration.
Step 3	Select **Agent** > **Client Settings** (on the gateway) or **Agent** (on the portal) and then select the configuration.
Step 4	Configure the following Authentication Override settings: • **Generate cookie for authentication override**—Enable the portal or gateway to generate encrypted, endpoint-specific cookies. The portal or gateway sends this cookie to the agent after the user first authenticates with the portal. • **Cookie Lifetime**—Specify the hours, days, or weeks that the cookie is valid. Typical lifetime is 24 hours. The range for hours is 1–72; for weeks, 1–52; and for days, 1–365. After the cookie expires, the user must enter login credentials and the portal or gateway subsequently encrypts a new cookie to send to the user endpoint. • **Accept cookie for authentication override**—Enable this option to instruct the portal or gateway to authenticate the agent through a valid, encrypted cookie. When the endpoint presents a valid cookie, the portal or gateway verifies that the cookie was encrypted by the portal or gateway, decrypts the cookie, and then authenticates the user. • **Certificate to Encrypt/Decrypt Cookie**—Select the certificate to use for encrypting and decrypting the cookie.  The portal and gateways must use the same certificate to encrypt and decrypt cookies.
Step 5	Click **OK** twice to save the configuration.

Client Authentication Configuration by Operating System or Browser

For increased flexibility, you can now specify the client operating system (Android, iOS, Mac, Windows, or Chrome) or the satellite device to which to apply a gateway client authentication configuration. You can also customize the client authentication for users who access the portal from a web browser (to download the GlobalProtect agent) or for third-party IPSec VPN (X-Auth) access to GlobalProtect gateways. This enhancement enables you to customize the authentication method for users according to the type of device they use. For example, you can configure Windows and Mac OS devices to authenticate using one-time passwords and configure Android and iOS devices to authenticate with a combination of LDAP and client certificates.

To configure client authentication for the GlobalProtect portal and gateways, use the following workflow:

Configure Client Authentication by OS	
• Configure the client authentication with the gateway.	1. Select **Network** > **GlobalProtect** > **Gateways** and then select an existing gateway configuration or **Add** a new one. 2. Select the **Authentication** tab. 3. Select an existing **Client Authentication** configuration or **Add** a new one. 4. Configure the settings for client authentication: • Enter a **Name** to identify the client authentication configuration. • Select the type of client to which to deploy this configuration. By default, the configuration applies to all clients. However, you can customize the type of client by **OS** (**Android**, **iOS**, **Mac**, **Windows**, or **Chrome**), by **Satellite** devices, or by third-party IPSec VPN clients (**X-Auth**). • Select or add an **Authentication Profile** for authenticating a client device or satellite that tries to access the gateway. • Enter an **Authentication Message** to help end users understand which credentials to use when logging in. The message can be up to 100 characters in length (default is `Enter login credentials`). 5. Click **OK** and **Commit**.

Configure Client Authentication by OS (Continued)	
• Configure the client authentication with the portal.	1. Select **Network** > **GlobalProtect** > **Portals** and then select an existing portal configuration or **Add** a new one. 2. Select the **Authentication** tab. 3. Select an existing **Client Authentication** configuration or **Add** a new one. 4. Configure the settings for client authentication: • Enter a **Name** to identify the client authentication configuration. • Enter the type of client to which to deploy this configuration. By default, the configuration applies to all clients. However, you can customize the type of client by a specific **OS** (**Android**, **iOS**, **Mac**, **Windows**, or **Chrome**), by **Satellite** devices, or by web-based **Browser** access. The **Browser** option is useful if you want to customize an authentication profile for users that need to access the portal to download the GlobalProtect software. • Select or add an **Authentication Profile** for authenticating a client device or satellite that tries to access the gateway. • Enter an **Authentication Message** to help end users understand which credentials to use when logging in. The message can be up to 100 characters in length (default is `Enter login credentials`). 5. Click **OK** and **Commit**.

Kerberos for Internal Gateway for Windows

GlobalProtect clients running on Windows 7, 8, or 10 now support Kerberos V5 single sign-on (SSO) for GlobalProtect portal and gateway authentication. A network that supports Kerberos SSO prompts users to log in only for initial access to the GlobalProtect portal or gateway. After initial login, users can access any browser-based service in the network (for example, webmail) without having to log in again until the SSO session expires. (The Kerberos administrator sets the duration of SSO sessions.)

In this implementation, the GlobalProtect portal and gateway act as Kerberos service principals and the GlobalProtect agent acts as a user principal to authenticate the user with a Kerberos service ticket from the Key Distribution Center (KDC).

Kerberos SSO is primarily intended for internal gateway deployments to provide accurate User-ID information transparently without user interaction. Using Kerberos SSO to authenticate remote users that connect to external gateways is supported but is not widely used because such a deployment requires you to host your authentication infrastructure in a DMZ.

If you enable both Kerberos SSO and external authentication services (for example, a RADIUS server), GlobalProtect tries SSO first. You can configure GlobalProtect to fall back to an external service for authentication when SSO fails or you can configure GlobalProtect to use only Kerberos SSO for authentication.

To support Kerberos SSO, your network requires the following:

- A Kerberos infrastructure, including a KDC with an authentication server (AS) and ticket-granting service (TGS). Additionally, to use Kerberos SSO for external gateway authentication, you must deploy the Kerberos infrastructure in a DMZ.
- A Kerberos service account for each GlobalProtect portal and gateway that authenticates users. An account is required to create a Kerberos keytab, which is a file that contains the principal name and hashed password of the device. The SSO process requires the keytab.

Use the following procedure to configure Kerberos SSO for GlobalProtect.

Configure Kerberos Single Sign-On for GlobalProtect	
Step 1 Create a Kerberos keytab.	1. Log in to the KDC and open a command prompt. 2. Enter the following command, where <principal_name>, <password>, and <algorithm> are variables. The Kerberos principal name and password are those configured for the GlobalProtect portal or gateway, not for the user. **ktpass /princ** <principal_name> **/pass** <password> **/crypto** <algorithm> **/ptype KRB5_NT_PRINCIPAL /out** <file_name>**.keytab** If the GlobalProtect portal or gateway is in FIPS or CC mode, the algorithm must be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96. If the portal or gateway is not in FIPS or CC mode, you can also use des3-cbc-sha1 or arcfour-hmac. To use an Advanced Encryption Standard (AES) algorithm, the functional level of the KDC must be Windows Server 2008 or later and you must enable AES encryption for the device account. The algorithm in the keytab must match the algorithm in the service ticket that the TGS issues to clients. (The Kerberos administrator determines which algorithms the service tickets use.)
Step 2 Import the keytab into an authentication profile. When using this authentication profile for GlobalProtect gateway or portal authentication or when including this profile in an authentication sequence, the portal and gateway challenge the GlobalProtect agent for a Kerberos service ticket.	Configure an authentication profile. 1. Configure authentication profile settings (**Name**, **Location**, **Type**, **User Domain**, and **Username Modifier**). In the event that Kerberos authentication fails, you can also configure GlobalProtect to authenticate using the credentials according to the **Type** specified here. For more information about enabling Kerberos authentication fall back, see Step 5. 2. In the Single Sign-On settings, enter the **Kerberos Realm** (usually the DNS domain to which users belong, except that the realm is uppercase). 3. **Import** the **Kerberos Keytab** you created.
Step 3 Assign the authentication profile to internal gateways. If your Kerberos authentication infrastructure is deployed in a DMZ, you can also assign the authentication profile to external gateways.	Configure GlobalProtect Gateways. 1. Select **Network** > **GlobalProtect** > **Gateways** and then select an existing gateway configuration or **Add** a new one. 2. Select **Authentication** and then select an existing client authentication configuration or **Add** a new one. 3. Configure the **Name**, **OS**, Kerberos **Authentication Profile** that you configured in Step 2, and **Authentication Message** to display when the user logs in.

Configure Kerberos Single Sign-On for GlobalProtect (Continued)		
Step 4	Assign the authentication profile to the GlobalProtect portal authentication configuration.	Configure the GlobalProtect Portal. 4. Select **Network** > **GlobalProtect** > **Portals** and then select an existing portal configuration or **Add** a new one. 5. Select **Authentication** and then select an existing client authentication configuration or **Add** a new one. 6. Configure the **Name**, **OS**, Kerberos **Authentication Profile** that you configured in Step 2, and **Authentication Message** to display when the user logs in.
Step 5	Configure the behavior when Kerberos SSO fails.	Customize the GlobalProtect Agent. 1. Select the **Agent** tab of a GlobalProtect portal configuration and select an existing agent configuration or **Add** a new one, select the **App** tab and, in App Configurations settings, specify whether to (New) **Use Default Authentication on Kerberos Authentication Failure (Windows Only)**: • **Yes**—Enables authentication fall back so that GlobalProtect can authenticate users with their username and password as determined by the authentication **Type** specified in the authentication profile (Local Database, RADIUS, LDAP, or TACACS+) if Kerberos authentication fails. • **No**—Forces GlobalProtect to use only Kerberos to authenticate users. 2. Click **OK** and then click **OK** again.
Step 6	Save your changes.	**Commit** your changes.

Customizable Password Expiry Notification Message

When using LDAP as the authentication method, you can now configure an optional custom password expiry notification message in the GlobalProtect portal agent configuration. The message can include additional instructions, such as help desk contact information or a link to a password portal where users can change their passwords. GlobalProtect appends the custom message to the standard notification, which the agent displays when a user's passwords is due to expire.

Consider configuring GlobalProtect agents to use pre-logon connect method. This allows users to connect and change their own expired passwords without administrative intervention. Otherwise, users cannot access the VPN if their passwords expire. See Remote Access VPN with Pre-Logon for details.

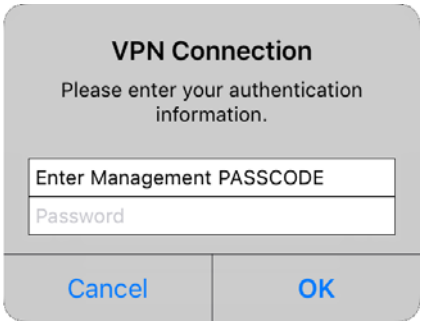
If users allow their passwords to expire, you may assign a temporary LDAP password to enable them to log in to the VPN. In this case, the user can use the temporary password to authenticate to the portal but the gateway login may fail because the same temporary password cannot be reused. To prevent this failure, enable **Authentication Override** in the portal configuration (**Network** > **GlobalProtect** > **Portal**) to enable the agent to use a cookie to authenticate to the portal and then use the temporary password to authenticate the gateway.

Configure a Custom Notification Message	
Step 1	In an authentication profile, configure the number of days before a password expires that the GlobalProtect agent should start displaying pending expiration notification messages. Notification messages display seven days before password expiry by default (range is 1-255). Because users must change their passwords before the end of the expiration period, make sure you provide a notification period that is adequate for your user base to ensure continued access to the VPN.
Step 2	In a GlobalProtect portal agent configuration, configure the **Custom Password Expiration Message (LDAP Authentication Only)** that users should see before their password expires. The message must be 200 or fewer characters.

Enhanced Authentication Challenge Support for Android and iOS Devices

GlobalProtect for iOS and Android devices now supports two-factor authentication using an SMS token challenge as a one-time password (OTP). To take advantage of this feature, configure two-factor authentication using OTPs on your mobile devices.

When prompted, the user can now cancel the login attempt to view the token password sent via SMS. The user must then return to the GlobalProtect app and log in with the valid token password within 30 seconds. If the user does not successfully enter the password within 30 seconds, the authentication challenge disappears and the user must restart the GlobalProtect app to enter a newly generated password.



Block Access from Lost or Stolen and Unknown Devices

For greater protection against unauthorized network access, you can now block device access to the network by adding the devices to a block list. Additionally, a new option enables you to block a session if the certificate for that session was not issued to the authenticating device, which is especially useful when a device is lost or stolen.

- Block Device Access from an Unknown Device
- Block Access from a Lost or Stolen Device

Block Device Access from an Unknown Device

Session blocking options enable you to validate the client certificate that GlobalProtect uses to authenticate users. The client certificate can be a pre-deployed client certificate or it can be a certificate that the GlobalProtect portal deploys to an end client. When any of the session blocking options are enabled, the GlobalProtect agent sends its client certificate and host ID (which contains the client serial number) for authentication when submitting a login request. Depending on the configuration of the certificate profile, GlobalProtect can block access when the Open Certificate Status Protocol (OCSP) or the certificate revocation list (CRL) service returns a certificate revocation status of unknown or when GlobalProtect registers an OCSP or CRL request timeout.

Additionally, a new option in a certificate profile—**Block session if the certificate was not issued to the authenticating device**—now enables GlobalProtect to block access when the device that presents the certificate does not match the device to which the certificate was issued. Authentication cannot succeed when this option is enabled unless GlobalProtect can validate that the presented client certificate was issued to the device that presented the certificate during a login request.

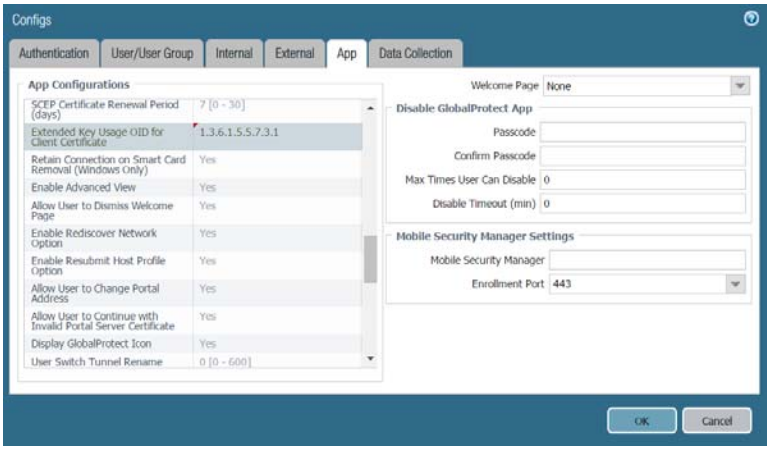
Block Access from a Lost or Stolen Device

You can now block a device from gaining access to the network by placing the device in a block list. Reasons for blocking a device can be loss or theft of the device. You need to be able to block a missing device because the extended period of automatic, transparent logins that OTPs support create a possible risk.

A block list is local to a logical network location (vsys1 for example) and has a maximum of 1,000 devices per location. Therefore, an organization with many locations that are each hosting GlobalProtect deployments can support many device block lists.

Certificate Selection by OID

In cases where multiple client certificates exist on the endpoint, you can now improve usability by filtering the client certificates by a secondary purpose. To do this, you can specify the certificate's object identifier (OID) in the **Extended Key Usage OID** field as part of a GlobalProtect portal agent configuration.

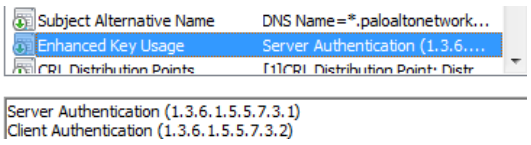


The OID is one of several methods GlobalProtect uses to identify a valid certificate on Windows and Mac endpoints. To be considered a valid client certificate, the certificate must:

- Be issued by the certificate authority (CA) you defined in the Certificate Profile that you specified in your portal and gateway configurations
- Specify a client authentication purpose
- Be located in the certificate store as specified in the GlobalProtect portal agent configuration. By default, the GlobalProtect agent looks in both the user and machine stores. With the default setting, client certificates stored in the user store take precedence over client certificates stored in the machine store. As a result, GlobalProtect automatically attempts to use the client certificate in the user store and does not continue looking in the machine store. To specify only one configure the **Client Certificate Store Lookup** option of a GlobalProtect portal agent configuration.
- (New) Match any additional purpose specified in the GlobalProtect portal agent configuration. To specify an additional purpose you must identify the certificate's object identifier (OID) and configure the value in the **Extended Key Usage OID** field of a GlobalProtect portal agent configuration.

  An OID is a numeric value that identifies the application or service for which a certificate is used and is automatically attached to a certificate when it is created by a certificate authority (CA). Some of the most commonly used OIDs are:

  - 1.3.6.1.5.5.7.3.1—Server Authentication
  - 1.3.6.1.5.5.7.3.2—Client Authentication (default match criteria)
  - 1.3.6.1.5.5.7.3.3—Code Signing
  - 1.3.6.1.5.5.7.3.4—Email Protection
  - 1.3.6.1.5.5.7.3.5—IPSec End System
  - 1.3.6.1.5.5.7.3.6—IPSec Tunnel
  - 1.3.6.1.5.5.7.3.7—IPSec User
  - 1.3.6.1.5.5.7.3.8—Time Stamping
  - 1.3.6.1.5.5.7.3.9—OCSP Signing



For example, say you have four client certificates but the one you want your users to select also specifies a Server Authentication purpose. Rather than allow the GlobalProtect agent to present all four client certificates to the user, you can enter the OID associated with the secondary purpose.

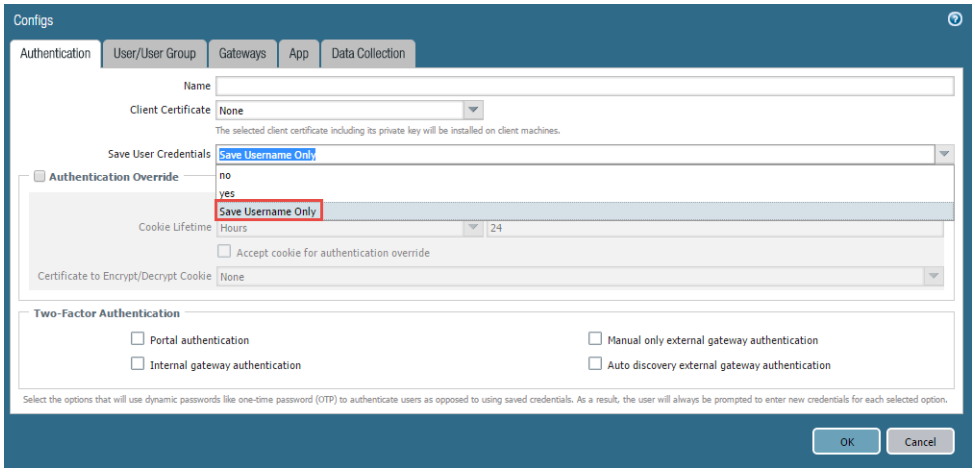
By default GlobalProtect automatically filters the certificates for those that specify a Client Authentication purpose so it is not necessary to specify the associated OID. Note that if multiple client certificates specify the secondary purpose, GlobalProtect would still prompt the user to select the certificate from the filtered list.

GlobalProtect uses only the Extended Key Usage OID field of the certificate and does not evaluate any other certificate fields such as Subject Name to determine whether to present the certificates. Note that the Extended Key Usage OID value is different from the Certificate Template Information OID.

If only one client certificate on the endpoint meets the above criteria, GlobalProtect automatically selects and uses that certificate to authenticate the user. Otherwise, when multiple certificates are installed on the endpoint which meet the above criteria, GlobalProtect prompts the user to select the appropriate certificate. By enabling GlobalProtect to automatically select and authenticate using the appropriate client certificate, you can simplify and improve the user experience.

Save Username Only Option

You can now configure GlobalProtect to save only the username when a user logs in to the GlobalProtect portal or gateway. This new option provides an alternative to saving both the username and password or saving neither. You can configure the new **Save User Credentials** option as part of a GlobalProtect client configuration.



The option supersedes the **Allow user to save password** option, which was available in PAN-OS 7.0. The default behavior for both options permits the GlobalProtect agent to save user credentials. Because the **Allow user to save password** option is now deprecated, the configuration of this setting is discarded upon upgrade of the firewall or Panorama to PAN-OS 7.1. As a result, if you do not want GlobalProtect to save credentials, you must configure an alternate value after you upgrade to PAN-OS 7.1.

If a GlobalProtect portal or gateway requires users to authenticate using dynamic passwords, such as one-time passwords, users must use unique passwords each time they log in. As a result, setting **Save User Credentials** to **Yes** has the same affect as setting **Save User Credentials** to **Save Username Only** because GlobalProtect saves only the username.

Use Address Objects in a GlobalProtect Gateway Client Configuration

You can now use an address object, which can include an IPv4 or IPv6 address (a single IP address, range, or subnet) or an FQDN when you configure any of the following network settings in a GlobalProtect gateway client configuration.

- IP address pools—Support address objects that define a single IP address, range of IP addresses, or IP netmask.
- Access routes—Support address objects that define a single IP address or IP netmask.

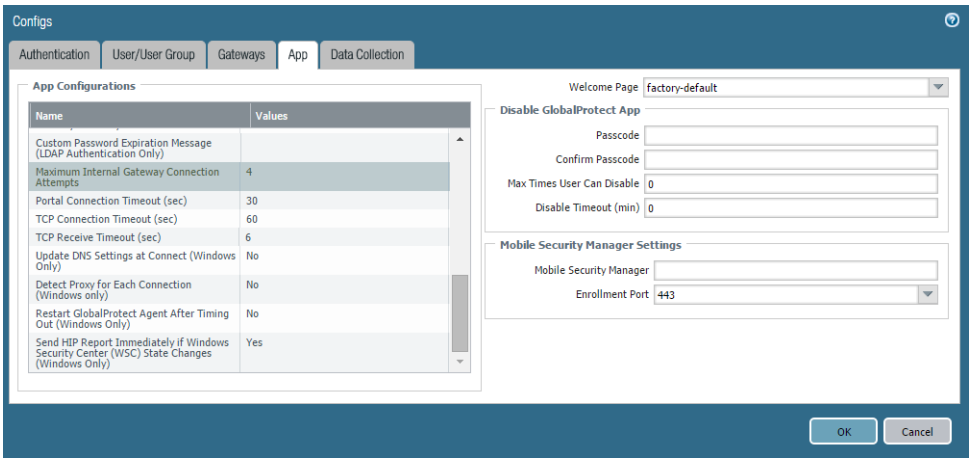
You can also define address objects in Panorama and deploy them with GlobalProtect settings to gateway devices.

Configure Address Objects in a GlobalProtect Gateway Client Configuration		
Step 1	Create an address object or, if managing multiple firewalls using Panorama, create a shared or device group object.	1. Select **Objects** > **Addresses**. 2. (Panorama device groups only) To create a device group object, select the appropriate device group from the Device Group drop-down. 3. **Add** a new object and then enter a **Name** to identify it. 4. Select **Shared** if you want the address object to be available for use elsewhere: • In every virtual system (vsys) on a multi-vsys firewall—if you clear the **Shared** option, the address object will be available only to the **Virtual System** selected in the **Objects** tab. • In every device group on Panorama—if you clear the **Shared** option, the address object will be available only to the **Device Group** selected in the **Objects** tab. 5. (Panorama only) **Disable Override** if you want to prevent administrators from creating local copies of the address in descendant device groups by overriding its inherited values. **Disable Override** is cleared by default, which means overriding is enabled. 6. (Optional) Enter a description for the object (up to 255 characters). 7. Select the **Type** of address object (**IP Netmask**, **IP Range**, or **FQDN**) and the associated value. For example, select **IP Range** and enter the IP address range. 8. (Optional) Select a one or more tags to group your object with other objects that share keywords or phrases. 9. Click **OK** and **Commit**. (Panorama only) To commit a shared object, you must also select **Panorama** for the **Commit Type** and click **Commit** again. To commit a device group object, click **Commit** and then, for the **Commit Type,** select **Device Group**, select the device group to which you added the object, and click **Commit** again.

Configure Address Objects in a GlobalProtect Gateway Client Configuration (Continued)	
Step 2 Configure a GlobalProtect Gateway (either an existing configuration or a new one) and then, for a tunnel interface, use the address object for an IP address pool or access route.	1. Select **Network** > **GlobalProtect** > **Gateways** and then select an existing gateway configuration or **Add** a new one. 2. Select **Agent** > **Client Settings** and then select an existing client configuration or **Add** a new one. 3. (New) On the **Network Settings** tab, **Add** the address object to the **IP Pool** or **Access Route**, as needed, by selecting it from the drop-down. 4. Click **OK** twice. 5. **Commit** your changes.

Maximum Internal Gateway Connection Retry Attempts

Starting with PAN-OS 7.1, you can now configure the **Maximum Internal Gateway Connection Attempts** option as part of the GlobalProtect portal client configuration.

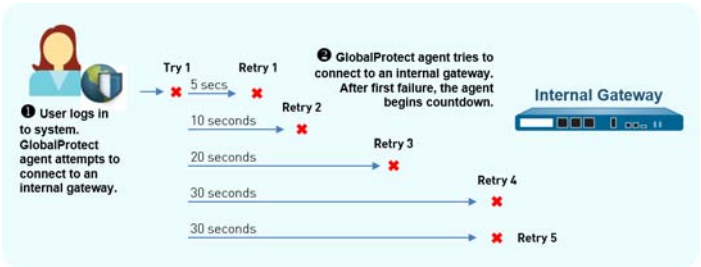


The new option specifies the maximum number of times the GlobalProtect agent should retry the connection to an internal gateway after the first attempt fails (default is 0, which means the GlobalProtect agent does not retry the connection).

By increasing the value, you enable the agent to automatically connect to an internal gateway that is temporarily down or unreachable during the first connection attempt but comes back up before the specified number of retries are exhausted. Increasing the value also ensures that the internal gateway receives the most up-to-date user and host information; However, it also delays the upload of user and host information to any connected internal gateways. This is because the agent waits to upload data until it has connected to all gateways or until all connection attempts are exhausted. During the retry period, all gateways that are reachable must use the previous, out-dated HIP report to enforce policies for the user.

With Content Release version 590-3397 or later, the logic for this feature has been enhanced so that GlobalProtect sends host information to any internal gateways to which it can authenticate during the retry attempt. GlobalProtect continues to authenticate to any internal gateways that were previously unreachable until the number of retry attempts is exhausted or GlobalProtect successfully connects to all the internal gateways. This change enables GlobalProtect to send the most up-to-date host information to available gateways without delays caused by unreachable gateways.

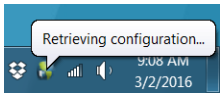
To help ensure that internal gateways receive the most current user and host information, increase the maximum number of connection attempts, to 5 for example. After each failed attempt to connect, the agent waits for a preconfigured amount of time before trying again to connect, as shown in the following figure.



If the agent retries the connection five times, this can delay the submission of user and host information by a minimum of 1 minute 35 seconds (5 + 10 + 20 + 30 + 30); However, with the enhanced logic released with Content Release version 590-3397 or later, the agent sends the host information as soon as it establishes a connection. Therefore, to reduce delays in receiving up-to-date host information, we recommend installing this content release.

GlobalProtect Notification Suppression on Windows

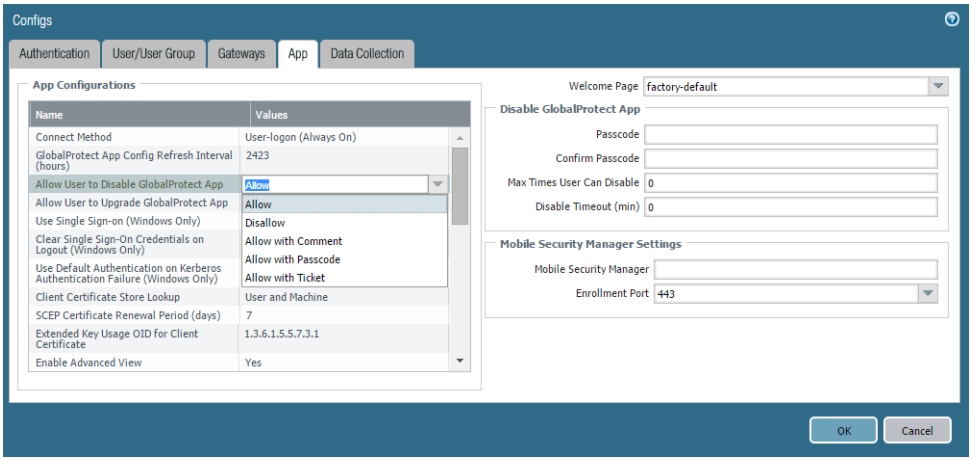
GlobalProtect displays bubble messages from the notification area (system tray) on Windows clients to alert users about changes in the GlobalProtect agent status.



For example, users see notifications for events such as when the agent performs a network rediscovery or attempts to connect to a gateway. You can now suppress these notifications by configuring the **Show System Tray Notifications** options from a GlobalProtect portal agent configuration. Suppressing the notifications can be useful if the notifications are distracting or if you want your users to have a more transparent experience.

Disable GlobalProtect Without Comment

For increased flexibility, you can now allow a user to disable the GlobalProtect app without providing a comment, passcode, or ticket number. Starting in PAN-OS 7.1, you can configure the **Allow User to Disable GlobalProtect App** option from a GlobalProtect portal agent configuration. In earlier releases, this option was only available in the Windows registry and Mac global property list (plist). Settings defined in the GlobalProtect portal agent configuration take precedence over settings defined in the Windows registry or the Mac plist.



Pre-logon then On-Demand Connect Method

This feature requires Content Release version 590-3397 or later.

You can now configure a new hybrid connect method called *pre-logon then on-demand*. The new connect method is supported on endpoints running Windows 7 or Mac OS 10.9 and later releases. The purpose of the new connect method is to provide the functionality of two existing connect methods:

- With *pre-logon* GlobalProtect authenticates the endpoint (not the user) before the user logs in and then establishes a VPN tunnel. As soon as the endpoint powers on, the GlobalProtect agent runs any domain scripts or other tasks of your choice. After the gateway authenticates a Windows user, the VPN tunnel is reassigned to that user (the IP address mapping on the firewall changes from the pre-logon endpoint to the authenticated user). Mac systems behave differently from Windows systems with pre-logon. With Mac OS, the tunnel created for pre-logon is torn down and a new tunnel created when the user logs in.
- With *on-demand*, users must manually initiate connections to external gateways.

The new connect method combines the pre-logon capability to authenticate the user before they log in and the on-demand capability to allow users to establish connections with external gateways manually for subsequent connections. This is useful when users forget their passwords or work with their IT helpdesk to change their password and require network access over a pre-logon VPN tunnel to log into their system. Then, if the tunnel disconnects for any reason, the user must manually connect to a gateway.

Configure Remote Access with Pre-logon then On-demand		
Step 3	Create interfaces and zones for GlobalProtect.	1. Configure a Layer 3 interface for each portal and/or gateway you plan to deploy. 2. On the firewall(s) hosting GlobalProtect gateway(s), configure the logical tunnel interface that will terminate VPN tunnels established by the GlobalProtect agents. 3. If you created a separate zone for tunnel termination of VPN connections, create a security policy to enable traffic flow between the VPN zone and your trust zone. 4. Save the configuration.
Step 4	Create security policy rules. A pre-logon VPN tunnel has no username association because the user has not logged in. Therefore, to enable access to resources in the trust zone, you must create security policies that match the pre-logon user.	• Create a rule that enables the pre-logon user access to basic services that are required for the computer to come up, such as authentication services, DNS, DHCP, and Microsoft Updates. • Create a rule to enable access between the corp-vpn zone and the l3-trust zone for any known user after the user successfully logs in.

Configure Remote Access with Pre-logon then On-demand (Continued)		
Step 5	Obtain a server certificate for the interface that hosts the GlobalProtect portal and gateway: • (Recommended) Import a server certificate from a well-known, third-party CA. • Use the root CA on the portal to generate a self-signed server certificate.	Select **Device** > **Certificate Management** > **Certificates** to manage certificates with the following criteria: • Obtain a server certificate. Because the portal and gateway are on the same interface, the same server certificate can be used for both components. • The CN of the certificate must match the FQDN, gp.acme.com. • To enable clients to connect to the portal without receiving certificate errors, use a server certificate from a public CA.
Step 6	On each firewall that hosts a GlobalProtect gateway, create a certificate profile to identify the CA certificate for validating the machine certificates. Optionally, if you plan to use client certificate authentication to authenticate users when they log in to the system, make sure that the CA certificate that issues the client certificates is referenced in the certificate profile in addition to the CA certificate that issued the machine certificates if they are different.	1. Select **Device** > **Certificates** > **Certificate Management** > **Certificate Profile**. 2. Click **Add** and enter a **Name** to uniquely identify the profile, such as `PreLogonCert`. 3. Set **Username Field** to **None**. 4. (Optional) If you will also use client certificate authentication to authenticate users upon login, add the CA certificate that issued the client certificates if it is different from the one that issued the machine certificates. 5. In the **CA Certificates** field, click **Add**, select the Trusted Root CA certificate you imported in Step 5 and then click **OK**. 6. Click **OK** to save the profile.
Step 7	Generate and deploy machine certificates. During pre-logon, the firewall sees the user as pre-logon for user-IP address mapping, logging and security policies.	1. Generate a machine certificate for each client system that will connect to GlobalProtect and import it into the personal certificate store on each machine. Although you could generate self-signed certificates for each client system, as a best practice, use your own public-key infrastructure (PKI) to issue and distribute certificates to your clients. 2. Import the trusted root CA certificate from the CA that issued the certificates onto the portal and gateways. 3. Click **OK** twice to save the configuration.
Step 8	Configure a GlobalProtect Gateway. Although you must create a certificate profile for access to the gateway using the pre-logon then on-demand connect method, you can use either client certificate authentication or authentication profile-based authentication for logged in users.	1. Select **Network** > **GlobalProtect** > **Gateways** and select and existing gateway configuration or add a new one. 2. After configuring the gateway, **Commit** your changes.

Configure Remote Access with Pre-logon then On-demand (Continued)	
Step 9 Configure the GlobalProtect Portal. First, configure the device details (networking parameters, the authentication service profile, and the certificate for the authentication server). Next, create two agent configuration profiles. With these two types of agent configurations, you can limit gateway access to one gateway for the pre-logon users and provide access to multiple gateways for the logged in users.  As a best practice, enable SSO in the second agent configuration so that the correct username is immediately reported to the gateway when the user logs in to the endpoint. If SSO is not enabled, the saved username in the Agent settings panel is used.	1. Select **Network** > **GlobalProtect** > **Portals**. 2. Select the portal configuration or **Add** one. 3. Set Up Access to the GlobalProtect Portal by configuring the **General** network settings and portal **Authentication** settings, for example: **Interface**—ethernet1/2 **IP Address**—203.0.113.1 **SSL/TLS Service Profile**—GP-server-cert-profile (issued by GoDaddy) **Certificate Profile**—None **Authentication Profile**—Corp-LDAP 4. Define the GlobalProtect Agent Configurations for pre-logon users and for logged in users, for example: First Agent Configuration: **Connect Method**—Pre-logon then on-demand **External Gateway Address**—gp.example.com **User/User Group**—pre-logon **Authentication Override**—Cookie authentication for transparently authenticating users and for configuration refresh Second Agent Configuration: **Use single sign-on**—enabled **Connect Method**—Pre-logon then on-demand **External Gateway Address**—gp.example.com **User/User Group**—any **Authentication Override**—Cookie authentication for transparently authenticating users and for configuration refresh 5. Make sure the pre-logon then on-demand client configuration is first in the list of configurations. If it is not, select it and click **Move Up**.
Step 10 Save the GlobalProtect configuration.	Click **Commit**.
Step 11 (Optional) If users will never log into a device (for example, a headless device) or a pre-logon connection is required on a system that a user has not previously logged into, create the Prelogon registry entry on the client system.  You must also pre-deploy additional agent settings such as the default portal IP address and connect method. For more information about registry settings, see Deploy Agent Settings Transparently.	1. Locate the GlobalProtect settings in the registry: `HKEY_LOCAL_MACHINE\SOFTWARE\Palo Alto Networks\GlobalProtect\PanSetup` 2. Create a **DWORD** named `Prelogon` with a value of `1` in the Value data field and Hexadecimal as the Base. This setting enables GlobalProtect to initiate a VPN connection before the user logs into the laptop. 3. Create a **String Value** named `Portal` that specifies the IP address or hostname of the default portal for the GlobalProtect client. 4. Create a **String Value** named `connect-method` with a value of pre-logon in the Value data field. This setting enables GlobalProtect to initiate a VPN tunnel before a user logs in to the device and connects to the GlobalProtect portal.

Enforce GlobalProtect for Network Access

This feature requires Content Release 590-3397 or a later version.

To reduce the security risk of exposing your enterprise when a user is off-premise, you can now force users on endpoints running Windows 7 or Mac OS 10.9 and later releases to connect to GlobalProtect to access to the network.

When this feature is enabled, GlobalProtect blocks all traffic until the agent is internal or connects to an external gateway. After the agent establishes a connection, GlobalProtect permits internal and external network traffic according to your security policy thus subjecting the traffic to inspection by the firewall and security policy enforcement. This feature also prevents the use of proxies as a means to bypass the firewall and access the Internet.

If users must connect to the network using a captive portal (such as at a hotel or airport), you can also configure a grace period that provides users enough time to connect to the captive portal and then connect to GlobalProtect.

Because GlobalProtect blocks traffic unless the GlobalProtect agent can connect to a gateway, we recommend that you enable this feature only for users that connect in **User-logon** or **Pre-logon** modes.

Enforce a GlobalProtect Connection for Network Access		
Step 1	Configure the GlobalProtect portal.	Select **Network** > **GlobalProtect** > **Portals** and select the portal configuration for which you want to add a client configuration or **Add** a new one.
Step 2	Begin or modify an agent configuration.	1. From the **Agent** tab, select the agent configuration you want to modify or **Add** a new one. 2. Select the **App** tab.
Step 3	Configure GlobalProtect to force all network traffic to traverse a GlobalProtect tunnel.	In the App Configuration area, set **Enforce GlobalProtect Connection for Network Access** to **Yes**. By default, this option is set to **No** meaning users can still access the internet if GlobalProtect is disabled or disconnected.
Step 4	(Optional) To provide additional information, configure a traffic blocking notification message (for example: `To access the network, you must first connect to GlobalProtect.`). The message can indicate the reason for blocking the traffic and provide instructions on how to connect. If you enable this message, GlobalProtect will display the message when GlobalProtect is disconnected but detects the network is reachable.	• In the App Configuration area, make sure **Display Traffic Blocking Notification Message** is set to **Yes**. This is the default. • Specify the message text in the **Traffic Blocking Notification Message** field. The message must be 512 or fewer characters. • To specify when to display the notification (how soon after GlobalProtect determines the network is reachable), configure the **Traffic Blocking Notification Delay** in seconds (default is 15; range is 5 to 120). • To always display traffic blocking notifications, set **Allow Users to Dismiss Traffic Blocking Notifications** to **No**. By default the value is set to **Yes.**

Enforce a GlobalProtect Connection for Network Access (Continued)		
Step 5	(Optional) To allow a grace period before blocking traffic that provides the user time to connect to a captive portal, configure a notification message (for example: `GlobalProtect has temporarily permitted network access for you to connect to the internet. Follow instructions from your internet provider. If you let the connection time out, open GlobalProtect and click Connect to try again.`) and timeout value. The message can provide additional information about connecting to the captive portal.	• In the App Configuration area, make sure **Display Captive Portal Detection Message** is set to **Yes**. The default is **No.** • Specify the message text in the **Captive Portal Detection Message** field. The message must be 512 or fewer characters. • To specify the amount of time in which the user has to authenticate with a captive portal, enter the **Captive Portal Exception Timeout** in seconds (default is 0; range is 0 to 3600). For example, a value of 60 means that the user must log in to the captive portal within one minute after GlobalProtect detects the captive portal. A value of 0 means GlobalProtect does not allow users to connect to a captive portal and immediately blocks access. • If you have a **Captive Portal Detection Message** enabled, the message appears 85 seconds before the **Captive Portal Exception Timeout** occurs. If the **Capture Portal Exception Timeout** is 90 seconds or less, the message appears 5 seconds after a captive portal is detected.
Step 6	Save your configuration changes.	1. Click **OK** twice. 2. **Commit** your changes.

Connection Behavior on Smart Card Removal

This feature requires Content Release version 590-3397 or later.

After you enable smart card authentication on Windows endpoints, users can authenticate using a smart card or common access card (CAC) containing a client certificate. Now, when a user removes that card, you can either retain or disconnect the connection with GlobalProtect. By default, GlobalProtect retains the tunnel when the user removes the smart card. The decision on whether to retain the connection depends on your security requirements.

Configure the Connection Behavior on Smart Card Removal	
Step 1 Enable smart card authentication.	1. Set up your smart card infrastructure. 2. Import the Root CA certificate that issued the client certificates contained on the end user smart cards. 3. Create the certificate profile. 4. Assign the certificate profile to the gateway(s) or portal. 5. Commit the configuration.
Step 2 Configure the GlobalProtect portal.	Select **Network** > **GlobalProtect** > **Portals** and select the portal configuration for which you want to add a client configuration or **Add** a new one.
Step 3 Begin or modify an agent configuration.	1. From the **Agent** tab, select the agent configuration you want to modify or **Add** a new one. 2. Select the **App** tab.
Step 4 Configure the connection behavior when a user removes a smart card.	In the App Configuration area, set **Retain Connection on Smart Card Removal (Windows Only)** to **Yes**.
Step 5 Save your configuration changes.	1. Click **OK** twice. 2. **Commit** your changes.

User-ID Features

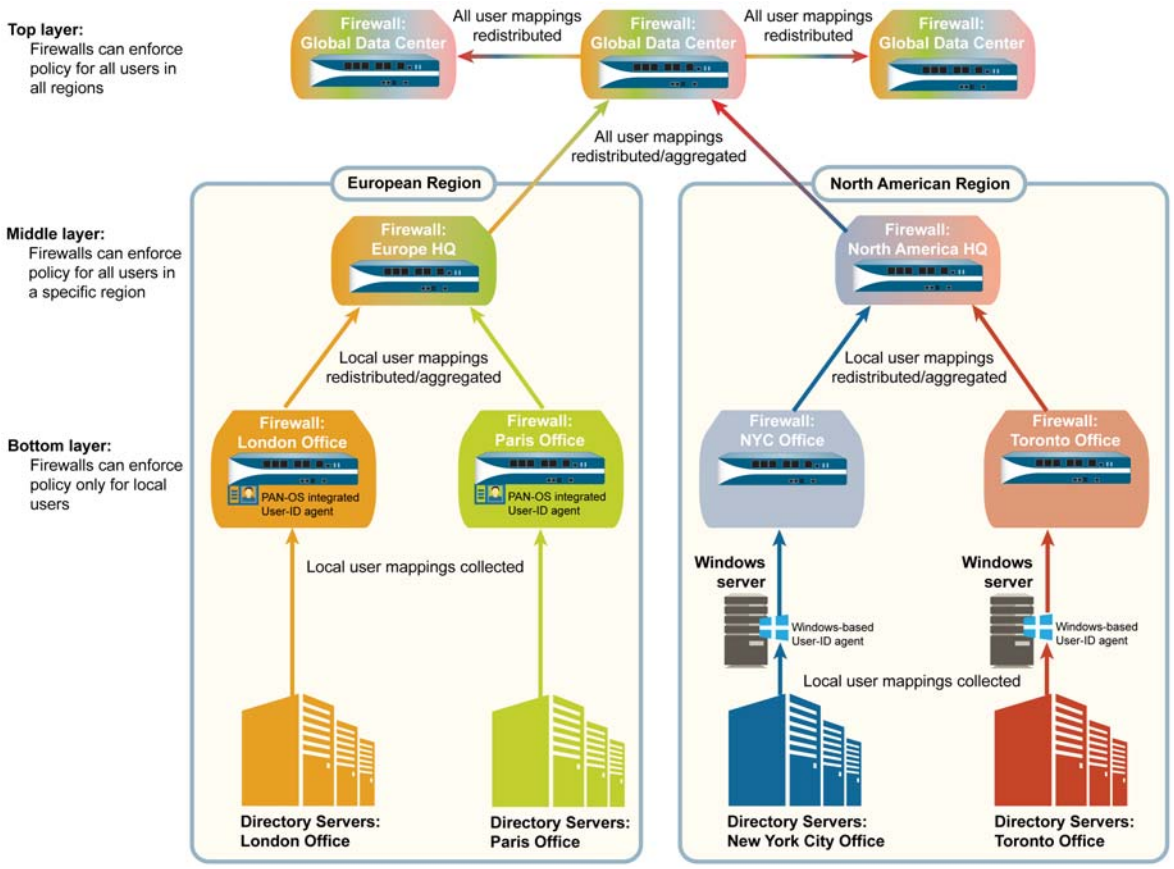
- User-ID Redistribution Enhancement
- Ignore User List Configurable in Web Interface
- User Group Capacity Increase

User-ID Redistribution Enhancement

You can now relay user mapping information from one firewall to another in a sequence of up to ten firewalls instead of only two. This increase in the relay sequence enables you to redistribute mapping information in a large-scale network that has hundreds of user identification sources or that has users who rely on local sources for authentication (such as regional directory services) but who require access to remote resources (such as global data center applications). Redistributing mapping information also reduces the resources that firewalls and information sources use because fewer firewalls query the sources directly.

Figure: User-ID-Redistribution shows how you can organize the redistribution sequence in layers, where each layer has one or more firewalls. In this example, bottom-layer firewalls in local offices redistribute mapping information to middle-layer firewalls in regional offices, which redistribute to one top-layer firewall in a global data center. The data center firewall redistributes the mapping information to other data center firewalls so that they can enforce global policies for all users.

Figure: User-ID-Redistribution



Configure User-ID Redistribution	
Step 1 Plan the redistribution architecture.	❑ Decide which User-ID agents and methods to use for user mapping (IP addresses to usernames). You cannot redistribute user mapping information that Terminal Services (TS) agents collect. You also cannot redistribute group mapping information. ❑ Determine the most efficient firewall deployment for User-ID redistribution.
Step 2 Configure User-ID agents to perform user mapping.	• Configure user mapping using PAN-OS Integrated User-ID agents. • Configure user mapping using Windows-based User-ID Agents.
Step 3 Configure the firewalls to receive and redistribute mapping information.	1. Enable each bottom-layer firewall to forward mapping information to one or more firewalls in the layer directly above. 2. Enable each firewall in the middle layers to receive mapping information from the layer below and forward that information to the layer above. You must also perform this task for a firewall (in any layer) that redistributes mapping information to other firewalls in the same layer. For example, Figure: User-ID-Redistribution shows one data center firewall that redistributes to other data center firewalls. Figure: User-ID-Redistribution shows only one middle layer of firewalls but you can deploy as many layers as the redistribution limit of ten hops allows. 3. Enable each top-layer firewall to receive mapping information from all other layers. You must also perform this task for any firewall that is an end point in the redistribution sequence within a layer. For example, Figure: User-ID-Redistribution shows two data center firewalls that receive mapping information from another data center firewall. 4. Verify that the top-layer firewalls are aggregating mapping information from all other layers.

Ignore User List Configurable in Web Interface

For the PAN-OS integrated User-ID agent, you can now use the firewall web interface as an alternative to the CLI to configure the ignore user list and specify user accounts that don't require IP address-to-username mapping (such as kiosk accounts). Using the web interface is easier and reduces the chance of errors that can compromise enforcement of user-based policies.

Configure the Ignore User List	
Step 1	Select **Device** > **User Identification** > **User Mapping** and edit the Palo Alto Networks User-ID Agent Setup.
Step 2	Select the **Ignore User List** tab.
Step 3	Click **Add** and enter a username. You can use an asterisk as a wildcard character to match multiple usernames, but only as the last character in the entry. For example, **`corpdomain\it-admin*`** would match all administrators in the **`corpdomain`** domain whose usernames start with the string **`it-admin`**. You can add up to 5,000 entries to exclude from user mapping.
Step 4	Click **OK** and **Commit**.

User Group Capacity Increase

On PA-5060 and PA-7000 Series firewalls that are configured without multiple virtual systems (feature is disabled), you can now base policies on up to 3,200 distinct user groups instead of 640. This ensures continued security on networks that use a large number of groups to control access to resources.

Configure a Group-Based Policy Rule on a PA-5060 or PA-7000 Series Firewall		
Step 1	Disable the multiple virtual systems capability if it is currently enabled.	1. Select **Device** > **Setup** > **Management** and edit the General Settings. 2. Clear **Multi Virtual System Capability** and click **OK**.
Step 2	Add an LDAP server profile.	1. Select **Device** > **Server Profiles** > **LDAP**, click **Add**, and enter a **Profile Name**. 2. For each LDAP server (up to four), click **Add** and enter the server **Name**, IP address (**LDAP Server**), and **Port** (default is 389). 3. Select the **Type** of servers you added (for example, **active-directory**); all servers in any single LDAP server profile must be the same **Type**. 4. Click **OK**.
Step 3	Configure group mapping.	1. Select **Device** > **User Identification** > **Group Mapping Settings** and click **Add**. 2. Enter a unique **Name** to identify the group mapping configuration. 3. Configure the **Server Profile** settings: a. Select the LDAP **Server Profile** you just created. b. Select **Enabled** (default). Do not add entries to the **Group Include List** or **Custom Group** list—doing so limits the number of groups that policy rules can reference. Populated lists can have a combined maximum of only 640 groups but, by default, leaving the lists empty enables policy rules to reference up to a maximum of 3,200 groups. 4. Click **OK**.
Step 4	Enable User-ID on the source zones that contain the users who will request resources that are subject to group-based access control.	1. Select **Network** > **Zones** and click the zone **Name** to edit the zone. 2. Select **Enable User Identification** and click **OK**.

Configure a Group-Based Policy Rule on a PA-5060 or PA-7000 Series Firewall (Continued)	
Step 5 Configure a group-based policy rule.	Perform these steps for each rule that references user groups. Collectively, all the rules of all policy types on the firewall can reference up to 3,200 distinct groups. 1. Select **Policies** > **Security** and click **Add**. 2. Enter a **Name** to identify the rule. 3. Select the **User** tab and, for each user group to match in the rule, click **Add** in the Source User section and select the group. 4. Configure the rest of the rule as appropriate. 5. Click **OK** and **Commit**.  If you later decide to enable multiple virtual systems on the firewall that you configured in this procedure, you must first reduce the number of distinct groups to 640. After you enable and add multiple virtual systems, the policies can then reference another 640 groups for each additional virtual system.

Networking Features

- Failure Detection with BFD
- LACP and LLDP Pre-Negotiation on an HA Passive Firewall
- Binding a Floating IP Address to an HA Active-Primary Firewall
- Multicast Route Setup Buffering
- Per-VLAN Spanning Tree (PVST+) BPDU Rewrite
- Configurable MSS Adjustment Size
- DHCP Client Support on Management Interface
- PA-3000 Series and PA-500 Firewall Capacity Increases
- SSL/SSH Session End Reasons
- Fast Identification and Mitigation of Sessions That Overutilize the Packet Buffer

Failure Detection with BFD

The firewall now supports Bidirectional Forwarding Detection (BFD), a protocol that recognizes a failure in the bidirectional path between two routing peers. BFD failure detection provides a faster failover than can be achieved by link monitoring or frequent dynamic routing health checks, such as Hello packets or heartbeats. Mission-critical data centers and networks that require high availability and extremely fast failover need the extremely fast failure detection that BFD provides. PAN-OS supports BFD on PA-3000 Series, PA-5000 Series, PA-7000 Series, and VM-Series firewalls starting with PAN-OS 7.1.

Configure BFD		
Step 1	Create a BFD profile.	A BFD profile is where you configure the BFD mode, transmit and receive intervals, detection time multiplier, and hold time.
Step 2	Enable BFD for a static route or a routing protocol.	For a virtual router, you can Configure BFD for a static route, the RIP, OSPF, or BGP routing protocols, or for a single interface where you are running the routing protocol.

LACP and LLDP Pre-Negotiation on an HA Passive Firewall

Firewalls in a high availability (HA) active/passive configuration must be able to fail over quickly. If the firewall is using LACP or LLDP, the LACP or LLDP negotiation upon failover prevents sub-second failover. To preempt this negotiation after a passive firewall becomes active, you can now enable an interface on a passive firewall to negotiate LACP and LLDP before a failover occurs. The firewall in passive or non-functional HA state communicates with neighboring devices using LACP or LLDP. Such pre-negotiation speeds up failover because LACP or LLDP is already negotiated before the failover occurs.

The PA-3000 Series, PA-5000 Series, and PA-7000 Series firewalls support a pre-negotiation configuration (**Enable in HA Passive State**) as shown in the following table. An HA passive firewall handles LACP and LLDP packets in one of two ways:

- **Active**—The firewall has LACP or LLDP configured on the interface and actively participates in LACP or LLDP pre-negotiation respectively.
- **Passive**—LACP or LLDP is not configured on the interface and the firewall does not participate in the protocol but allows the peers on either side of the firewall to pre-negotiate LACP or LLDP respectively.

Use the information in the following topics to determine where and how you can enable LACP and LLDP pre-negotiation on an HA passive firewall:

▲ LACP and LLDP Pre-Negotiation Support

▲ Enable LACP and LLDP Pre-Negotiation on an HA Passive Firewall

LACP and LLDP Pre-Negotiation Support

The following table displays what deployments are supported on Ethernet and Aggregate Ethernet (AE) interfaces.

Interface Deployment	AE Interface	Ethernet Interface
LACP in Layer 2	Active	Not supported
LACP in Layer 3	Active	Not supported
LACP in Virtual Wire	Not supported	Passive
LLDP in Layer 2	Active	Active
LLDP in Layer 3	Active	Active
LLDP in Virtual Wire	Active	• Active if LLDP itself is configured. • Passive if LLDP itself is not configured.

Pre-negotiation is not supported on subinterfaces or tunnel interfaces.

Enable LACP and LLDP Pre-Negotiation on an HA Passive Firewall

You should enable LACP and LLDP before you configure HA pre-negotiation if you want the firewall to actively participate in pre-negotiation respectively. Perform the following procedure on both firewalls to configure pre-negotiation.

Enable LACP or LLDP Pre-Negotiation for an Interface on an HA Passive Firewall		
Step 1	Configure active/passive HA.	When you configure active/passive HA, set the link state to Auto. 1. Select **Device** > **High Availability** > **General** and edit Active Passive Settings. 2. Set the **Passive Link State** to **Auto**.
Step 2	Select an interface for LACP or LLDP pre-negotiation.	Select **Network** > **Interfaces** > **Ethernet** and then enable appropriate pre-negotiation: Enable LACP active pre-negotiation for an HA passive firewall 1. Select an Aggregate Ethernet (AE) interface in a Layer 2 or Layer 3 deployment. 2. On the **LACP** tab, select **Enable in HA Passive State**. You cannot also select **Same System MAC Address for Active-Passive HA** because pre-negotiation requires unique interface MAC addresses on the active and passive firewalls. 3. Click **OK**. Enable LACP passive pre-negotiation for an HA passive firewall 1. Select an Ethernet interface in a virtual wire deployment. 2. Select the **Advanced** tab. 3. On the **LACP** tab, select **Enable in HA Passive State**. 4. Click **OK**. Enable LLDP active pre-negotiation for an HA passive firewall If you want to allow LLDP passive pre-negotiation for a virtual wire deployment, perform this step but do not enable LLDP itself. 1. Select an Ethernet interface in Layer 2, Layer 3, or virtual wire deployment. 2. Select the **Advanced** tab. 3. On the **LLDP** tab, select **Enable in HA Passive State**. 4. Click **OK**.
Step 3	Save the configuration.	Click **Commit**.

Step 4	(Optional) Display pre-negotiation configuration and a summary of all interfaces on which pre-negotiation is enabled.	• In the web interface, select **Dashboard** > **Widgets** > **System** > **High Availability**. The passive firewall indicates **(Network pre-negotiation enabled)**. Click that link to display a summary of all interfaces enabled with pre-negotiation.
		• In the CLI, use any of the following operational commands:
		  • `show lacp aggregate-ethernet all`
		  • `show lldp config all`
		  • `show high-availability pre-negotiation summary`

Binding a Floating IP Address to an HA Active-Primary Firewall

In a high availability (HA) active/active configuration, a Layer 3 deployment often uses floating IP addresses, which can move between HA firewalls to allow a persistent connection when a link or firewall fails. You can now bind a floating IP address to whichever firewall is in the active-primary state. Thus, on a failover, when the active-primary firewall (Peer A) goes down and the active-secondary firewall (Peer B) takes over as the active-primary peer, the floating IP address moves to Peer B. Peer B remains the active-primary firewall, even when Peer A recovers and becomes the active-secondary firewall. You control when Peer A becomes the active-primary firewall again.

In mission-critical data centers, you can benefit from binding the floating IP address to the active-primary firewall. You can have an HA active/active configuration for path monitoring out of both firewalls but have the firewalls function like an HA active/passive configuration because traffic directed to the floating IP address always goes to the active-primary firewall.

When you also disable preemption on both firewalls, you gain the following additional benefits:

- The floating IP address does not move back and forth between HA firewalls if the active-secondary firewall flaps up and down.
- You can run health checks on the recovered firewall before manually directing traffic to it again, which you can do during a convenient downtime.
- You have control over which firewall owns the floating IP address so that you keep all flows of new and existing sessions on the active-primary firewall, thereby minimizing traffic on the HA3 link.

Bind a Floating IP Address to an HA Active-Primary Firewall		
Step 1	Configure active/active HA with the floating IP address bound to the active-primary firewall.	The HA virtual address is a floating IP address that you bind to the active-primary firewall.
Step 2	(Optional) Disable preemption.  Disabling preemption gives you full control over when the recovered firewall becomes the active-primary firewall.	1. Select **Device** > **High Availability** > **General** and edit the Election Settings. 2. Clear **Preemptive** if checked. 3. Click **OK**.
Step 3	Enable link monitoring on the interface of the HA virtual address (floating IP address).	To enable link monitoring, see Step 1 in Define HA Failover Conditions.
Step 4	Enable path monitoring.	To enable path monitoring, see Step 3 in Define HA Failover Conditions.
Step 5	Next Steps...	Configure the HA peer firewall.

Multicast Route Setup Buffering

You can now enable buffering of the first packet in a multicast session when the multicast route or forwarding information base (FIB) entry does not, yet, exist for the corresponding multicast group. By default, the firewall does not buffer the first multicast packet in a new session; instead, it uses the first packet to set up the multicast route. This is expected behavior for multicast traffic. You need to enable multicast route setup buffering only if your content servers are directly connected to the firewall and your custom application cannot withstand the first packet in the session being dropped.

Enable Multicast Route Setup Buffering		
Step 1	Enable buffering of the first packet in the multicast session.	1. Select **Device** > **Setup** > **Session** and edit the Session Settings. 2. Select **Multicast Route Setup Buffering** to enable the feature. 3. If you want to modify the buffer size, continue to the next step. Otherwise, click **OK** to save the setting.
Step 2	(Optional) Tune the multicast route setup buffer.  The firewall can buffer a maximum of 5,000 packets.	1. In the Session Settings dialog, set the Buffer Size per flow to a value from 1-2,000. 2. To save the settings, click **OK**.
Step 3	(Optional) Tune the amount of time a multicast route stays in the routing table.	1. Select **Network** > **Virtual Router** and select the virtual router that handles the multicast traffic. 2. Select **Multicast** > **Advanced**. 3. Set the **Multicast Route Age Out Time (sec)** to a value from 210 (default) to 7,200. 4. To save the settings, click **OK**.
Step 4	Save the configuration.	Click **Commit**.

Per-VLAN Spanning Tree (PVST+) BPDU Rewrite

When an interface on the firewall is configured for a Layer 2 deployment, the firewall now rewrites the inbound Port VLAN ID (PVID) number in a Cisco per-VLAN spanning tree (PVST+) or Rapid PVST+ bridge protocol data unit (BPDU) to the proper outbound VLAN ID number and forwards the BPDU out. This default behavior beginning in PAN-OS 7.1 allows the firewall to correctly tag Cisco proprietary PVST+ and Rapid PVST+ frames between Cisco switches in VLANs on either side of the firewall so that spanning tree loop detection using Cisco PVST+ and Rapid PVST+ can function properly. The firewall is not participating in the Spanning Tree Protocol (STP) election process and there is no behavior change for other types of spanning tree.

The Cisco switch must have the loopguard disabled for the PVST+ or Rapid PVST+ BPDU rewrite to function properly on the firewall.

This feature is supported on Layer 2 Ethernet and Aggregated Ethernet (AE) interfaces only. The firewall supports a PVID range of 1-4,094 with a native VLAN ID of 1 to be compatible with the Cisco native VLAN implementation.

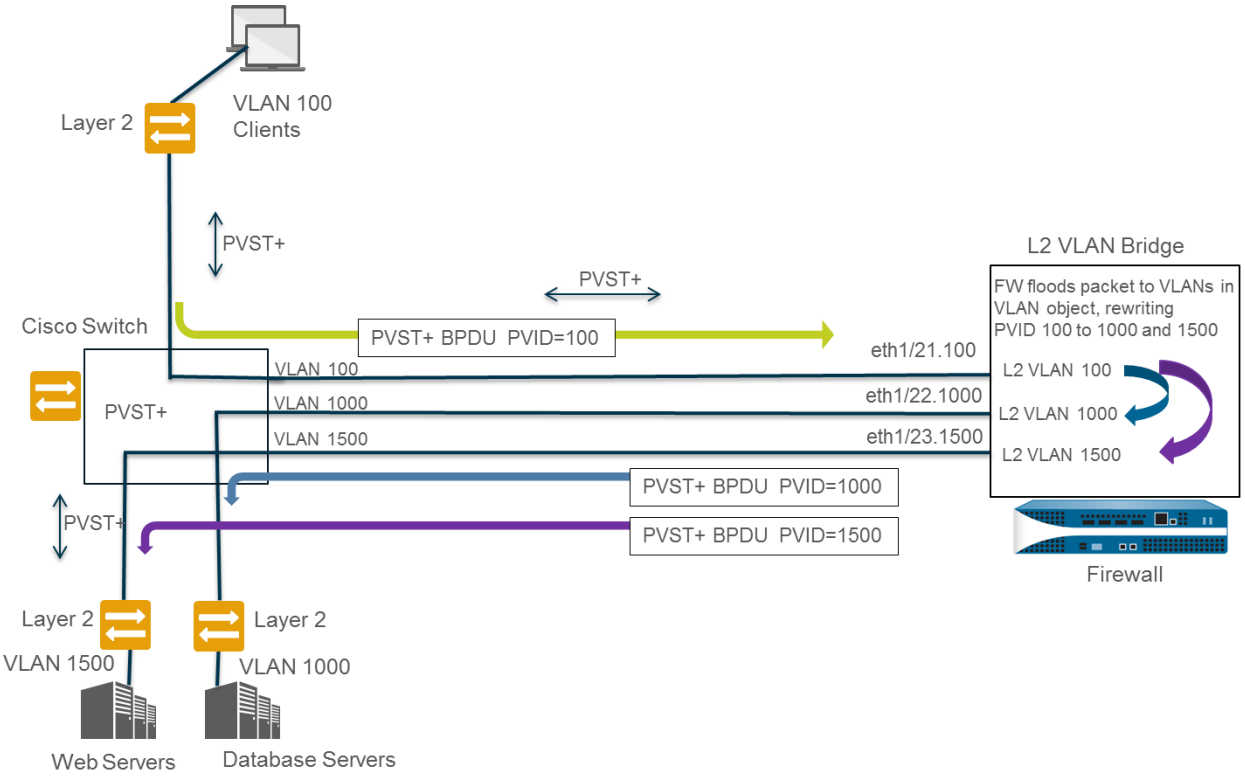
To support the PVST+ BPDU rewrite feature, PAN-OS now supports the concept of a PVST+ native VLAN. Frames sent to and received from a native VLAN are untagged with a PVID equal to the native VLAN. All switches and firewalls in the same Layer 2 deployment must have the same native VLAN for PVST+ to function properly. Although the Cisco native VLAN defaults to vlan1, the VLAN ID could be a number other than 1.

For example, the firewall is configured with a VLAN object (named VLAN_BRIDGE), which describes the interfaces and subinterfaces that belong to a switch or broadcast domain. In this example, the VLAN includes three subinterfaces: ethernet1/21.100 tagged with 100, ethernet1/22.1000 tagged with 1000, and ethernet1/23.1500 tagged with 1500.

The subinterfaces belonging to VLAN_BRIDGE look like this:

Interface	Interface Type	Link State	Tag	VLAN / Virtual-Wire	Security Zone
ethernet1/21	Layer2		Untagged	none	none
ethernet1/21.100	Layer2		100	VLAN_BRIDGE	Zone_Trust
ethernet1/22	Layer2		Untagged	none	none
ethernet1/22.1000	Layer2		1000	VLAN_BRIDGE	Zone_Untrust
ethernet1/23	Layer2		Untagged	none	none
ethernet1/23.1500	Layer2		1500	VLAN_BRIDGE	Zone_Management

The sequence in which the firewall automatically rewrites the PVST+ BPDU is shown in the following topology illustration:



- The Cisco switch port belonging to VLAN 100 sends a PVST+ BPDU—with the PVID and 802.1Q VLAN tag set to 100—to the firewall.
- The firewall interfaces and subinterfaces are configured as a Layer 2 interface type. The ingress subinterface on the firewall is tagged with VLAN 100, which matches the PVID and VLAN tag of the incoming BPDU so the firewall accepts the BPDU. The firewall floods the PVST+ BPDU to all other interfaces belonging to the same VLAN object (in this example, ethernet1/22.1000 and ethernet1/23.1500). If the VLAN tags did not match, the firewall would have, instead, dropped the BPDU.
- When the firewall floods the BPDU out through other interfaces (belonging to the same VLAN object), the firewall rewrites the PVID and any 802.1Q VLAN tags to match the VLAN tag of the egress interface. In this example, the firewall rewrites the BPDU PVID from 100 to 1000 for one subinterface and from 100 to 1500 for the second subinterface as the BPDU traverses the Layer 2 bridge on the firewall.
- Each Cisco switch receives the correct PVID and VLAN tag on the incoming BPDU and processes the PVST+ packet to detect possible loops in the network.

The following table describes different options you can use to manage PVST+ and Rapid PVST+ BPDUs.

Manage PVST+ and Rapid PVST+ BPDUs	
The PVST+ and Rapid PVST+ BPDU rewrite of the PVID is enabled by default; you can globally disable and re-enable it.	Use the following CLI operational command: `set session rewrite-pvst-pvid yes|no`

Manage PVST+ and Rapid PVST+ BPDUs (Continued)	
Set the native VLAN ID for the firewall (range is 1-4,094; default is 1). If the native VLAN ID on your switch is a value other than 1, you must set the native VLAN ID on the firewall to that same number; otherwise, the firewall will drop packets with that VLAN ID. This applies to trunked and non-trunked interfaces.	Use the following CLI operational command: `set session pvst-native-vlan-id <vid>`
Drop all STP BPDU packets. Examples of why you might want to drop all STP BPDU packets: • If there is only one switch on each side of the firewall and no other connections between the switches that can cause a loop, then STP is not required and can be disabled on the switch or blocked by the firewall. • If there is a misbehaving STP switch inappropriately flooding BPDUs, you can drop the STP packets at the firewall to stop the BPDU flood.	Use the following CLI operational command: `set session drop-stp-packet yes|no`

Verify whether PVST+ BPDU rewrite is enabled, view the PVST native VLAN ID, and determine whether the firewall is dropping all STP BPDU packets.	Use the following CLI operational command:
	`admin@pa-vm-30-20> show vlan all`
	`pvst+ tag rewrite: disabled`
	`pvst native vlan id: 5`
	`drop stp: disabled`
	`total vlans shown: 1`
	`name interface virtual interface`
	`bridge ethernet1/1`
	`ethernet1/2`
	`ethernet1/1.1`
	`ethernet1/2.1`
	`ethernet1/2.5`
	`ethernet1/1.5`

Troubleshoot PVST+ BPDU errors.	Use the following CLI operational command: `show counter global` Look at the `flow_pvid_inconsistent` counter, which counts the number of times the 802.1Q Tag and PVID fields inside a PVST+ BPDU packet do not match.

Configurable MSS Adjustment Size

The maximum transmission unit (MTU) is a value indicating the largest number of bytes that can be transmitted in a single TCP packet. The MTU includes the length of headers so, when you subtract the number of bytes in the headers from the MTU, the remaining value is the maximum segment size (MSS), which is the maximum number of data bytes that can be transmitted in a single packet.

Based on typical IP header and TCP header lengths of 20 bytes each, releases prior to PAN-OS 7.1 used a fixed length of 40 bytes as the IPv4 adjustment size to determine the MSS and used 60 bytes for the IPv6 adjustment size. Beginning with PAN-OS 7.1, the value of the MSS adjustment size is configurable. This flexibility allows the firewall to pass traffic with headers totaling more (or less) than 40 bytes as needed. Encapsulation adds length to headers so it is helpful to be able to configure the MSS adjustment size to allow bytes, for example, to accommodate an MPLS header or for tunneled traffic that includes a VLAN tag.

Modify the MSS Adjustment Size		
Step 1	Change the MSS adjustment size settings for a Layer 3 interface if the default settings are not what you need.	1. Select **Network** > **Interfaces**, select **Ethernet**, **VLAN**, or **Loopback**, and select a Layer 3 interface. 2. On the **Advanced** tab, select **Other Info**. 3. Select **Adjust TCP MSS** and enter a value for one or both of the following: • **IPv4 MSS Adjustment Size** (range is 40-300 bytes; default is 40 bytes). • **IPv6 MSS Adjustment Size** (range is 60-300 bytes; default is 60 bytes). 4. Click **OK**.
Step 2	Save the configuration.	Click **Commit**.

DHCP Client Support on Management Interface

In cloud and multi-tenant service provider environments, one goal is to automatically deploy and provision firewalls without manually assigning an IP address to the management interface. The management interface on the firewall now supports the option to enable a DHCP client for IPv4 so that the management interface can receive its IPv4 address from a DHCP server. The management interface also supports DHCP Option 12 and Option 61; these options allow the firewall to send its host name and client identifier, respectively, to DHCP servers.

DHCP client functionality on the management interface is enabled by default on VM-Series firewalls in the AWS and Azure public cloud deployments and on VMware NSX edition firewalls. VM-Series firewalls in these environments require this automation and must use the management interface as a DHCP client to obtain the IP address (instead of using a static IP address). For VM-Series firewalls on all other hypervisors and on all hardware-based firewalls, DHCP client functionality on the management interface is disabled by default. You can enable the DHCP client using the web interface or the CLI on the firewall, or as a part of the process to Bootstrap the Firewall.

WildFire and Panorama do not support DHCP on the management interface—you must assign a static IP address, instead.

Configure the Management Interface as a DHCP Client	
Configure the Management interface as a DHCP client.	The Management interface can receive its IPv4 address, netmask, and default gateway from the DHCP server. Additionally, you have the option to configure your firewall to receive its hostname and domain from the server. You can also send the hostname and client identifier of the firewall to the server if the orchestration system you use accepts this information.

PA-3000 Series and PA-500 Firewall Capacity Increases

PA-3000 Series and PA-500 firewalls support larger networking capacities in PAN-OS 7.1 than in earlier PAN-OS releases. The increase is a doubling of capacity unless you executed the `debug system arp-mac-capacity increase` operational command (available in PAN-OS 6.1 and 7.0.1 releases) on a PA-3020 or PA-3050 firewall, in which case you already doubled the capacity.

The following table lists the capacities in PAN-OS 7.1 and later releases.

Capacity Description	PA-500	PA-3020	PA-3050	PA-3060
Number of entries in an ARP table per broadcast domain	2,000	3,000	5,000	10,000
Number of entries in an ARP table per firewall	2,000	3,000	5,000	10,000
Number of addresses in a MAC table per broadcast domain	2,000	3,000	5,000	5,000
Number of addresses in a MAC table per firewall	2,000	3,000	5,000	5,000
Number of addresses in a Forwarding Information Base (FIB) table per virtual router	1,250	5,000	10,000	10,000
Number of routes in a Forwarding Information Base (FIB) table per virtual router	1,250	5,000	10,000	10,000
Number of addresses in a FIB table per firewall	1,250	5,000	10,000	10,000
Number of addresses in an IPv6 Neighbor table per firewall	2,000	3,000	5,000	10,000

If you decide to downgrade to an older PAN-OS release and you want to keep the larger capacities, see Downgrade While Maintaining Enhanced Capacities on PA-3050 Firewalls and PA-3020 Firewalls.

SSL/SSH Session End Reasons

The Session End Reason column in Traffic logs now includes additional end reasons pertaining to terminated SSL/SSH sessions. You can use this information to troubleshoot access issues for internal users requesting external services or for external users requesting internal services. If a session ends for multiple reasons, the field displays only the highest priority reason based on the following list, where the first reason in the list is the highest priority (the **decrypt-** prefix indicates an SSL/SSH session end reason): threat, policy-deny, **decrypt-cert-validation**, **decrypt-unsupport-param**, **decrypt-error**, tcp-rst-from-client, tcp-rst-from-server, resources-unavailable, tcp-fin, tcp-reuse, decoder, aged-out, and unknown.

- Diagnose SSL/SSH Session Terminations
- Monitor SSL/SSH Session Termination Events

Diagnose SSL/SSH Session Terminations

The SSL/SSH session end reasons indicate that a session ended because you configured a firewall decryption rule with a Decryption Profile that blocks SSL forward proxy decryption or SSL inbound inspection when one (or more) of the following conditions occurs:

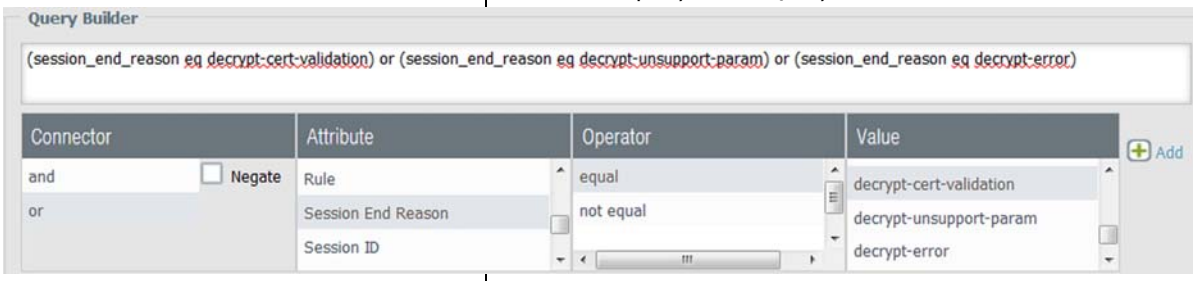
SSL/SSH Session End Reason	Conditions
decrypt-cert-validation	The session used client authentication or used a server certificate with one or more of the following conditions: expired, untrusted issuer, unknown status, or status verification time-out. This session end reason is also displayed when the server certificate produced a fatal error alert of type bad_certificate, unsupported_certificate, certificate_revoked, access_denied, or no_certificate_RESERVED (SSLv3 only).
decrypt-unsupport-param	The session used an unsupported protocol version, cipher, or SSH algorithm. This session end reason is also displayed when the session produced a fatal error alert of type unsupported_extension, unexpected_message, or handshake_failure.
decrypt-error	Firewall resources or the hardware security module (HSM) were unavailable for the session. This session end reason is also displayed when you configured the firewall to block SSL traffic that has SSH errors or that produced any fatal error alert other than those listed for the decrypt-cert-validation and decrypt-unsupport-param end reasons.

Monitor SSL/SSH Session Termination Events

To see session end reasons, select **Monitor** > **Logs** > **Traffic** and check the Session End Reason column.

To configure a custom report that lists SSL/SSH session termination events, perform the following steps.

Monitor SSL/SSH Session Termination Events		
Step 1	Configure the report parameters.	1. Select **Monitor** > **Manage Custom Reports** and **Add** a new report. 2. Enter a **Name** for the report. 3. In the **Database** drop-down, under Detailed Logs, select **Traffic Log**. 4. Select **Scheduled** to automatically run the report each night. 5. In the **Available Columns** list, double-click **Session_end_reason** and any other columns you want the report to include.
Step 2	Configure queries if you want to filter the report. This example shows how to configure the report to display only SSL/SSH session termination events as shown in the following screen capture.	Perform the following steps for each SSL/SSH session end reason: 1. Set the **Connector** to **or**. 2. Set the **Attribute** to **Session End Reason**. 3. Set the **Operator** to **equal**. 4. Set the **Value** to an SSL/SSH session end reason. 5. **Add** the query to the Query Builder field.
Step 3	Test and save the report.	1. **Run Now** to test the report settings; a new tab within the dialog displays the report. 2. Modify the settings as needed and then click **OK** and **Commit**.



Fast Identification and Mitigation of Sessions That Overutilize the Packet Buffer

When a firewall exhibits signs of resource depletion, it might be experiencing an attack that is sending an overwhelming number of packets. In such events, the firewall starts buffering inbound packets. Now you can quickly identify the sessions that are using an excessive percentage of the packet buffer and mitigate their impact by discarding them.

- Identify Sessions That Use an Excessive Percentage of the Packet Buffer
- Discard a Session Without a Commit

Identify Sessions That Use an Excessive Percentage of the Packet Buffer

Perform the following task on any hardware-based firewall platform (not a VM-Series firewall) to identify the packet buffer percentage used, the top five sessions using more than two percent of the packet buffer, and the source IP addresses associated with those sessions; this information allows you to take appropriate actions.

View Firewall Resource Usage, Top Sessions, and Session Details

Step 1 View firewall resource usage, top sessions, and session details. Execute the following operational command in the CLI (sample output from the command follows):

```
admin@PA-7050> show running resource-monitor ingress-backlogs
-- SLOT:s1, DP:dp1 --
USAGE - ATOMIC: 92%  TOTAL: 93%
TOP SESSIONS:
SESS-ID      PCT   GRP-ID   COUNT
6            92%   1        156
                   7        1732
SESSION DETAILS
SESS-ID  PROTO SZONE SRC       SPORT  DST      DPORT  IGR-IF     EGR-IF     APP
6        6     trust 192.168.2.35  55653  10.1.8.89  80     ethernet1/21 ethernet1/22 undecided
```

The command displays a maximum of the top five sessions that each use 2% or more of the packet buffer.

To restrict the display output:

- On a PA-7000 Series platform, you can limit output to a slot, a dataplane, or both. For example:

```
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1
admin@PA-7050> show running resource-monitor ingress-backlogs slot s1 dp dp1
```

- On a PA-5000 Series platform, you can limit output to a dataplane. For example:

```
admin@PA-5060> show running resource-monitor ingress-backlogs dp dp1
```

View Firewall Resource Usage, Top Sessions, and Session Details (Continued)

Step 2 Use the command output to determine whether the source at the source IP address using a high percentage of the packet buffer is sending legitimate or attack traffic.

In the sample output above, a single-session attack is likely occurring. A single session (Session ID 6) is using 92% of the packet buffer for Slot 1, DP 1, and the application at that point is `undecided`.

- If you determine a single user is sending an attack and the traffic is not offloaded, you can Use the CLI to End a Single Attacking Session. At a minimum, you can Configure DoS Protection Against Flooding of New Sessions.
- On a hardware platform that has a field-programmable gate array (FPGA), the firewall offloads traffic to the FPGA when possible to increase performance. However, if the traffic is offloaded to hardware, clearing the session does not help because then the software must handle the barrage of packets. You should instead Discard a Session Without a Commit.

To see whether a session is offloaded or not, use the `show session id <session-id>` operational command in the CLI as shown in the following example. The `layer7 processing value` indicates `completed` for sessions offloaded or `enabled` for sessions not offloaded.

```
admin@PA-5060> show session id 68088184

Session        68088184

        c2s flow:
                source:      1.1.42.15 [trust]
                dst:         1.2.27.99
                proto:       6
                sport:       55993           dport:      6881
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        s2c flow:
                source:      1.2.27.99 [untrust]
                dst:         1.1.42.15
                proto:       6
                sport:       6881            dport:      55993
                state:       ACTIVE          type:       FLOW
                src user:    unknown
                dst user:    unknown
                offload:     Yes

        DP                                   : 2
        index(local):                        : 979320
        start time                           : Tue Oct 27 14:20:09 2015
        timeout                              : 1200 sec
        time to live                         : 1167 sec
        total byte count(c2s)                : 270
        total byte count(s2c)                : 270
        layer7 packet count(c2s)             : 3
        layer7 packet count(s2c)             : 3
        vsys                                 : vsys1
        application                          : bittorrent
        rule                                 : rule1
        session to be logged at end          : True
        session in session ager              : True
        session updated by HA peer           : False
        layer7 processing                    : completed
        URL filtering enabled                : False
        session via syn-cookies              : False
        session terminated on host           : False
        session traverses tunnel             : False
        captive portal session               : False
        ingress interface                    : ethernet1/21
        egress interface                     : ethernet1/22
        session QoS rule                     : N/A (class 4)
        tracker stage l7proc                 : ctd decoder bypass
        end-reason                           : unknown
```


Discard a Session Without a Commit

Perform this task to permanently discard a session, such as a session that is overloading the packet buffer. No commit is required; the session is discarded immediately after executing the command. The commands apply to both offloaded and non-offloaded sessions.

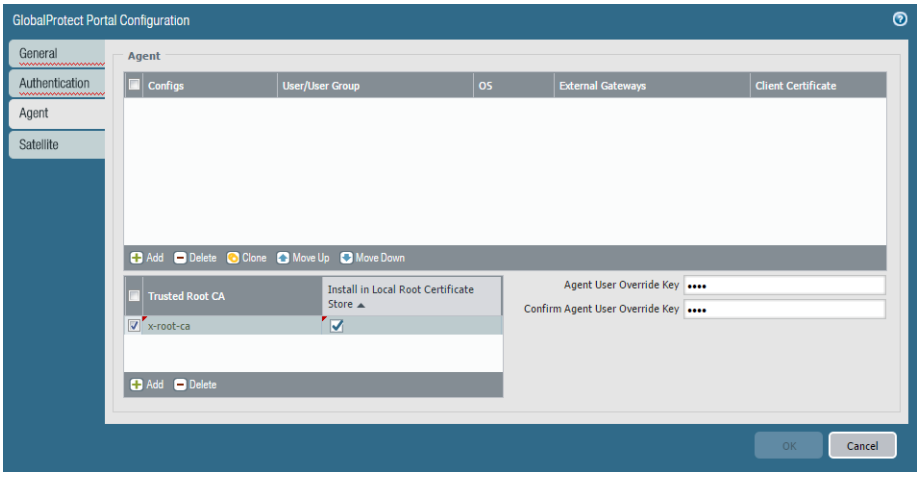
Discard a Session Without a Commit	
Step 1	In the CLI, execute the following operational command on any hardware platform. `admin@PA-7050>` **request session-discard [timeout <seconds>] [reason <reason-string>] id <session-id>**
Step 2	Verify that sessions that have been discarded. `admin@PA-7050>` **show session all filter state discard**

Decryption Features

- Transparent Certificate Distribution for SSL Forward Proxy
- Perfect Forward Secrecy (PFS) Support

Transparent Certificate Distribution for SSL Forward Proxy

You can now easily and transparently install the trusted root certificate authority (CA) certificates that are required for SSL Forward Proxy decryption by enabling a new option in a GlobalProtect portal agent configuration for each certificate.



This enables the GlobalProtect portal to automatically distribute the certificate and install it in the certificate store on Windows and Mac endpoints. The firewall uses these certificates to establish itself as a trusted third party to the session between the client and the server.

Use GlobalProtect to Distribute Certificates for SSL Forward Proxy Decryption

Step 1 **Before You Begin:**

- ❑ Get started with GlobalProtect.
- ❑ Configure the forward trust certificate (could be a self-signed certificate or an enterprise CA-signed certificate) for use with SSL Forward Proxy decryption.

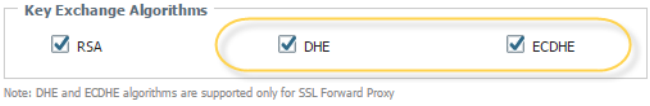
Step 2	Select **Network** > **GlobalProtect** > **Portals** and then select an existing portal configuration or **Add** a new one.
Step 3	Select **Agent** and then select an existing agent configuration or **Add** a new one.
Step 4	If it doesn't already exist, **Add** the SSL Forward Proxy forward trust certificate to the Trusted Root CA section.
Step 5	**Install in Local Root Certificate Store** so that the GlobalProtect portal automatically distributes the certificate and installs it in the certificate store on GlobalProtect client systems.
Step 6	Click **OK** twice.
Step 7	Ensure that you complete all steps to enable SSL Forward Proxy decryption, including setting up a decryption policy rule to define traffic the firewall decrypts.
Step 8	**Commit** your changes.

Perfect Forward Secrecy (PFS) Support

The firewall now supports Perfect Forward Secrecy (PFS) for SSL Forward Proxy decrypted sessions. PFS is a secure communication protocol that prevents the compromise of one encrypted session from leading to the compromise of multiple encrypted sessions. With PFS, a server generates unique private keys for each secure session that it establishes with a client. If a server private key is compromised, only the single session established with that key is vulnerable—an attacker cannot retrieve data from past and future sessions because the server establishes each connection with a uniquely generated key.

In releases prior to PAN-OS 7.1, the firewall did not decrypt SSL sessions established using PFS key exchange algorithms. Depending on your security policy, the firewall either blocked these SSL sessions without decrypting them or decrypted the SSL sessions without maintaining PFS. Now, for SSL sessions established with PFS key exchange algorithms, the firewall both decrypts the SSL session and preserves PFS protection for both past and future sessions.

Decryption support for ephemeral Diffie-Hellman (DHE)-based PFS and elliptic curve Diffie-Hellman (ECDHE)-based PFS is enabled by default when you upgrade a firewall to PAN-OS 7.1 for sessions decrypted with the SSL Forward Proxy decryption method. You can disable support for these PFS key exchange algorithms by modifying the firewall decryption profile you apply to SSL Forward Proxy decrypted traffic.

Modify PFS Support for Decrypted SSL Traffic		
Step 1	**Before You Begin:** If the firewall is not already configured to decrypt SSL traffic from internal clients to the web, start by configuring SSL Forward Proxy decryption.	
Step 2	(New) Enable or disable support to safely decrypt SSL sessions with Perfect Forward Secrecy (PFS).	1. Select **Objects** > **Decryption Profile** and **Add** or modify an existing decryption rule. 2. Select **SSL Decryption** > **SSL Protocol Settings**. 3. (New Settings) Modify support to decrypt SSL sessions established using the **DHE** and **ECDHE** key exchange algorithms as needed:  4. Click **OK**. After an upgrade to PAN-OS 7.1, both the **DHE** and **ECDHE** options are selected by default.

Modify PFS Support for Decrypted SSL Traffic (Continued)	
Step 3 Apply the updated PFS settings to decrypted traffic.	**Verify that the updated decryption profile rule is attached to an existing decryption policy rule:** Select **Decryption** > **Policies** and scan the Decryption Profile column for the policy rule. Check the Type column to make sure that the decryption profile rule with the updated PFS settings is attached to an SSL Forward Proxy policy rule. **Add the updated decryption profile rule to a decryption policy rule:** 1. Select **Policies** > **Decryption**. 2. **Add** or modify an existing policy as needed. 3. Select **Options** and set the policy rule action to **Decrypt** and the policy rule type to **SSL Forward Proxy**. 4. From the **Decryption Profile** drop-down, select the updated profile rule with the modified PFS settings. 5. Click **OK** and **Commit**.

VPN Features

- DES Support for Crypto Profiles

DES Support for Crypto Profiles

To provide backward compatibility with legacy devices that do not use stronger encryption methods, IKE gateways and IPSec tunnels on the firewall now support Data Encryption Standard (DES) as an encryption algorithm in crypto profiles for site-to-site VPN connections.

During tunnel negotiation, the firewall negotiates with the peer at the opposite end of the tunnel and uses the first encryption algorithm that both peers support based on the encryption list each peer has in its profile.

Palo Alto Networks does not recommend DES encryption; instead, we recommend using a stronger encryption algorithm, such as 3DES or Advanced Encryption Standard (AES) if the peer can support it. You should list the algorithms from strongest to weakest so that the firewall matches the strongest possible encryption algorithm first.

Configure DES only if the legacy devices in your network cannot support a stronger encryption type.

Configure DES for an IKE Gateway and IPSec Tunnel Profile for Site-to-Site VPN	
• Configure DES for an IKE gateway.	1. Select **Network** > **Network Profiles** > **IKE Crypto** and select a crypto profile. 2. For **Encryption**, **Add** the **des** encryption option from the drop-down. After an upgrade to PAN-OS 7.1, both the **DHE** and **ECDHE** options are selected by default.  (Not recommended) **Move Up** the **des** encryption type to the top of the list only if you want the firewall to negotiate DES over other, stronger encryption algorithms. 3. Click **OK**. 4. See Define Cryptographic Profiles to configure the remainder of the profile. 5. See Step 7 of Set Up an IKE Gateway to apply the profile to an IKE gateway.

Configure DES for an IKE Gateway and IPSec Tunnel Profile for Site-to-Site VPN (Continued)	
• Configure DES for an IPSec tunnel.	Perform one of the following tasks, depending on whether you want to configure DES using an IPSec tunnel profile or using a manual key: **Configure DES Using an IPSec Tunnel Profile** 1. Select **Network** > **Network Profiles** > **IPSec Crypto** and select a crypto profile. 2. For **Encryption**, **Add** the **des** encryption option from the drop-down. If there are other encryption types in the profile, select **des** and **Move Up** the selection to the top of the list.  (Not recommended) **Move Up** the **des** type to the top of the list only if you want the firewall to negotiate DES over other, stronger encryption algorithms. 3. Click **OK**. 4. See Define IPSec Crypto Profiles to configure the remainder of the profile. 5. See Step 4 in Set Up an IPSec Tunnel to apply the profile to an IPSec tunnel. **Configure DES Using a Manual Key** 1. Select **Network** > **IPSec Tunnels** and select a tunnel. 2. On the **General** tab, select **Manual Key**. 3. For **Encryption**, select **des**. 4. Click **OK**.
• Save the configuration.	Click **Commit**.

Panorama Features

- Role Privileges for Commit Types
- Increased (8TB) Disk Support on the Panorama Virtual Appliance

Role Privileges for Commit Types

For custom Panorama administrator roles, you can now assign commit privileges by type (Panorama, device group, template, or Collector Group) instead of assigning one comprehensive commit privilege. This improves the security of Panorama, firewalls, and Log Collectors by providing more granular control over the types of configuration changes that each Panorama administrator can commit.

Assign Commit Privileges to a Panorama Administrator		
Step 1	Configure the Admin Role profile with granular commit privileges.	1. Select **Panorama** > **Admin Roles** and **Add** a new profile. 2. Enter a **Name** for the profile and set the **Role** type to **Panorama**. 3. In the **Web UI** tab, enable the appropriate **Commit** permissions. This example shows how to create a custom Panorama role that can commit changes to Panorama, device group, and template settings but not to Collector Groups settings. a. Enable the **Commit** permissions for **Panorama**, **Device Groups**, **Templates**, and **Force Template Values** (all are enabled by default). The **Force Template Values** permission enables administrators to replace overridden settings in local firewall configurations with template settings. b. Disable the **Commit** permission for **Collector Groups**. 4. Click **OK**.
Step 2	Configure the administrator account to use the new Admin Role profile.	1. Select **Panorama** > **Administrators** and **Add** a new administrator. 2. Enter a user **Name** for the administrator. 3. Select the authentication type. This example uses local authentication but you can also use an external server for authentication. a. Set the **Authentication Profile** to **None**. b. Enter and confirm a **Password**. 4. Set the **Administrator Type** to **Custom Panorama Admin**. 5. Select the Admin Role **Profile** you just created. 6. Click **OK** and **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again.

Assign Commit Privileges to a Panorama Administrator (Continued)		
Step 3	Verify that the administrator you added can commit changes to Panorama, device group, and template settings but cannot commit changes to Collector Group settings.	1. Log in to Panorama as the administrator you just added. 2. Verify that you can commit changes to a Panorama, device group, and template setting. For example: a. Select **Panorama** > **Setup** > **Management** and edit General Settings. b. Modify the **Login Banner** text and click **OK**. c. Click **Commit**, set the **Commit Type** to **Panorama**, and click **Commit** again. 3. Verify that you cannot commit changes to a Collector Group setting. For example: a. Select **Panorama** > **Collector Groups** and **Add** a Collector Group. b. Enter a **Name** for the Collector Group and click **OK**. c. Click **Commit**. For the **Commit Type**, the **Collector Group** option should not appear.

Increased (8TB) Disk Support on the Panorama Virtual Appliance

You can now add a virtual disk of up to 8TB on a Panorama virtual appliance that runs on a VMware ESXi server (version 5.5 or later) or on vCloud Air. This increased disk capacity (maximum was previously 2TB) enables Panorama to store more logs.

If you replace an existing virtual disk of up to 2TB storage capacity with a disk of up to 8TB, you will lose the logs on the existing disk. To preserve the logs, you can set up a new Panorama virtual appliance for the new disk and maintain access to the Panorama containing the old disk for as long as you need its logs. Alternatively, you can copy logs from the old disk to the new disk. Copying can take several hours, depending on how many logs the disk currently stores, and Panorama cannot collect logs during the copy process. Contact Palo Alto Networks Customer Support for instructions to copy logs.

Add a Virtual Disk to Panorama	
• Add a Virtual Disk to Panorama on an ESXi Server.	Access the VMware vSphere Client, power off the Panorama virtual appliance, configure a new virtual disk with the following settings, and then power on the Panorama virtual appliance. • **Disk Size**—Up to 8TB • **Disk Provisioning**—**Thick Provision Lazy Zeroed** • **Location**—**Store with the virtual machine** • **Virtual Device Node**—The selected node must be in SCSI format; otherwise, Panorama will fail to boot.
• Add a Virtual Disk to Panorama on vCloud Air.	Access the vCloud Air web console, select your Panorama virtual appliance, select **Actions** > **Edit Resources**, **Add another disk**, and set the **Storage** (up to 8TB).