

Palo Alto Networks Compatibility Matrix

Contact Information

Corporate Headquarters:

Palo Alto Networks

3000 Tannery Way

Santa Clara, CA 95054

www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2016-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

July 7, 2023

Table of Contents

Supported OS Releases by Model.....	9
Palo Alto Networks Next-Generation Firewalls.....	10
Palo Alto Networks Appliances.....	13
WildFire Appliance Analysis Environment Support.....	14
Palo Alto Networks PA-7000 Series Cards.....	16
Palo Alto Networks PA-5450 Cards.....	18
HA Port and Processor Support.....	19
VM-Series Firewalls.....	25
VM-Series Firewall Hypervisor Support.....	26
Private Cloud Deployments.....	26
Public Cloud Deployments.....	33
VM-Series Firewall for VMware Cloud on AWS.....	34
PacketMMAP and DPDK Drivers on VM-Series Firewalls.....	35
SR-IOV Access Mode.....	35
PacketMMAP Driver Versions.....	35
DPDK Driver Versions.....	37
Partner Interoperability for VM-Series Firewalls.....	38
Palo Alto Networks Certified Integrations.....	38
Partner-Qualified Integrations.....	44
VM-Series Plugin.....	48
VM-Series Plugin 4.0.x.....	48
VM-Series Plugin 3.0.x.....	48
VM-Series Plugin 2.1.x.....	49
VM-Series Plugin 2.0.x.....	50
VM-Series Plugin 1.0.x.....	51
AWS Regions.....	54
Azure Regions.....	56
Google Cloud Regions.....	57
Alibaba Cloud Regions.....	58
VM-Series Firewall Amazon Machine Images (AMI).....	59
PAN-OS Images for AWS GovCloud.....	59
CN-Series Firewalls.....	61
CN-Series Supported Environments.....	62
CN-Series Firewall Image and File Compatibility.....	67
Panorama.....	69
Panorama Plugins.....	70

Cisco ACI.....	70
Cisco TrustSec.....	74
Panorama CloudConnector Plugin (Formerly, AIOps Plugin for Panorama).....	76
Cloud Services.....	77
Enterprise Data Loss Prevention (DLP).....	77
Panorama Interconnect.....	80
IPS Signature Converter.....	81
Kubernetes.....	83
Clustering Plugin.....	84
Nutanix.....	85
OpenConfig (Firewall Only).....	85
Panorama Software Firewall License Plugin.....	86
Public Cloud—AWS, Azure, and GCP.....	87
SD-WAN.....	92
VMware NSX.....	96
VMware vCenter.....	100
Zero Touch Provisioning (ZTP).....	101
Compatible Plugin Versions for PAN-OS 10.2.....	103
Panorama Management Compatibility.....	108
Panorama Hypervisor Support.....	110
Device Certificate for a Palo Alto Networks Cloud Service.....	113
MFA Vendor Support.....	115
MFA Vendor Support.....	116
Supported Cipher Suites.....	117
Cloud Identity Engine Cipher Suites.....	118
Cipher Suites Supported in PAN-OS 11.0.....	119
PAN-OS 11.0 GlobalProtect Cipher Suites.....	119
PAN-OS 11.0 IPSec Cipher Suites.....	121
PAN-OS 11.0 IKE and Web Certificate Cipher Suites.....	122
PAN-OS 11.0 Decryption Cipher Suites.....	124
PAN-OS 11.0 Administrative Session Cipher Suites.....	126
PAN-OS 11.0 HA1 SSH Cipher Suites.....	128
PAN-OS 11.0 PAN-OS-to-Panorama Connection Cipher Suites.....	128
PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode.....	129
Cipher Suites Supported in PAN-OS 10.2.....	132
PAN-OS 10.2 GlobalProtect Cipher Suites.....	132
PAN-OS 10.2 IPSec Cipher Suites.....	134
PAN-OS 10.2 IKE and Web Certificate Cipher Suites.....	135

PAN-OS 10.2 Decryption Cipher Suites.....	137
PAN-OS 10.2 Administrative Session Cipher Suites.....	139
PAN-OS 10.2 HA1 SSH Cipher Suites.....	141
PAN-OS 10.2 PAN-OS-to-Panorama Connection Cipher Suites.....	141
PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode.....	142
Cipher Suites Supported in PAN-OS 10.1.....	145
PAN-OS 10.1 GlobalProtect Cipher Suites.....	145
PAN-OS 10.1 IPSec Cipher Suites.....	147
PAN-OS 10.1 IKE and Web Certificate Cipher Suites.....	148
PAN-OS 10.1 Decryption Cipher Suites.....	149
PAN-OS 10.1 Administrative Session Cipher Suites.....	152
PAN-OS 10.1 HA1 SSH Cipher Suites.....	153
PAN-OS 10.1 PAN-OS-to-Panorama Connection Cipher Suites.....	154
PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode.....	154
Cipher Suites Supported in PAN-OS 9.1.....	158
PAN-OS 9.1 GlobalProtect Cipher Suites.....	158
PAN-OS 9.1 IPSec Cipher Suites.....	160
PAN-OS 9.1 IKE and Web Certificate Cipher Suites.....	161
PAN-OS 9.1 Decryption Cipher Suites.....	162
PAN-OS 9.1 Administrative Session Cipher Suites.....	164
PAN-OS 9.1 HA1 SSH Cipher Suites.....	166
PAN-OS 9.1 PAN-OS-to-Panorama Connection Cipher Suites.....	167
PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode.....	167
Cipher Suites Supported in PAN-OS 8.1.....	170
PAN-OS 8.1 GlobalProtect Cipher Suites.....	170
PAN-OS 8.1 IPSec Cipher Suites.....	172
PAN-OS 8.1 IKE and Web Certificate Cipher Suites.....	173
PAN-OS 8.1 Decryption Cipher Suites.....	174
PAN-OS 8.1 Administrative Session Cipher Suites.....	176
PAN-OS 8.1 HA1 SSH Cipher Suites.....	178
PAN-OS 8.1 PAN-OS-to-Panorama Connection Cipher Suites.....	179
PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode.....	179

GlobalProtect..... 183

Where Can I Install the GlobalProtect App?.....	184
Apple macOS.....	184
Microsoft Windows.....	185
Linux.....	186
Apple iOS and iPadOS.....	190
Google Android.....	191
Google Chrome.....	192

Internet of Things (IoT).....	193
Hypervisors.....	193
Third-Party VPN Client Support.....	194
What Third-Party VPN Clients are Supported?.....	194
What GlobalProtect Features Do Third-Party Clients Support?.....	194
How Many Third-Party Clients Does Each Firewall Model Support?.....	195
What Features Does GlobalProtect Support?.....	198
What Features Does GlobalProtect Support for IoT?.....	210
What GlobalProtect Features Do Third-Party Mobile Device Management Systems Support?.....	213
Prisma Access.....	215
What Features Does Prisma Access Support?.....	216
Prisma Access Feature Support.....	216
Management.....	217
Remote Networks.....	218
Service Connections.....	219
Mobile Users—GlobalProtect.....	220
Mobile Users—Explicit Proxy.....	222
Security Services.....	222
Network Services.....	224
Identity Services.....	226
Policy Objects.....	228
Logs.....	231
Reports.....	231
Integration with Other Palo Alto Networks Products.....	233
Multitenancy Unsupported Features and Functionality.....	233
Prisma Access and Panorama Version Compatibility.....	235
Minimum Required Panorama Software Versions.....	235
End-of-Support (EoS) Dates for Panorama Software Version Compatibility with Prisma Access.....	238
Supported IKE Cryptographic Parameters.....	240
User-ID Agent.....	243
Where Can I Install the User-ID Agent?.....	244
Which Servers Can the User-ID Agent Monitor?.....	245
Where Can I Install the User-ID Credential Service?.....	247
Terminal Server (TS) Agent.....	249
Where Can I Install the Terminal Server (TS) Agent?.....	250
How Many TS Agents Does My Firewall Support?.....	251

Cortex Data Lake.....	253
Cortex Data Lake Software Compatibility.....	254
Cortex XDR.....	257
Where Can I Install the Cortex XDR Agent?.....	258
Cortex XDR Supported Kernel Module Versions by Distribution.....	259
Cortex XDR and Traps Compatibility with Third-Party Security Products.....	260
Endpoint Security Manager (ESM).....	261
Where Can I Install the Endpoint Security Manager (ESM)?.....	262
Where Can I Install the Cortex XDR Agent?.....	263
IPv6 Support by Feature.....	265
IPv6 Support by Feature.....	266
Mobile Network Infrastructure Feature Support.....	271
PAN-OS Releases by Model that Support GTP, SCTP, and 5G Security.....	272
3GPP Technical Standard References.....	273
3GPP TS References for GTP Security.....	273
3GPP TS References for 5G Security.....	273
3GPP TS References for 5G Multi-Edge Security.....	274
3GPP TS References for UE-to-IP Address Correlation with PFCP in 4G.....	274

Supported OS Releases by Model

Use the tables throughout this Palo Alto Networks Compatibility Matrix to determine support for Palo Alto Networks Next-Generation Firewalls, appliances, and agents. Additionally, refer to the [product comparison tool](#) for detailed information about Palo Alto Networks firewalls by model, including specifications for throughput, maximum number of sessions, rules, objects, tunnels, and zones.

For supported operating systems on firewalls and appliances and for high-availability (HA) port and processor support on firewalls, review the following topics:

- [Palo Alto Networks Next-Generation Firewalls](#)
- [Palo Alto Networks Appliances](#)
- [WildFire Appliance Analysis Environment Support](#)
- [Palo Alto Networks PA-7000 Series Firewall Cards](#)
- [HA Port and Processor Support](#)

Palo Alto Networks Next-Generation Firewalls

The following table shows the PAN-OS® releases supported for each of the Palo Alto Networks Next-Generation Firewall [hardware](#), and [VM-Series](#), and [CN-Series](#) models. You can also review PAN-OS support for [PA-7000 Series cards](#) and [PA-5450 firewall cards](#) as well as for [Palo Alto Networks appliances](#).

Palo Alto Networks Firewall Model	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.0**	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Hardware Firewalls						
PA-200 Firewall (EoS***)	✓	—	—	—	—	—
PA-220 Firewall	—	✓	✓	✓	✓	—
PA-220R Firewall	—	✓	✓	✓	✓	—
PA-410 Firewall	—	—	—	✓ 10.1.2 & later	✓	✓
PA-415 and PA-445 Firewalls	—	—	—	—	—	✓
PA-440, PA-450, and PA-460 Firewalls	—	—	—	✓	✓	✓
PA-500 Firewall (EoS***)	✓	—	—	—	—	—
PA-800 Series Firewalls	—	✓	✓	✓	✓	✓
PA-1400 Series Firewalls	—	—	—	—	—	✓
PA-3000 Series Firewalls (EoS***)	—	✓	—	—	—	—
PA-3200 Series Firewalls	—	✓	✓	✓	✓	✓

Palo Alto Networks Firewall Model	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.0**	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
PA-3400 Series Firewalls	—	—	—	—	✓	✓
PA-5000 Series Firewalls (EoS***)	✓	—	—	—	—	—
PA-5200 Series Firewalls	—	✓	✓	✓	✓	✓
PA-5410, PA-5420, and PA-5430 Firewalls	—	—	—	—	✓	✓
PA-5440 Firewalls	—	—	—	—	—	✓
PA-5450 Firewall	—	—	—	✓	✓	✓
PA-7000 Series Firewalls (**)	—	✓	✓**	✓	✓	✓

VM-Series Firewalls

Flexible vCPU Firewalls (Up to 32 cores)	—	—	—	✓	✓	✓
Flexible vCPU Firewalls (Up to 64 cores)	—	—	—	—	✓	✓
VM-50 Firewall	—	✓	—	✓	✓	✓
VM-100 Firewall	—	✓	—	✓	✓	✓
VM-200 Firewall	—	✓	—	✓	✓	✓
VM-300 Firewall	—	✓	—	✓	✓	✓
VM-500 Firewall	—	✓	—	✓	✓	✓
VM-700 Firewall	—	✓	—	✓	✓	✓
VM-1000-HV Firewall	—	✓	—	✓	✓	✓

Palo Alto Networks Firewall Model	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.0**	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
CN-Series Firewall						
CN-Series Small CN-MGMT Mem: 2GB CN-NGFW Mem: 2 to 2.5GB	—	—	—	✓	✓	✓
CN-Series Medium CN-MGMT Mem: 2GB CN-NGFW Mem: 6GB	—	—	—	✓	✓	✓
CN-Series Large CN-MGMT Mem: 4GB CN-NGFW Mem: 48GB	—	—	—	✓	✓	✓

* PAN-OS 8.1 is supported only on PA-200, PA-500, and PA-5000 Series firewalls (and the M-100 appliance) and only until each reaches its [hardware end-of-life \(EoL\) date](#).

** PAN-OS 10.0 releases are supported only for two PA-7000 cards (PA-7000-20G-NPC and PA-7000-20GQ-NPC) in PA-7000 Series firewall after July 16, 2022, and will be supported until the [hardware EoL](#) for these cards on January 31, 2024.

*** You should also review the [hardware EoL information](#) for more specific information about firewalls and appliances that have reached end-of-sale (EoS) status.

Palo Alto Networks Appliances

The following table shows PAN-OS® release support for each Palo Alto Networks (non-firewall) appliance. You can also review [PAN-OS release support for Palo Alto Networks Next-Generation Firewalls](#).

Palo Alto Networks Appliance	Release 6.2	Release 8.1*	Release 9.1**	Release 10.1	Release 10.2	Release 11.0
GP-100 Appliance (EoS***)	✓	—	—	—	—	—
Panorama Virtual Appliance	—	—	✓	✓	✓	✓
M-100 Appliance (EoS***)	—	✓	✓**	—	—	—
M-200 Appliance	—	—	✓	✓	✓	✓
M-300 Appliance	—	—	—	—	✓	✓
M-500 Appliance (EoS***)	—	—	✓	✓	—	—
M-600 Appliance	—	—	✓	✓	✓	✓
M-700 Appliance	—	—	—	—	✓	✓
WF-500 Appliance(****)	—	—	✓	✓	✓ 10.2.2 & later	✓
WF-500-B Appliance(****)	—	—	—	—	✓ 10.2.2 & later	✓

* PAN-OS 8.1 is supported only on the M-100 appliance (and PA-200, PA-500, and PA-5000 Series firewalls) and only until each reaches its [hardware end-of-life \(EoL\) date](#).

** PAN-OS 9.1 releases support M-100 appliances only after you [upgrade the M-100 appliance to 32GB of memory](#) (from the default of 16GB).

*** For more specific information about firewalls and appliances that have reached end-of-sale (EoS) status, review our [hardware EoL web page](#).


**** WildFire appliances have optional guest VM images that provides support for additional analysis environments. For information about which VMs are available for a specific WildFire releases, refer to [WildFire Appliance Analysis Environment Support](#).

WildFire Appliance Analysis Environment Support

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



Verify that you download and install the correct WildFire VM image for your WildFire appliance. Installing a WildFire VM image that is not supported by the WildFire (PAN-OS) release running on your appliance will produce error messages and will be unable to process samples or detect malware.

WildFire Analysis Environment	WildFire VM ID	WildFire Appliance Guest VM Filename	Minimum Compatible PAN-OS Version
Windows XP (Adobe Reader 11, Flash 11, Office 2010)	vm-3	WFWinXpAddon3_m-1.0.1.xpaddon3	10.2.2 and later
		WFWinXpAddon3_m-1.0.0.xpaddon3*	10.1 and earlier
Windows 7 x64 SP1 (Adobe Reader 11, Flash 11, Office 2010)	vm-5	WFWin7_64Addon1_m-1.0.1.7_64addon1	10.2.2 and later
		WFWin7_64Addon1_m-1.0.0.7_64addon1	10.1 and earlier
		WFWin7_64Base_m-1.0.0.7_64base  <i>This is a required base VM image package for the proper function of the Windows 7 analysis environment.</i>	10.1 and earlier
Windows XP (Internet Explorer 8, Flash 11, Elink analysis support)	vm-6**	WFWinXpGf_m-1.0.0.xpgf	10.1 and earlier
		WFWinXpGf_m-1.0.1.xpgf	10.2.2 and later
Windows 10 x64 (Adobe Reader 11, Flash 11, Office 2010)	vm-7	WFWin10Base_m-1.0.1.10base	10.2.2 and later

WildFire Analysis Environment	WildFire VM ID	WildFire Appliance Guest VM Filename	Minimum Compatible PAN-OS Version
		WFWin10Base_m-1.0.0-c2.10base	10.1 and earlier



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

Palo Alto Networks PA-7000 Series Cards

The following table shows the PAN-OS® releases supported for each of the [system cards](#) and for each of the [networking and data plane cards](#) supported on PA-7000 Series firewalls. You can also review PAN-OS support for each [Palo Alto Networks Next-Generation Firewall](#) and for [all other Palo Alto Networks appliances](#).

PA-7000 Series Firewall Cards	PAN-OS 9.1	PAN-OS 10.0	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Networking and Data Plane Cards					
PAN-PA-7000-20G-NPC	✓	✓* (*until Jan. 31, 2024)	—	—	—
PAN-PA-7000-20GQ-NPC	✓	✓* (*until Jan. 31, 2024)	—	—	—
PAN-PA-7000-20GXM-NPC	✓	✓	✓	—	—
PAN-PA-7000-20GQXM-NPC	✓	✓	✓	—	—
PAN-PA-7000-100G-NPC-A	✓	✓	✓	✓	✓
PAN-PA-7000-DPC-A	—	✓	✓	✓	✓
System Cards					
PAN-PA-7050-SMC	✓	✓	✓* (*until Feb. 28, 2026)	—	—
PAN-PA-7050-SMC (v2)	✓	✓	✓* (*until Feb. 28, 2026)	—	—
PAN-PA-7050-SMC-B	✓	✓	✓	✓	✓
PAN-PA-7080-SMC	✓	✓	✓*	—	—

PA-7000 Series Firewall Cards	PAN-OS 9.1	PAN-OS 10.0	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
			(*until Feb. 28, 2026)		
PAN-PA-7080-SMC (v2)	✓	✓	✓* (*until Feb. 28, 2026)	—	—
PAN-PA-7080-SMC-B	✓	✓	✓	✓	✓
PAN-PA-7000-LPC	✓	✓	✓* (*until Feb. 28, 2026)	—	—
PAN-PA-7000-LFC-A	✓	✓	✓	✓	✓

Palo Alto Networks PA-5450 Cards

The following table shows the PAN-OS® releases supported for each of the system, network, and data processing cards available for the PA-5450 firewall. You can also review PAN-OS support for each [Palo Alto Networks Next-Generation Firewall](#), each of our other [Palo Alto Networks appliances](#), and for the [data processing cards available for the PA-7000 Series firewalls](#).

PA-5450 Firewall Cards	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
------------------------	-------------	-------------	-------------

Networking and Data Processing Cards

PAN-PA-5400-NC-A	✓	✓	✓
PAN-PA-5400-DPC-A	✓	✓	✓

System Cards

PAN-PA-5400-BC-A	✓	✓	✓
PAN-PA-5400-MPC-A	✓	✓	✓

HA Port and Processor Support

The following table identifies which Palo Alto Networks Next-Generation Firewall (NGFW) can support the HA ports and processor functionality you require in your network.

Additionally, some firewall models and PA-7000 Series firewall cards include an offload processor—a Content Engine (CE) for accelerating signature matches or a Crypto Accelerator (CA) for accelerating SSL processing; some firewalls support either one but none can support both simultaneously.

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
-----------------------------------	-------------------------------	-------------------	-------------------	------------------------	----------	----------	-----------

Firewalls

PA-200 (EoS)*	—	—	—	—	—	—	—
PA-220	—	—	—	—	—	—	—
PA-220R	—	—	—	—	—	—	—
PA-410	—	—	—	—	—	—	—
PA-415	—	—	—	—	—	—	—
PA-440	—	—	—	—	—	—	—
PA-445	—	—	—	—	—	—	—
PA-450	—	—	—	—	—	—	—
PA-460	—	—	—	—	—	—	—
PA-500 (EoS)*	√	—	—	—	—	—	—
PA-820	—	—	—	—	√	√	—
PA-850	—	—	—	—	√	√	—
PA-1410	—	—	—	—	√ (x2)	—	√

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
PA-1420	—	—	—	—	√ (x2)	—	√
PA-3020 (EoS)	√	—	√ (CE)	—	√	√	—
PA-3050 (EoS)	√	√	√ (CE)	—	√	√	—
PA-3060 (EoS)	√	√	√ (CE)	—	√	√	—
PA-3220	√	√	—	—	√ (x2)	—	√
PA-3250	√	√	√ (CE)	—	√ (x2)	—	√
PA-3260	√	√	√ (CE)	—	√ (x2)	—	√
PA-3410	√	√	—	—	√ (x2)	—	√
PA-3420	√	√	—	—	√ (x2)	—	√
PA-3430	√	√	—	—	√ (x2)	—	√
PA-3440	√	√	—	—	√ (x2)	—	√
PA-5020 (EoS)*	√	√	√ (CE)	—	√	√	—
PA-5050	√	√	√	—	√	√	—

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
(EoS)*			(CE)				
PA-5060 (EoS)*	✓	✓	✓ (CE)	—	✓	✓	—
PA-5220	✓	✓	✓ (CE or CA)	✓	✓ (x2)	—	✓
PA-5250	✓	✓	✓ (CE or CA)	✓	✓ (x2)	—	✓
PA-5260	✓	✓	✓ (CE or CA)	✓	✓ (x2)	—	✓
PA-5280	✓	✓	✓ (CE or CA)	✓	✓ (x2)	—	✓
PA-5410	—	—	—	—	✓ (x2)	—	✓
PA-5420	—	—	—	—	✓ (x2)	—	✓
PA-5430	—	—	—	—	✓ (x2)	—	✓
PA-5440	—	—	—	—	✓ (x2)	—	✓
PA-5450	✓	✓	✓ (CE or CA)	✓	✓ (x2)	—	✓ (x2)
PA-7050	✓	✓	✓	✓	✓	—	✓

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
			(CE or CA)		(x2)		(x2)
PA-7080	✓	✓	✓ (CE or CA)	✓	✓ (x2)	—	✓ (x2)

PA-7000 Series Firewall Cards

PA-7050-SMC (EoS)	✓	—	—	✓	✓ (x2)	—	✓ (x2)
PA-7080-SMC (EoS)	✓	—	—	✓	✓ (x2)	—	✓ (x2)
PA-7050-SMC-B	✓	—	—	✓	✓ (x2)	—	✓ (x2)
PA-7080-SMC-B	✓	—	—	✓	✓ (x2)	—	✓ (x2)
PA-7000-20G-NPC (EoS)	—	✓	✓ (CE x2)	—	—	—	—
PA-7000-20GQ-NPC (EoS)	—	✓	✓ (CE x2)	—	—	—	—
PA-7000-20GXM-NPC (EoS)	—	✓	✓ (CE x2)	—	—	—	—
PA-7000-20GQXM-NPC (EoS)	—	✓	✓ (CE x2)	—	—	—	—
PA-7000-100G-NPC-A	—	✓	✓ (CE or CA)	—	—	—	—

Palo Alto Networks Firewall Model	Separate Mgmt Plane Processor	Network Processor	Offload Processor	First Packet Processor	HA1 Port	HA2 Port	HSCI Port
PA-7000-DPC-A	—	—	√ (CA x2)	—	—	—	—

* These firewalls are supported only on PAN-OS 8.1 and only until each reaches its [hardware end-of-life \(EoL\) date](#). You can also review the [hardware EoL information](#) for more specific information about firewalls and appliances that have reached end-of-sale (EoS) status.

VM-Series Firewalls

The hypervisors and the public cloud regions in which you can deploy the VM-Series firewalls:

- [VM-Series Firewall Hypervisor Support](#)
- [PacketMMAP and DPDK Drivers on VM-Series Firewalls](#)
- [Partner Interoperability for VM-Series Firewalls](#)
- [VM-Series Plugin](#)
- [AWS and AWS Gov Cloud Regions](#)
- [Azure Regions](#)
- [Google Cloud Regions](#)
- [Alibaba Cloud Regions](#)
- [AWS CFT Amazon Machine Images \(AMI\) List](#)



For for the best instance types for optimal VM-Series capacity and performance, see the [VM-Series Capacity & Performance](#) document.

VM-Series Firewall Hypervisor Support

Palo Alto Networks offers hypervisor version support on the VM-Series firewall for both the following deployments:

- [Private Cloud Deployments](#)
- [Public Cloud Deployments](#)

Private Cloud Deployments

The following Private Clouds require a PAN-OS for VM-Series base image from the [Palo Alto Networks Support Portal](#):

- [VM-Series for VMware vSphere Hypervisor \(ESXi\)](#)
- [VM-Series for VMware NSX-V](#)
- [VM-Series for VMware NSX-T](#)
- [VM-Series for KVM](#)
- [VM-Series for Nutanix](#)
- [VM-Series for Hyper-V](#)
- [VM-Series for OpenStack](#)
- [Cisco ACI: Hardware and VM-Series Firewalls in Cisco ACI](#)

In the compatibility matrices below, the PAN-OS Version Support column displays the range of versions and the (**Minimum**) version in parentheses. For example, if the PAN-OS Version column displays **PAN-OS 9.1.x (9.1.3)**, it indicates that the integration supports PAN-OS 9.1 releases beginning with PAN-OS 9.1.3.

Further I/O Enhancement support is detailed in [PacketMMAP and DPDK Drivers on VM-Series Firewalls](#).

VM-Series for VMware vSphere Hypervisor (ESXi)

This ESXi version support list does not include NSX. For NSX, see [VM-Series for VMware NSX-V](#) or [VM-Series for VMware NSX-T](#).

You can download base images from the [Palo Alto Networks Support Portal](#).



Access mode with SR-IOV on VMware ESXi is supported on PAN-OS 9.1.5 and later PAN-OS 9.1 versions and PAN-OS 10.1 and later PAN-OS versions—both with VM-Series plugin 2.0.5 and later

. See [Enable VLAN Access Mode for ESXi](#) for more information.

PAN-OS Version Support (Minimum)	VMware ESXi Version Support	VMware Virtual Machine Hardware Version	I/O Enhancement Support	Base Image
PAN-OS 9.1.x (9.1.0)	6.5, 6.7	vmx-10	SR-IOV, DPDK	PA-VM-ESX-9.1.0.ova
PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0)	6.7, 7.0	vmx-10	SR-IOV, DPDK	PA-VM-ESX-9.1.0.ova PA-VM-ESX-10.1.0.ova
PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	6.7, 7.0, 8.0	vmx-10	SR-IOV, DPDK	PA-VM-ESX-10.2.0.ova PA-VM-ESX-11.0.0.ova

VM-Series for VMware NSX-V

vSphere with VMware NSX is available on all VM-Series firewalls except the VM-50 and VM-700 firewalls.

The vSphere with VMware NSX and Panorama combinations listed here are approved by Palo Alto Networks. For versions of PAN-OS certified by VMware, see the [VMware Compatibility Guide](#).

Panorama 9.1 and later versions require the VMware NSX plugin. For more plugin version information, see [Panorama Plugins for VMware NSX](#).

You can download base images from the [Palo Alto Networks Support Portal](#).

VMware having already announced EoS for NSX-V, Palo Alto Networks will continue to support the VM-Series on NSX-V running PAN-OS 10.0.x, and lesser, managed by Panorama 10.1.x or 10.2.x.

- No VM-Series for VMware NSX-V base images for PAN-OS 10.1.x or 10.2.x will be made available
- You cannot upgrade the VM-Series firewall for NSX-V to 10.1.x or 10.2.x
- Panorama 10.1.x, 10.2.x supports 9.1.x base images until EOL date

See the [Palo Alto Networks End-of-Life Summary](#) for more information about the PAN-OS EoL schedule.

Supported Panorama Versions	PAN-OS Version Support	Panorama Plugin for NSX	VMware NSX-V Manager	vSphere	VMware Virtual Machine Hardware Version	Minimum Base Image	I/O Enhancement Support
<ul style="list-style-type: none"> 9.1.x 10.1.x 	9.1.0 to 9.1.6	3.2.0 to latest 4.0.x	6.4.1 to 6.4.7	<ul style="list-style-type: none"> 6.5 6.7 	vmx-10	PA-VM-NSX-9.1.0.zip	LRO
<ul style="list-style-type: none"> 9.1.x 10.1.x 	9.1.7 to latest 9.1.x	3.2.0 to latest 4.0.x	6.4.8 and later	<ul style="list-style-type: none"> 6.5 6.7 7.0 	vmx-10	PA-VM-NSX-9.1.9.zip	LRO
10.2.x	9.1.0 to 9.1.6	5.0.0 and later	6.4.1 to 6.4.7	<ul style="list-style-type: none"> 6.5 6.7 	vmx-10	PA-VM-NSX-9.1.0.zip	LRO
10.2.x	9.1.7 to latest 9.1.x	5.0.0 and later	6.4.8 and later	<ul style="list-style-type: none"> 6.5 6.7 7.0 	vmx-10	PA-VM-NSX-9.1.9.zip	LRO

VM-Series for VMware NSX-T

You can download base images from the [Palo Alto Networks Support Portal](#).

The VMware NSX-T and Panorama combinations listed here are approved by Palo Alto Networks. For versions of PAN-OS certified by VMware, see the [VMware Compatibility Guide](#).



VMware NSX 4.0.x Service Deployments, for partner Service Virtual Machines (SVM), may experience traffic redirect known issues. Please contact VMware NSX Technical Support for details

Panorama Version Support	Panorama Plugin for NSX	VMware NSX-T Version Support	VMware Virtual Machine Hardware Version	PAN-OS Version Support (Minimum)	Latest Base Image
10.2.x	5.0.0 and later	3.2.x, 4.0.x, 4.1.x	vmx-10	PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.4)	PA-VM-NST-10.2.4-vmwaresigned.zip PA-VM-NST-10.1.9-h1-vmwaresigned.zip

Panorama Version Support	Panorama Plugin for NSX	VMware NSX-T Version Support	VMware Virtual Machine Hardware Version	PAN-OS Version Support (Minimum)	Latest Base Image
10.1.x	3.2.0 to 4.0.x	2.5.x, 3.0.x, 3.1.x, 3.2.x	vmx-10	PAN-OS 10.1.x (10.1.0)	PA-VM-NST-10.1.9-h1-vmwaresigned.zip PA-VM-NST-9.1.9-vmwaresigned.zip
	4.0.x	4.0.x	vmx-10	PAN-OS 10.1.x (10.1.9-h1)	PA-VM-NST-10.1.9-h1-vmwaresigned.zip
9.1.x	3.2.0 to 4.0.x	2.5.x, 3.0.x, 3.1.x	vmx-10	PAN-OS 9.1.x (9.1.0)	PA-VM-NST-9.1.9.zip

VM-Series for KVM

You can download base images from the [Palo Alto Networks Support Portal](#).

PAN-OS Version Support (Minimum)	VM-Series for KVM Version Support (Minimum)	I/O Enhancement Support	PAN-OS for VM-Series KVM Base Images
PAN-OS 9.1.x (9.1.0)	CentOS/Red Hat Enterprise Linux: <ul style="list-style-type: none"> 7.x.x (7.6.x) 8.x.x (8.0.x) 	<ul style="list-style-type: none"> DPDK with SR-IOV DPDK with Virtio 	PA-VM-KVM-9.1.x.qcow2
PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	CentOS/Red Hat Enterprise Linux: <ul style="list-style-type: none"> 7.x.x (7.6.x) 8.x.x (8.0.x) 9.0.x (9.0.x) 	<ul style="list-style-type: none"> DPDK with SR-IOV DPDK with Virtio 	PA-VM-KVM-10.1.x.qcow2 PA-VM-KVM-10.2.x.qcow2 PA-VM-KVM-11.0.0.qcow2
PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	CentOS/Red Hat Enterprise Linux 9.1.x (9.1.x)	<ul style="list-style-type: none"> DPDK with SR-IOV DPDK with Virtio 	PA-VM-KVM-10.2.x.qcow2 PA-VM-KVM-11.0.0.qcow2

PAN-OS Version Support (Minimum)	VM-Series for KVM Version Support (Minimum)	I/O Enhancement Support	PAN-OS for VM-Series KVM Base Images
PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0)	Ubuntu 18.04	<ul style="list-style-type: none"> DPDK with SR-IOV DPDK with Virtio 	PA-VM-KVM-9.1.x.qcow2 PA-VM-KVM-10.1.x.qcow2
PAN-OS 10.1.x (10.1.0)	Ubuntu 20.04	<ul style="list-style-type: none"> DPDK with SR-IOV DPDK with Virtio 	PA-VM-KVM-10.1.x.qcow2
PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	Ubuntu 22.04	<ul style="list-style-type: none"> DPDK with SR-IOV DPDK with Virtio 	PA-VM-KVM-10.2.x.qcow2 PA-VM-KVM-11.0.0.qcow2
PAN-OS 10.1.x (10.1.0)	SUSE Enterprise Server 15 with QEMU 3.1.1	<ul style="list-style-type: none"> MacVTap Virtio 	PA-VM-KVM-10.1.x.qcow2

VM-Series for Nutanix

You can download base images from the [Palo Alto Networks Support Portal](#).



The VM-Series firewall for Nutanix uses the VM-Series firewall for KVM base image (qcow2).

PAN-OS Version Support (Minimum)	VM-Series for Nutanix Version Support (Minimum)	I/O Enhancement Support	VM-Series for KVM Base Image
PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) Layer 3 deployments, and virtual wire deployments with Service Chaining.	Nutanix AOS Version 5.10, 5.15 Nutanix AHV Release 20170830.185	DPDK supported	PA-VM-KVM-9.1.0.qcow2 PA-VM-KVM-10.1.x.qcow2
PAN-OS 10.1.x (10.1.0)	Nutanix AOS Version 5.20	DPDK supported	PA-VM-KVM-10.1.x.qcow2

PAN-OS Version Support (Minimum)	VM-Series for Nutanix Version Support (Minimum)	I/O Enhancement Support	VM-Series for KVM Base Image
PAN-OS 10.2.x (10.2.0) Layer 3 deployments, and virtual wire deployments with Service Chaining.	Nutanix AHV Release 20201105.2030		PA-VM-KVM-10.2.x.qcow2
PAN-OS 10.1.x (10.1.0) Layer 3 deployments, and virtual wire deployments with Service Chaining.	Nutanix AOS 6.5 version 6.0.5 in VPC mode	L3 mode only	PA-VM-KVM-10.1.x.qcow2

VM-Series for Hyper-V

You can download base images from the [Palo Alto Networks Support Portal](#).

PAN-OS Version Support (Minimum)	VM-Series for Hyper-V Version Support (Minimum)	I/O Enhancement Support	Base Image
PAN-OS 9.1.x (9.1.0)	<ul style="list-style-type: none"> Windows Server 2012 R2 with Hyper-V role or Hyper-V 2012 R2 Windows Server 2016 with Hyper-V role or Hyper-V 2016 Windows Server 2019 with Hyper-V role or Hyper-V 2019 	<ul style="list-style-type: none"> Packet MMAP supported DPDK not supported 	PA-VM-HPV-9.1.0.vhdx
PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	<ul style="list-style-type: none"> Windows Server 2012 R2 with Hyper-V role or Hyper-V 2012 R2 Windows Server 2016 with Hyper-V role or Hyper-V 2016 	<ul style="list-style-type: none"> DPDK with SR-IOV supported Packet MMAP with Virtio supported Packet MMAP with SR-IOV 	PA-VM-HPV-10.1.0.vhdx PA-VM-HPV-10.2.0.vhdx PA-VM-HPV-11.0.0.vhdx

PAN-OS Version Support (Minimum)	VM-Series for Hyper-V Version Support (Minimum)	I/O Enhancement Support	Base Image
	<ul style="list-style-type: none"> Windows Server 2019 with Hyper-V role or Hyper-V 2019 	supported	

VM-Series for OpenStack

You can download base images from the [Palo Alto Networks Support Portal](#).

PAN-OS Version Support (Minimum)	VM-Series for OpenStack Version Support (Minimum)	I/O Enhancement Support	Base Image
PAN-OS 9.1.x (9.1.5) PAN-OS 10.1.x (10.1.0)	Redhat OpenStack Queens 13	<ul style="list-style-type: none"> DPDK with Virtio DPDK with SR-IOV Packet MMAP with Virtio Packet MMAP with SR-IOV 	PA-VM-KVM-9.1.5.qcow2 PA-VM-KVM-10.1.0.qcow2
PAN-OS 10.1.x (10.1.3)	Redhat OpenStack Train 16	<ul style="list-style-type: none"> DPDK with Virtio DPDK with SR-IOV Packet MMAP with Virtio Packet MMAP with SR-IOV 	PA-VM-KVM-10.1.3.qcow2

Cisco ACI: Hardware and VM-Series Firewalls in Cisco ACI

See [Cisco ACI](#) for supported PAN-OS, Panorama, and Cisco ACI plugin versions.

You can download base images from the [Palo Alto Networks Support Portal](#).

Public Cloud Deployments

Palo Alto Networks supports the following public cloud deployments:

- [Public Cloud Deployments Available from a Marketplace—AWS, Azure, GCP, and Oracle](#)
- [Public Cloud Deployments Requiring a Base Image—Alibaba, Oracle, vCloud Air](#)
- [VM-Series Firewall for VMware Cloud on AWS](#)

Public Cloud Deployments Available from a Marketplace—AWS, Azure, GCP, and Oracle

Public Cloud Deployment	PAN-OS Version Support (Minimum)	I/O Enhancement Support
VM-Series on AWS List of supported AWS Regions . Support for AWS Outposts on PAN-OS 9.1 and later.	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	
VM-Series on Azure List of supported Azure Regions .	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0) Azure Stack Edge: PAN-OS 10.1.x (10.1.5)	DPDK is supported in PAN-OS 9.1 and later PAN-OS releases.
VM-Series on Google Cloud List of supported Google Cloud Regions	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0)	DPDK is supported and enabled by default.
VM-Series on Oracle Cloud Infrastructure	PAN-OS 9.1.x (9.1.0) PAN-OS 10.1.x (10.1.0) PAN-OS 10.2.x (10.2.0) PAN-OS 11.0.x (11.0.0) Oracle Gov Cloud: PAN-OS 9.1.x (9.1.3) PAN-OS 10.1.x (10.1.2) PAN-OS 10.2.x (10.2.0)	<ul style="list-style-type: none"> • DPDK is supported and enabled by default. • SR-IOV and MMAP mode is supported with jumbo and non-jumbo frames on PAN-OS 9.1.x and PAN-OS 10.1.x and later with VM-Series plugin 2.1.0 and later.

Public Cloud Deployment	PAN-OS Version Support (Minimum)	I/O Enhancement Support
	PAN-OS 11.0.x (11.0.0)	
VM-Series on IBM Cloud	PAN-OS 10.1.x (10.1.0)	—

Further I/O Enhancement support is detailed in [PacketMMAP and DPDK Drivers on VM-Series Firewalls](#).

To view the hypervisor support for Panorama versions, see [Panorama Hypervisor Support](#). To view the Panorama plugin requirements for public clouds, see [Public Cloud-AWS, Azure, GCP](#).

Public Cloud Deployments Requiring a Base Image—Alibaba, Oracle, vCloud Air

The following Public Clouds require a PAN-OS for VM-Series base image from the [Palo Alto Networks Support Portal](#).

Public Cloud Deployment	PAN-OS Version Support (Minimum)	I/O Enhancement Support	Base Image
VM-Series on Alibaba Cloud	PAN-OS 9.1.x (9.1.0)	DPDK and Packet MMAP are supported. DPDK is enabled by default.	PA-VM-KVM-9.1.0.qcow2

Further I/O Enhancement support is detailed in [PacketMMAP and DPDK Drivers on VM-Series Firewalls](#).

VM-Series Firewall for VMware Cloud on AWS

You can deploy the VM-Series firewall on VMware Cloud on AWS. Refer to the [Set Up a VM-Series Firewall on an ESXi Server](#) for information on deploying the VM-Series firewall. Refer to [VM-Series for VMware vSphere Hypervisor \(ESXi\)](#) for supported VMware ESXi versions.



The VM-Series firewall on VMware NSX-V and NSX-T is not supported on VMware Cloud on AWS.

PAN-OS Version Support	I/O Enhancement Support	Documentation
PAN-OS 9.1.x (9.1.0)	DPDK and SR-IOV	<ul style="list-style-type: none"> VMware Cloud on AWS Documentation VM-Series Firewall on VMware ESXi

PacketMMAP and DPDK Drivers on VM-Series Firewalls

The VM-Series firewall supports the PacketMMAP and Data Plane Development Kit (DPDK) drivers listed in the tables below. VM-Series firewalls use their own drivers to communicate with the drivers on the host. You should install host-driver versions that are equal to or later than the driver versions on your VM-Series firewall.

To choose host drivers for SR-IOV:

- **KVM**—On your KVM host, install a physical function (PF) driver version that is equal to or later than the virtual function (VF) native driver version listed below.
- **ESXi**—Refer to the [VMware Compatibility Matrix](#) and install the latest driver for the firmware version (PF=i40e, VF=i40evf).

For more on communication between VF drivers on the VM-Series firewall, and PF drivers on the host (the hypervisor), see [PacketMMAP and DPDK Drivers on VM-Series Firewalls](#) in the VM-Series Deployment Guide.

- [SR-IOV Access Mode](#)
- [PacketMMAP Driver Versions](#)
- [DPDK Driver Versions](#)

SR-IOV Access Mode

VM-Series firewalls support [SR-IOV Access Mode](#) on KVM and ESXi hypervisors. To enable single root I/O virtualization (SR-IOV) access mode, you can include the bootstrap parameter `plugin-op-commands=sriov-access-mode-on` in the `initcfg.txt` file.

- **KVM**—Requires PAN-OS 9.1.5 or a later PAN-OS release with VM-Series plugin 2.0.1 or a later plugin version.
- **ESXi**—Requires PAN-OS 9.1.5 or a later PAN-OS 9.1 release or PAN-OS 10.1 or a later PAN-OS release—with VM-Series plugin 2.0.5 or a later plugin version.

PacketMMAP Driver Versions

VM-Series firewalls use their virtual function (VF) drivers to communicate with the host's physical function (PF) drivers during SR-IOV. For example, i40e is a PF driver and i40evf is a VF driver.

PAN-OS Version	Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
11.0	bnx2x	1.713.36-0	
	i40e	2.14.13	
	iavf	4.0.2	

PAN-OS Version	Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
	igb	5.6.0	
	igbvf	2.4.0	
	ixgbe	5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf	4.1.0	
	mlx-en	4.9	
10.2	bnx2x	1.712.30-0	
	i40e	2.13.10	
	iavf	3.2.3	i40evf renamed to iavf; still compatible with i40en host driver.
	igb	5.4.0	
	igbvf	2.4.0	
	ixgbe	5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf	4.1.0	
	mlx-en	4.9	
10.1	bnx2x	1.712.30-0	
	i40e	2.13.10	
	iavf	3.2.3	i40evf renamed to iavf; still compatible with i40en host driver.
	igb	5.4.0	
	igbvf	2.4.0	
	ixgbe	5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf	4.1.0	
	mlx-en	4.9	

PAN-OS Version	Driver Filename	Virtual Firewall Native Drivers (Linux Version)	Comment
9.1	bnx2x	1.713.36-0	
	i40e	2.3.2	
	i40evf	3.2.2	Compatible with i40en host driver.
	igb	5.4.0	
	igbvf	2.4.0	
	ixgbe	5.1.0	The minimum version for multiple queues is 4.2.5
	ixgbevf	4.1.0	

DPDK Driver Versions

When the firewall is in DPDK mode, it uses DPDK drivers. Please check the official [DPDK](#) release notes for more information.

By default DPDK is enabled on VM-Series firewalls as stated below. If the VM-Series firewall detects an unsupported driver, the firewall reverts to PacketMMap mode.

Hypervisor	Virtual Driver	NIC Drivers
KVM	virtio	ixgbe, ixgbevf, i40e, i40evf, and mlx-en (PAN-OS 10.1 and later)
ESXi	VMXNET3	ixgbe, ixgbevf, i40e, i40evf



See [VM-Series for KVM](#) and [VM-Series for VMWare vSphere Hypervisor \(ESXi\)](#) for PAN-OS versions that support DPDK, DPDK with SR-IOV, or DPDK with Virtio.

PAN-OS Version	DPDK Version	Comment
11.0	20.11.1	
10.2	20.11.1	
10.1	19.11.3	
9.1	18.11	

Partner Interoperability for VM-Series Firewalls

Palo Alto Networks offers two tiers of support for third-party partner platforms for the VM-Series next-generation firewall—Palo Alto Networks Certified and Partner-Qualified. The VM-Series firewall provides the same security features and functionality regardless of support tier; the difference lies in what types of issues Palo Alto Networks is able to help you resolve.

- **Partner Qualified**—Palo Alto Networks Customer Support assists you with any issue directly related to the VM-Series firewall. VM-Series issues are defined as issues that occur after a packet enters the firewall. This does not include issues related to a partner platform.

VM-Series issues include:

- PAN-OS configuration
- VM-Series upgrades
- VM-Series licensing
- VM-Series documentation
- **Palo Alto Networks Certified**—Palo Alto Networks customer support assists with all VM-Series firewall issues as well as issues related to the partner platform. Platform issues are defined as issues that involve a packet outside of the VM-Series firewall, such as arriving or leaving the firewall or hypervisor or an issue with the hardware configuration.

Platform issues include:

- Network interfaces not recognized by the VM-Series firewall
- VM-Series firewall not booting
- Platform configuration
- Bootstrapping of the VM-Series firewall
- Connections to other networking devices
- High availability (HA)
- I/O Acceleration (DPDK, SR-IOV, and PCI passthrough)

For a complete list of the partner platforms supported in each tier, review the integration information:

- [Palo Alto Networks Certified Integrations](#)
- [Partner-Qualified Integrations](#)

Palo Alto Networks Certified Integrations

The following topic shows the Palo Alto Networks certified partner products with which VM-Series firewalls interoperate. Refer to the tables for details about hardware platforms and software versions on which you can deploy the VM-Series firewall.



*The partner software version and the PAN-OS® version columns display the range of versions and the minimum version in parentheses. For example, where the PAN-OS Version column displays **PAN-OS 10.1.x (10.1.4)**, it indicates that the integration supports PAN-OS 10.1 releases beginning with PAN-OS 10.1.4.*

- [Ciena](#)
- [Cisco Cloud Services Platform](#)
- [Cisco Enterprise Computer System \(ENCS\)](#)
- [Citrix SD-WAN](#)
- [Juniper NFX Network Services Platform](#)
- [NSX SD-WAN by VeloCloud](#)
- [Nuage Networks](#)
- [Versa Networks](#)
- [Vyatta](#)

Ciena

The following table shows the Ciena products with which VM-Series firewalls interoperate.

Hardware	Hypervi	SAOS Supported Software Version (Minimum)	SAOS Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
3906mvi and 3926mvi	KVM	18.x.x (18.06.00)	18.06.x (18.06.00)	9.1.x (9.1.0)	Layer 3 mode on the VM-50, VM-100, and VM-300 VirtIO and DPDK mode.	Ciena documentation

Cisco Cloud Services Platform

The following table shows the Cisco Cloud Services Platform (CSP) products with which VM-Series firewalls interoperate.

Hardware	Hypervi	CSP Supported Software Version (Minimum)	CSP Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
CSP5400 Series CSP2100 Series	KVM	2.x.x (2.4.0)	2.4.x (2.4.0)	9.1.x (9.1.0)	Layer 2, Layer3, Virtual wire deployments on all VM-	Set Up the VM-Series Firewall on Cisco CSP (PAN-OS 9.1)

Hardware	Hypervisor	CSP Supported Software Version (Minimum)	CSP Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
CSP5400 Series		4.6.x (4.6)	4.6.x (4.6.1-FC1)	10.1.x (10.1.0)	Series models except VM-50 VM-Series Firewalls in an HA configuration SR-IOV, Packet MMAP, and DPDK mode	Set Up the VM-Series Firewall on Cisco CSP (PAN-OS 10.1)

Cisco Enterprise Computer System (ENCS)

The following table shows the Cisco Enterprise Computer System (ENCS) products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	NFVIS Supported Software Version (Minimum)	Tested NFVIS Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Cisco 5400 Series	KVM	3.x.x (3.8) 4.6.x (4.6.1-FC1)	3.10.x (3.10.1) 3.12.x (3.12.1) 4.6.x (4.6.1-FC1)	9.1.x (9.1.0)	<ul style="list-style-type: none"> Layer 2, Layer3, Virtual wire deployments Firewalls in HA Virtio with DPDK mode enabled by default 	VM-Series on Cisco ENCS
		4.6.x (4.6)	4.6.x (4.6.1-FC1)	10.1.x (10.1.0)		

Citrix SD-WAN

The following table shows the Citrix SD-WAN products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	Supported Software Version (Minimum)	Tested Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Citrix SD-WAN 1100 Appliance	KVM	11.x.x (11.0.1)	11.0.x (11.0.1)	9.1.x (9.1.0)	Virtual wire deployments VirtIO with packet MMAP mode support only; so you must disable DPDK with op-cmd-dpdk-pkt-io=off in the <code>init-cfg.txt</code> file used for bootstrapping or use the CLI command set system setting dpdk-pkt-io off	<ul style="list-style-type: none"> Citrix SD-WAN Deployment Guide Citrix SD-WAN Solution Brief
				9.1.x (9.1.0)	Virtual wire DPDK Mode	

Juniper NFX Network Services Platform

The following table shows the Juniper NFX Network Services Platform products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	Junos Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
NFX 250	KVM	15.1X53-D470.x (15.1X53-D470.5)	9.1.x (9.1.0)	Layer 2, Layer 3, Virtual Wire DPDK mode	Juniper NFX documentation

NSX SD-WAN by VeloCloud

The following table shows the NSX SD-WAN by VeloCloud products with which VM-Series firewalls interoperate.

Hardware	Hypervi	VCE Supported Software Version (Minimum)	Tested VCE Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Edge 520v Edge 840	KVM	3.x.x (3.2.0)	3.3.x (3.3.1)	9.1.x (9.1.0)	Virtual wire deployments DPDK	NSX SD-WAN by VeloCloud documentation

Nuage Networks

The following table shows the Nuage Networks products with which VM-Series firewalls interoperate.

Hardware	Hypervi	VSP Supported Software Version (Minimum)	Tested VSP Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Nuage NSG-X series	—	5.x.x (5.3.3U3)	5.3.x (5.3.3U3)	TBD	Virtual wire deployments on VM-50 and VM-100 models VirtIO with packet MMAP mode support only DPDK must be disabled: If you bootstrap, include op-cmd-dpdk-pkt-io=off in the <code>init-cfg.txt</code> file, or, on the VM Series firewall, use the CLI command	Nuage Networks documentation

Hardware	Hypervisor	VSP Supported Software Version (Minimum)	Tested VSP Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
					set system setting dpdk-pkt-io off	

Versa Networks

The following table shows the Versa Networks products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	Supported Versa FlexVNF Software Version (Minimum)	Tested Versa FlexVNF Software Version (Minimum)	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
Versa 930 (Dell VEP4600)	KVM	21.x.x (21.1.2)	21.1.x (21.1.2)	9.1.x (9.1.0)	Virtual wire, L3 deployments with DPDK	Versa Documentation

Vyatta

The following table shows the Vyatta products with which VM-Series firewalls interoperate.

Platform	Hypervisor	Vyatta Software Version	PAN-OS Version (Minimum)	Deployment Modes Supported	Documentation
AT&T vRouter 5600	KVM	19.x (1903f)	9.1.x (9.1.0)	Virtual wire, L2, L3 deployments with DPDK VM-50, VM-100, and VM-300	—

Partner-Qualified Integrations

The following section shows the partner-qualified products with which VM-Series firewalls interoperate. Refer to the tables for details about hardware platforms and software versions on which you can deploy VM-Series firewalls.



The partner software version and PAN-OS® version columns display the range of versions and the minimum version in parentheses. For example, where the PAN-OS Version column displays **PAN-OS 10.1.x (10.1.4)**, it indicates that the integration supports PAN-OS 10.1 releases beginning with PAN-OS 10.1.4.

- [ADVA](#)
- [Aryaka](#)
- [Corsa](#)
- [Megaport](#)
- [SEL](#)
- [Siemens](#)
- [ZPE](#)
- [Zededa](#)

ADVA

The following table shows the ADVA products with which VM-Series firewalls interoperate.

Hardware	Supported ADVA Ensemble Connector Version	PAN-OS Version	I/O Acceleration	Documentation
FSP 150-XG304u	19.1.1.33	10.0.x (10.0.4)	DPDK mode with SR-IOV	ADVA Documentation

Aryaka

The following table shows the Aryaka products with which VM-Series firewalls interoperate.

Hardware	Supported Aryaka Software Versions	PAN-OS Version	I/O Acceleration	Documentation
2600 3000 10000	<ul style="list-style-type: none"> • 4.6.x • 4.8.x 	10.1.x (10.1.0)	<ul style="list-style-type: none"> • DPDK and Virtio • Virtio and Packet MMAP mode 	Aryaka Documentation

Hardware	Supported Aryaka Software Versions	PAN-OS Version	I/O Acceleration	Documentation
2600 3000	3.6.x	10.0.x (10.0.0) 9.1.x (9.1.0)	<ul style="list-style-type: none"> DPDK and Virtio Virtio and Packet MMAP mode 	
	<ul style="list-style-type: none"> 3.0.x 3.2.x 	9.1.x (9.1.0)	Virtio and Packet MMAP mode	

Corsa

The following table shows the Corsa products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
Corsa Security Platform	2.x.x	10.1.x (10.1.4)	SR-IOV with Packet MMAP	Corsa Documentation
	1.x.x	9.1.x (9.1.0)	SR-IOV with Packet MMAP	

Megaport

The following table shows the Megaport products with which VM-Series firewalls interoperate.

Hardware	Hypervisor	Mode	PAN-OS Version	I/O Acceleration	Documentation
Megaport Virtual Edge <ul style="list-style-type: none"> 2vCPU/8GB 4vCPU/16GB 8vCPU/32GB 12vCPU/48GB 	KVM	MVE provides Virtual Cross Connect (VXC) private network paths provisioned as a layer-2 802.1q VLANs.	10.2.x (10.2.0)	SR-IOV	Megaport Documentation

SEL

The following table shows the SEL products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
SEL-3350	AlmaLinux 8.6 RHEL 8.5	10.2.x (10.2.0)	None	SEL Documentation
SEL-3355	AlmaLinux 8.6 RHEL 8.5	10.2.x (10.2.0)	SR-IOV supported on SEL-3355 onboard ports	

Siemens

The following table shows the Siemens products with which VM-Series firewalls interoperate.

Hardware	Supported Software Version	PAN-OS Version	I/O Acceleration	Documentation
RUGGEDCOM APE 1808	Ubuntu 20.04 KVM	10.1.x (10.1.0) 9.1.x (9.1.4)	L3 mode Virtio with DPDK	Siemens Support Siemens Technology Partners RUGGEDCOM ROX II v.2.14 CLI Configuration Manual RUGGEDCOM ROX II v.2.14 WebUI Configuration Manual RUGGEDCOM APE1808 Configuration Manual

ZPE

The following table shows the ZPE products with which VM-Series firewalls interoperate.

Hardware	Supported Nodegrid Software Version	PAN-OS Version	I/O Acceleration	Documentation
Gate SR NSR	4.1.x	9.1.x (9.1.0)	Virtio with DPDK	ZPE Documentation

Zededa

The following table shows the Zededa products with which VM-Series firewalls interoperate.



Bootstrapping is not supported for the VM-Series firewall deployed on Zededa.

EVE Version	PAN-OS Version	Mode	I/O Acceleration	Documentation
8.5.4	11.0.x (11.0.0)	L3 Mode only IPv4 only	VirtIO	Zededa Documentation

VM-Series Plugin

The VM-Series plugin is built in to the VM-Series firewalls. You can configure this plugin directly on the VM-Series firewall or install it on a Panorama™ M-Series or virtual appliance.

To manage the VM-Series plugin configuration on your managed firewalls from Panorama, you must manually install the VM-Series plugin on Panorama. Refer to [Panorama Plugins](#). You can also compare [VM-Series Plugin and Panorama Plugins](#).

The following table briefly describes the features introduced in each version of the [VM-Series plugin](#). For additional information about each version, refer to the [VM-Series plugin release notes](#).

VM-Series Plugin 4.0.x

VM-Series plugin 4.0 versions are compatible with PAN-OS 11.0 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
4.0.3	11.0.2	Includes fixes to known issues.
4.0.2	11.0.2	Includes fixes to known issues.
4.0.1	11.0.1	Includes fixes to known issues.
4.0.0	11.0.0	Introduces support for Advanced Routing on the VM-Series firewall.

VM-Series Plugin 3.0.x

VM-Series plugin 3.0 versions are compatible with PAN-OS 10.2 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
3.0.5	10.2.5	Addresses known issues.
3.0.4	10.2.4	Addresses known issues.
3.0.3	10.2.3	Addresses known issues and introduces two new features—Configuring OCI CloudWatch monitoring and Publishing custom metrics in the OCI console.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
3.0.2	10.2.2	Addresses known issues.
3.0.1	10.2.1	Introduces one new feature—PAYG License Support for VM-Series on AWS, OCI, GCP and Azure.
3.0.0	10.2.0	Addresses known issues.

VM-Series Plugin 2.1.x

VM-Series plugin 2.1 versions are compatible with PAN-OS 10.1 releases. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.1.13	10.1.10	Introduces fixes for issues.
2.1.12	—	Introduces fixes for issues.
2.1.11	—	Introduces two new features—Full Bootstrap Support for the VM-Series on OCI and HA Support for the VM-Series on OCI in FIPS mode.
2.1.10	10.1.9-h1	Introduces fixes for issues.
2.1.9	10.1.9	Introduces fixes for issues.
2.1.8	—	Addresses known issues and introduces two new features—Configuring OCI CloudWatch monitoring and Publishing custom metrics in the OCI console.
2.1.7	10.1.7	Introduces fixes for issues.
2.1.6	10.1.6	Introduces fixes for issues.
2.1.5	10.1.5	Introduces fixes for issues.
2.1.4	10.1.4	Introduces one new feature—Limit the number of vCPUs licensed and used by a VM-Series firewall.
2.1.3	10.1.3	Addresses a known issue.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.1.2	10.1.2	Introduces two new features—Bootstrapping support for NUMA Performance Optimization and Azure Stack API Endpoint Access.
2.1.1	10.1.1	Introduces two new features—NUMA Performance Optimization and Six-Core Support for Intelligent Traffic Offload.
2.1.0	10.1.0	Default VM-Series plugin for PAN-OS 10.1.0.

VM-Series Plugin 2.0.x

VM-Series plugin 2.0 versions are compatible only with PAN-OS 9.1. The following table describes new features or changes introduced in each plugin version and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.0.7	9.1.10 10.0.6*	Introduces management interface swap support for the VM-Series on VMware ESXi and KVM and addresses known issues.
2.0.6	9.1.9 10.0.5*	Addresses a known issue.
2.0.5	—	Addresses known issues and adds 1500 MTU for Google Cloud Platform and SR-IOV access mode on ESXi with PAN-OS 9.1.5 and later or 10.0.1 and later.
2.0.4	10.0.4*	Addresses known issues and adds licensing support for future PAN-OS releases.
2.0.3	10.0.3*	<ul style="list-style-type: none"> Introduces custom image creation for the VM-Series firewall on Microsoft Azure. Introduces Pay-As-You-Go license support for the VM-Series on Oracle Cloud Infrastructure. Introduces enhancements for the VM-Series firewall on Alibaba Cloud. Addresses known issues.


VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
2.0.2	9.1.6 9.1.7 9.1.8 10.0.2*	<ul style="list-style-type: none"> Introduces shared storage on AWS, Azure and GCP. Supports subdirectories within cloud storage, enabling you to store multiple bootstrap files in one storage bucket. Introduces support for secure bootstrap on AWS. Change in default behavior: VM-Series plugin now uses HTTPS to communicate with the AWS CloudWatch endpoint. Addresses known issues.
2.0.1	10.0.1*	<ul style="list-style-type: none"> Introduces AWS active-passive high availability using a secondary IP address. Change in default behavior: In new VM-Series deployments on AWS, the default Packet IO mode is DPDK. Introduces bootstrapping with user data on AWS, Azure, and GCP. Introduces bootstrapping VLAN access mode on SR-IOV for VM-Series firewall on KVM only. Requires PAN-OS 9.1.5 and later, or 10.0.1 and later. Addresses known issues.
2.0.0	10.0.0*	Addresses known issues.


*PAN-OS 10.0 reached end-of-life (EoL) status on July 16, 2022.

VM-Series Plugin 1.0.x

VM-Series plugin 1.0 versions are compatible with PAN-OS 9.0 and PAN-OS 9.1 releases. The following table describes new features or changes introduced in each plugin versions and the VM-Series PAN-OS base image that includes each version of the plugin.

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
1.0.13	9.0.14 9.0.13 9.0.12 9.0.11	Addresses known issues.
1.0.12	9.1.4	<ul style="list-style-type: none"> Additional PAN-OS custom metrics for AWS, Azure, and GCP public clouds (panSessionConnectionsPerSecond,

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
	9.1.5	<p>panSessionThroughputKbps, and panSessionThroughputPps).</p> <ul style="list-style-type: none"> New system startup updates, system health periodic updates, and live health failure updates for AWS CloudWatch. Addresses known issues.
1.0.11	9.0.8 9.0.9 9.0.10 9.1.2 9.1.3	Introduces Deeper Visibility with AWS CloudWatch Enhancement and addresses known issues.
1.0.10	—	Addresses known issues on AWS.
1.0.9	—	Introduces support for Oracle Cloud Infrastructure marketplace deployment and high availability for the VM-Series firewall, and addresses known issues. PAN-OS 9.1.1 is required to use these OCI features.
1.0.8	9.1.0 9.1.1	<p>Addresses known issues.</p> <p>Default VM-Series plugin version for PAN-OS 9.1.</p>
1.0.7	—	<p>Addresses known issues, including bug fixes and support for high availability (HA) on Azure Government for the VM-Series on Azure.</p> <p>Earliest version on which you can enable (HA) on Azure Government for the VM-Series on Azure.</p>
1.0.6	—	Introduces support for the VM-Series firewall on NSX-T (North-South) and addresses known issues.
1.0.5	—	<p>Introduces the PAN-OS accelerated feature releases (images with .xfr in the filename*) for only VM-Series firewalls to enable support for new features and bug fixes; also addresses known issues.</p> <p>PAN-OS 9.0.4 requires plugin 1.0.5 or later.</p> <p> *All PAN-OS 9.0-xfr releases are end-of-life (EoL) as of September 19, 2020.</p>

VM-Series Plugin Version	Included in PAN-OS Base Image	New Features or Changes
1.0.4	—	Addresses known issues.
1.0.3	—	Addresses known issues.  <i>If you want to enable management interface swap on GCP or AWS platforms and you are running PAN-OS 9.0.2, you must install VM-Series plugin 1.0.3 or later.</i>
1.0.2	—	Addresses known issues.
1.0.0	—	Enables publishing metrics for supported public clouds: AWS , Azure , and Google Cloud Platform . Default VM-Series plugin version for PAN-OS 9.0.

AWS Regions

The AWS regions—public, GovCloud, and AWS Outposts—in which you can deploy the VM-Series firewall from the AWS Marketplace.

AWS Regions	Region ID
US East (N. Virginia)	us-east-1
US East (Ohio)	us-east-2
US West (N. California)	us-west-1
US West (Oregon)	us-west-2
Asia Pacific (Hong Kong)	ap-east-1
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Asia Pacific (Seoul)	ap-northeast-2
Asia Pacific (Osaka-Local) Available in BYOL as a Shared AMI. You can find the AMI for the VM-Series firewall on the EC2 console (Instances > Launch Instance > Community AMIs) using the AMI ID (ami-0d326a4c332ce4726) or by searching for Palo Alto Networks .	ap-northeast-3
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Beijing)	cn-north-1
Asia Pacific (Ningxia)	cn-northwest-1
Canada Central	ca-canada-1
EU (Frankfurt)	eu-central-1
EU (Ireland)	eu-west-1
EU (London)	eu-west-2

AWS Regions	Region ID
EU (Paris)	eu-west-3
EU (Stockholm)	eu-north-1
South America (Sao Paulo)	sa-east-1
Middle East (Bahrain)	me-south-1
Africa (Cape Town)	af-south-1
AWS Gov Cloud (US)	us-gov-west
	us-gov-east
AWS Outposts	On all regions listed above, where AWS Outposts is supported.

Azure Regions

The VM-Series firewall is available on the Azure public and the Azure Government Marketplace.

Locations	VM-Series Next-Generation Firewall Bundle 1*	VM-Series Next-Generation Firewall Bundle 2*	VM-Series Next-Generation Firewall (BYOL and ELA)**
All geographies (except China)	✓	✓	✓
Azure China	—	—	Only BYOL for PAN-OS 8.1
Azure Government (US)	✓	✓	✓
Azure DoD	✓	✓	✓

Refer to [Azure geography](#) for the list of regions.

Google Cloud Regions

You can deploy the VM-Series firewall with any supported PAN-OS® release in all Google Cloud Platform [regions](#).

Alibaba Cloud Regions

You can deploy the VM-Series firewall with PAN-OS® 8.1.3 and later PAN-OS 8.1 releases ([where supported](#)) or later supported PAN-OS releases in all Alibaba Cloud [regions](#).

VM-Series Firewall Amazon Machine Images (AMI)

The two most recent versions—2.0 and 2.1—of the CFT for auto scaling the VM-Series firewall on AWS and the VM-Series Auto Scale Template are supported on all supported PAN-OS releases.

Please [use the AWS CLI to find the AMI IDs](#) for automating your deployment of VM-Series firewalls. (For convenience, we captured the list of [PAN-OS Images for AWS GovCloud](#).)

PAN-OS Images for AWS GovCloud

Because AWS GovCloud had restricted access owing to specific U.S. regulatory requirements, the AMI IDs for the VM-Series firewall on AWS GovCloud are listed below for your convenience.

AMI IDs for VM-Series Firewalls on AWS GovCloud

Bring Your Own License (BYOL)

	us-gov-west-1 Cloned AMI ID	us-gov-east-1 Cloned AMI ID
PAN-OS 10.1.3	ami-0b0fb1dc91f1a5b9a	ami-0d1efc973806198d3
PAN-OS 10.1.1	ami-02f7ea8be900f9955	ami-0eeec392d066b8ae
PAN-OS 9.1.9	ami-01686e0ff6dccff8c	ami-067d99132a54489a7
PAN-OS 9.1.8	ami-013219291e2bfe323	ami-07df5511d166c456e
PAN-OS 9.1.3	ami-019045558d9d46abe	

Pay-as-You-Go (PAYG) Bundle 1

	us-gov-west-1 Cloned AMI ID	us-gov-east-1 Cloned AMI ID
PAN-OS 10.1.3	ami-004b1a1777dcd9f	ami-016368ea5efba04e1
PAN-OS 10.1.1	ami-084ed91c50f9b4d96	ami-057662646115fdce4
PAN-OS 10.1.0	ami-0a5f5b771f7f8e5d3	ami-07ac1c7c5ce547d69
PAN-OS 9.1.15	ami-0e91c03870e1cd93c	ami-03437a1f70f52e166
PAN-OS 9.1.12-h3	ami-0b5bc9e573a08b041	ami-06749834defebd4e0
PAN-OS 9.1.10-c15	ami-0099471b6d15fbddb	ami-07797e48453a0682f
PAN-OS 9.1.10	ami-0709b58e478cab702	ami-0a098d4a886576dad

AMI IDs for VM-Series Firewalls on AWS GovCloud

PAN-OS PAN-OS 9.1.3	ami-011be089674af6421	
------------------------	-----------------------	--

Pay-as-You-Go (PAYG) Bundle 2

	us-gov-west-1 Cloned AMI ID	us-gov-east-1 Cloned AMI ID
PAN-OS 10.1.3	ami-0fb205aaef8ce2043	ami-0cb03b7f09207667b
PAN-OS 10.1.1	ami-0828cee4fb427a163	ami-0997795d86a05ede0
PAN-OS 10.1.0	ami-099a18de4da9ae98f	ami-0debf73b0bb9c2dbe
PAN-OS 9.1.15	ami-0a3050b051091a0eb	ami-0d67ea2069394aaba
PAN-OS 9.1.12-h3	ami-004abe9b7a57eed38	ami-068bf7a0c5746f727
PAN-OS 9.1.10-c15	ami-0a192fdfa754d6c40	ami-01df4c86af829b978
PAN-OS 9.1.10	ami-0fc65b7bb5280ec09	ami-050f8775e829afef7
PAN-OS 9.1.3	ami-06695afbfbca39f61	




CN-Series Firewalls





The CN-Series firewall is supported only in certain environments and is compatible with or requires a specific set of files to do so.

- [CN-Series Supported Environments](#)
- [CN-Series Firewall Image and File Compatibility](#)

CN-Series Supported Environments




You can deploy the CN-Series firewall in the following environments.

Product	Version		
	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Container runtime	Docker CRI-O Containerd	Docker CRI-O Containerd	Docker CRI-O Containerd
Kubernetes version	1.17 through 1.27	1.17 through 1.27	1.17 through 1.27
Cloud provider managed Kubernetes	<ul style="list-style-type: none"> AWS EKS (1.17 through 1.26) EKS on AWS Outpost (1.17 through 1.22) <div>  <p>CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.</p> </div>	<ul style="list-style-type: none"> AWS EKS (1.17 through 1.26) EKS on AWS Outpost (1.17 through 1.22) <div>  <p>CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.</p> </div>	<ul style="list-style-type: none"> AWS EKS (1.17 through 1.26) EKS on AWS Outpost (1.17 through 1.22) <div>  <p>CN-Series for EKS on AWS Outpost does not support SR-IOV or Multus.</p> </div>

Product	Version		
	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
	<ul style="list-style-type: none"> Azure AKS (1.17 through 1.27) <p> In Azure AKS, the PAN-OS 10.1.10h1 is the minimum required version to support kubernetes 1.25 and above.</p> <ul style="list-style-type: none"> AliCloud ACK (1.26) GCP GKE (1.17 through 1.23) 	<ul style="list-style-type: none"> Azure AKS (1.17 through 1.27) <p> In Azure AKS, the PAN-OS 10.2.4h3 is the minimum required version to support kubernetes 1.25 and above.</p> <ul style="list-style-type: none"> GCP GKE (1.17 through 1.26) <p> In GCP GKE, the PAN-OS 10.2.4h3 is the minimum required version to support kubernetes 1.25 and above.</p> <ul style="list-style-type: none"> Google Anthos 1.12.3 OCI OKE (1.23) 	<ul style="list-style-type: none"> Azure AKS (1.17 through 1.27) <p> In Azure AKS, the PAN-OS 11.0.2 is the minimum required version to support kubernetes 1.25 and above.</p> <ul style="list-style-type: none"> GCP GKE (1.17 through 1.24) OCI OKE (1.23)
Customer managed Kubernetes	<p>On the public cloud or on-premises data center.</p> <p>Make sure that the Kubernetes version, CNI Types, and Host VM OS</p>	<p>On the public cloud or on-premises data center.</p> <p>Make sure that the Kubernetes version, CNI Types, and Host VM OS</p>	<p>On the public cloud or on-premises data center.</p> <p>Make sure that the Kubernetes version, CNI Types, and Host VM OS</p>

Product	Version		
	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
	<p>versions are included in this table.</p> <p>VMware TKG+ version 1.1.2</p> <ul style="list-style-type: none"> Infrastructure Platform—vSphere 7.0 Kubernetes Host VM OS—Photon OS 	<p>versions are included in this table.</p> <p>VMware TKG+ version 1.1.2</p> <ul style="list-style-type: none"> Infrastructure Platform—vSphere 7.0 Kubernetes Host VM OS—Photon OS 	<p>versions are included in this table.</p> <p>VMware TKG+ version 1.1.2</p> <ul style="list-style-type: none"> Infrastructure Platform—vSphere 7.0 Kubernetes Host VM OS—Photon OS
Kubernetes Host VM	<p>Operating System:</p> <ul style="list-style-type: none"> Ubuntu 16.04 Ubuntu 18.04 Ubuntu-22.04 RHEL/Centos 7.3 and later CoreOS 21XX, 22XX Container-Optimized OS 	<p>Operating System:</p> <ul style="list-style-type: none"> Ubuntu 16.04 Ubuntu 18.04 Ubuntu-22.04 RHEL/Centos 7.3 and later CoreOS 21XX, 22XX Container-Optimized OS 	<p>Operating System:</p> <ul style="list-style-type: none"> Ubuntu 16.04 Ubuntu 18.04 Ubuntu-22.04 RHEL/Centos 7.3 and later CoreOS 21XX, 22XX Container-Optimized OS
	<p>Linux Kernel Netfilter: Iptables</p>	<p>Linux kernel version:</p> <ul style="list-style-type: none"> 4.18 or later (K8s Service Mode only) 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information. 	<p>Linux kernel version:</p> <ul style="list-style-type: none"> 4.18 or later (K8s Service Mode only) 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information.
	<p>Linux kernel version:</p> <ul style="list-style-type: none"> 4.18 or later (K8s Service Mode only) 5.4 or later required to enable AF_XDP mode. See Editable Parameters in CN-Series Deployment YAML Files for more information. 	<p>Linux kernel Netfilter: Iptables</p>	<p>Linux kernel Netfilter: Iptables</p>

Product	Version		
	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
CNI Plugins	CNI Spec 0.3 and later: <ul style="list-style-type: none"> • AWS-VPC • Azure • Calico • Flannel • Weave • For AliCloud, Terway • For Openshift, OpenshiftSDN • The following are supported on the CN-Series firewall as a DaemonSet. <ul style="list-style-type: none"> • Multus • Bridge • SR-IOV • Macvlan 	CNI Spec 0.3 and later: <ul style="list-style-type: none"> • AWS-VPC • Azure • Calico • Flannel • Weave • For Openshift, OpenshiftSDN • The following are supported on the CN-Series firewall as a DaemonSet. <ul style="list-style-type: none"> • Multus • Bridge • SR-IOV • Macvlan 	CNI Spec 0.3 and later: <ul style="list-style-type: none"> • AWS-VPC • Azure • Calico • Flannel • Weave • For Openshift, OpenshiftSDN • The following are supported on the CN-Series firewall as a DaemonSet. <ul style="list-style-type: none"> • Multus • Bridge • SR-IOV • Macvlan

Product	Version		
	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
OpenShift	CN-Series as a DaemonSet: 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, and 4.13	<ul style="list-style-type: none"> Version 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, and 4.13 	<ul style="list-style-type: none"> Version 4.2, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, and 4.13
	CN-Series as a K8s Service: (PAN-OS 10.1.2 and later) 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, and 4.13  The PAN-OS 10.1.10h1 is the minimum required version to support 4.12 and above.	<ul style="list-style-type: none"> OpenShift 4.7 is qualified on the CN-Series as a DaemonSet only. OpenShift on AWS  The PAN-OS 10.2.4h3 is the minimum required version to support 4.12 and above.	 OpenShift 4.7 is qualified on the CN-Series as a DaemonSet only. The PAN-OS 11.0.2 is the minimum required version to support 4.12 and above. <ul style="list-style-type: none"> OpenShift on AWS

CN-Series Firewall Image and File Compatibility

Deploying the CN-Series firewall requires a number of different of files. To help ensure a successful deployment, check the following information to make sure you download the correct combination of files for your CN-Series firewall deployment.

PAN-OS Version	YAML Version	CNI Version	mgmt-init Version
PAN-OS 11.0.x	3.0.x	3.0.x	3.0.x
PAN-OS 10.2.x			
PAN-OS 10.1.x			

Panorama

This section includes information about Panorama™ and compatible versions for devices that Panorama can manage, as well as about plugins that are available for Panorama.

- [Plugins](#)
- [Compatible Plugin Versions for PAN-OS 10.2](#)
- [Panorama Management Compatibility](#)
- [Panorama Hypervisor Support](#)
- [Device Certificate for a Palo Alto Networks Cloud Service](#)

Panorama Plugins

The following tables describe the features and functionality introduced with the Panorama™ extensible plugin architecture.

- [Cisco ACI](#)
- [Cisco TrustSec](#)
- [Panorama CloudConnector Plugin \(Formerly, AIOps Plugin for Panorama\)](#)
- [Cloud Services](#)
- [Enterprise Data Loss Prevention \(DLP\)](#)
- [Panorama Interconnect](#)
- [IPS Signature Converter](#)
- [Kubernetes](#)
- [Clustering Plugin](#)
- [Nutanix](#)
- [OpenConfig \(Firewall Only\)](#)
- [Panorama Software Firewall License Plugin](#)
- [Public Cloud—AWS, Azure, and GCP](#)
- [SD-WAN](#)
- [VMware NSX](#)
- [VMware vCenter](#)
- [Zero Touch Provisioning \(ZTP\)](#)

For more information on Panorama plugin versions, refer to the [VM-Series and Panorama Plugins Release Notes](#).

Cisco ACI


The following table shows the features introduced in each version of the Panorama™ plugin for Cisco ACI. The plugin uses device groups on Panorama to push the configuration to the managed firewalls.




End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
3.0.0	<ul style="list-style-type: none"> • 6.0.x 	10.2(10.2.4)	Latest	Introduces enhancements to

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	<ul style="list-style-type: none"> 5.2.x 5.1.x 	10.2(10.2.0)		increase reliability and robustness.
2.0.3	• 6.0.x	10.1 (10.1.9)	Latest	Introduces a fix for a known issue.
	<ul style="list-style-type: none"> 5.2.x 5.1.x 	10.1 (10.1.0) 10.0 (10.0.0)		

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	<ul style="list-style-type: none"> 5.0.x 4.2.x 4.1.x 4.0.x 3.2 	9.1 (9.1.0) 9.0 (9.0.0)		 You can do a new deployment of Cisco ACI 2.0.3 on Panorama 9.0 or later. You can also upgrade from Cisco ACI 2.0.x to Cisco ACI 2.0.3. However, if you need to upgrade from Cisco ACI 1.0.0 or Cisco ACI 1.0.1, you will need to upgrade your Panorama to 10.0 or later, and then upgrade the ACI plugin to 2.0.3.
2.0.2	<ul style="list-style-type: none"> 5.1.x 5.0.x 4.2.x 4.1.x 	10.1 (10.1.0) 10.0 (10.0.0) 9.1 (9.1.0)	Latest	Introduces Cisco ACI 5.1 support and fixes for known issues.

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	<ul style="list-style-type: none"> 4.0.x 3.2 	9.0 (9.0.0)		 You can do a new deployment of Cisco ACI 2.0.2 on Panorama 9.0 or later. You can also upgrade from Cisco ACI 2.0.x to Cisco ACI 2.0.2. However, if you need to upgrade from Cisco ACI 1.0.0 or Cisco ACI 1.0.1, you will need to upgrade your Panorama to 10.0 or later, and then upgrade the ACI plugin to 2.0.2.
2.0.1	<ul style="list-style-type: none"> 5.0.x 4.2.x 4.1.x 4.0.x 	10.1 (10.1.0) 10.0 (10.0.0) 9.1 (9.1.0) 9.0 (9.0.0)	Latest	Introduces fixes for known issues.

Plugin Version	Supported Cisco ACI Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
	<ul style="list-style-type: none"> 3.2 			
2.0.0	<ul style="list-style-type: none"> 5.0.x 4.2.x 4.1.x 4.0.x 3.2 	10.1 (10.1.0) 10.0 (10.0.0) 9.1 (9.1.0) 9.0 (9.0.0)	Latest	Introduces the Panorama Plugin for Cisco ACI Dashboard and two new monitored attributes—L2 external endpoint groups and subnets under bridge domains.
1.0.1	<ul style="list-style-type: none"> 5.0.x 4.0.x 3.2 3.1 2.3(1e) 	8.1 (8.1.6)	9.1	Introduces support for multiple IP addresses per endpoint and Cisco ACI 4.0 and later.
1.0.0	<ul style="list-style-type: none"> 5.0.x 3.2 3.1 2.3(1e) 	8.1 (8.1.6)	9.1	Enables support for Endpoint Monitoring from Panorama. Configure the Panorama plugin for Cisco ACI to monitor endpoints so that you can consistently enforce security policy that automatically adapts to changes within your ACI deployment.

Cisco TrustSec

The following table shows the features introduced in each version of Panorama™ plugin for Cisco TrustSec.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Minimum Panorama PAN-OS Version	Qualified Cisco ISE Versions	Features
2.0.0	10.2.0	<ul style="list-style-type: none"> • ISE 3.1 • ISE 2.7 	<p>Introduces support for Panorama 10.2.x.</p> <p>Introduces support for security group tags (SGT). Use these tags as match criteria for placing IP addresses in dynamic address groups.</p>
1.0.3	9.0.0	<ul style="list-style-type: none"> • ISE 3.1 • ISE 2.7 	Introduces a fix for one issue.
1.0.2	9.0.0	<ul style="list-style-type: none"> • ISE 2.4 • ISE 2.6 	Introduces the PubSub monitoring mode, which parses notifications directly from the server. The plugin enables PubSub mode when v1.0.2 is running on Panorama 10.0.0 and later. If v1.0.2 is running on a Panorama version earlier than 10.0.0, the monitoring mode is Bulk Sync.
1.0.1			<ul style="list-style-type: none"> • Lowers the minimum monitoring interval from 30 seconds to 10 seconds. • Combined Logs for the Panorama Plugin for Cisco TrustSec.
1.0.0			Enables support for endpoint monitoring from Panorama. Configure the Panorama plugin for Cisco TrustSec to monitor endpoints so that you can consistently enforce

Plugin Version	Minimum Panorama PAN-OS Version	Qualified Cisco ISE Versions	Features
			security policy that automatically adapts to changes within your TrustSec environment.

Panorama CloudConnector Plugin (Formerly, AIOps Plugin for Panorama)

The following table shows the features introduced in each version of the plugin for [AIOps](#).

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	New Features or Changes
2.0.1	10.2 (10.2.3)	Latest	Introduces enhancements for Cloud NGFW for AWS integration with Panorama.
2.0.0	10.2 (10.2.3)	Latest	Enables you to use the Panorama AWS plugin 5.0.0 to author and push device group based policies to Cloud NGFW for AWS resources.
1.1.0	10.2 (10.2.3)	Latest	Enables the policy analyzer feature that helps you to check if a new security rule meets your intended purpose and that it does not duplicate, shadow, or conflict with your existing rules (pre-commit). You can also check for duplication and other anomalies across your current Security policy rulebase (post-commit).
1.0.0	10.2 (10.2.1)	Latest	Enables you to proactively enforce best practice checks by validating your commits and letting you know if a policy needs work before pushing it to your Panorama.

Cloud Services

You use the Cloud Services plugin to activate Panorama Managed Prisma Access and to retrieve logs from [Panorama-managed firewalls](#) using [Cortex Data Lake](#). Review the following table to see the minimum Panorama and plugin versions for your deployment type.

Deployment Type	Panorama and Plugin requirements
Panorama Managed Prisma Access	Dependent on plugin version. Review the minimum required Panorama software versions required for the plugin you are running. To find the plugin version you are running, select Panorama > Cloud Services > Configuration > Service Setup and find the plugin version in the Plugin Alert area.
Cortex Data Lake log retrieval from Panorama-managed firewalls only	Cortex Data Lake Software Compatibility has the minimum Panorama and plugin requirements.

Enterprise Data Loss Prevention (DLP)

The following table shows the features introduced in each version of the Panorama™ plugin for Enterprise Data Loss Prevention (DLP).



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
4.0.1	11.0.2	Latest	Cloud Services 4.0 Preferred	<p>Enterprise Data Loss Prevention (E-DLP) now supports creating a file type include or exclude list for data filtering profiles configured for file-based inspection. This allows you to select one of two modes:</p> <ul style="list-style-type: none"> • Inclusion Mode—Allow only specified file types be scanned by Enterprise DLP. • Exclusion Mode—Allow all supported files to be scanned

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
				<p>by Enterprise DLP by default but excluding the file types you specify.</p> <p>Exclusion Mode includes True File Type Support and does not rely on file extensions to determine file types.</p>
4.0.0	11.0.0	11.0.1	Cloud Services 4.0 Preferred	<p>You must upgrade to Enterprise DLP 4.0 plugin to upgrade to PAN-OS 11.0. Additionally, you must download the Enterprise DLP 4.0 plugin before you attempt to install PAN-OS 11.0.</p>
3.0.5	10.2.4-h3	Latest 10.2 Release	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Minor bug and performance fixes.
3.0.4	10.2.4	10.2.4-h3	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Enterprise DLP now supports new applications , expanded download support and large file inspection for many existing applications, and FedRAMP High compliance.
3.0.3	10.2.3-h4	10.2.4	Prisma Access 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Enterprise DLP now supports upload inspection of files up to 100MB in size for the Box Web App and Web Browsing applications .

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
3.0.2	10.2.3	Latest 10.2.3-h4	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	Enterprise DLP now supports inspection of file and non-file based HTTP/2 traffic.
3.0.1	10.2.1	10.2.3	Cloud Services 3.1.0-h50 (PAN-OS 10.2.2-h1 and later releases)	The Panorama plugin for Enterprise DLP supports creating a data filtering profile to scan non-file based traffic for sensitive data.
3.0.0	10.2.0	10.2.1	Not Supported	Upgrade to the Enterprise DLP plugin to increase reliability. Enterprise DLP plugin 3.0 is required to upgrade to PAN-OS 10.2 and is supported only on PAN-OS 10.2 and later releases.
1.0.7	10.0.5	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.6	10.0.5	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.5	10.0.5	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.4	10.0.5	Latest 10.1 Release	Cloud Services 2.2	Minor bug and performance fixes.
1.0.3	10.0.5	Latest 10.1 Release	Cloud Services 2.2	The Panorama plugin for DLP supports the integration of Enterprise DLP with Prisma Access.
1.0.2	10.0.5	Latest 10.1 Release	Not Supported	No new features were added for this release.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Cloud Services Plugin (Minimum)	Features
1.0.1	10.0.2	Latest 10.1 Release	Not Supported	Enables support for Enterprise DLP from Panorama. Configure the Panorama plugin for Enterprise DLP to protect against unauthorized access, misuse, extraction, and sharing of sensitive information and effectively filter network traffic to block or generate an alert before sensitive information leaves the network.

Panorama Interconnect

The following table shows the features introduced in each version of the [Panorama™ Interconnect](#) plugin.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Minimum PAN-OS Version	Maximum PAN-OS Version	New Features or Changes
2.0.0	10.2.4 (PAN-OS 10.2 release)	Latest 10.2 version (PAN-OS 10.2 release)	You must upgrade to Panorama Interconnect 2.0.0 plugin to upgrade to PAN-OS 10.2.
1.1.0	10.0.0	Latest 10.1 version	Enables you to selectively push device groups, template stacks, and some common Panorama configurations from the Panorama Controller to the Panorama Nodes to avoid pushing extraneous configurations to Panorama Nodes to

Plugin Version	Minimum PAN-OS Version	Maximum PAN-OS Version	New Features or Changes
			minimize configuration bloat and operational delays across your Panorama Interconnect deployment.
1.0.2	8.1.3	Latest 10.1 version	Minor bug and performance fixes.
1.0.1	8.1.3	Latest 10.1 version	Minor bug and performance fixes.
1.0.0	8.1.3	Latest 10.1 version	First plugin introduced to support a two-tier Panorama deployment for a horizontal scale-out architecture.

IPS Signature Converter

The following table shows the features introduced in each version of the Panorama™ IPS Signature Converter plugin.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Minimum PAN-OS Version	Features
2.0.2	10.2	Supports SMTP and FTP protocols.
2.0.1	10.2	Supports HTTP sticky buffers. Now converts Snort rules that have commas separating content patterns and their associated suboption.
2.0.0	10.2	Uses Python 3 for compatibility with PAN-OS 10.2.
1.0.6	10.0	Supports SMTP and FTP protocols.
1.0.5	10.0	Supports HTTP sticky buffers.

Plugin Version	Minimum PAN-OS Version	Features
		Now converts Snort rules that have commas separating content patterns and their associated suboption.
1.0.4	10.0	No significant changes in functionality.
1.0.3	10.0	<p>Converts rules into SSL custom signatures if their port is 443.</p> <p>Converts server-to-client HTTP rules without content modifiers into custom signatures with the http-rsp-status-line and http-rsp-headers contexts.</p> <p>Converts Suricata TLS rules into TLS custom signatures and supports additional TLS and file data sticky buffers.</p>
1.0.2	10.0	<p>Converts rules that use the smb protocol or port 445.</p> <p>Supports HTTP sticky buffer keywords in Suricata rules.</p> <p>Converts HTTP rules into HTTP custom signatures if either the port in the rule is HTTP-PORTS or the protocol is http.</p>
1.0.1	10.0	Identifies whether newly converted signatures are already included as part of your Palo Alto Networks Threat Prevention subscription.
1.0.0	10.0	<p>Enables support for third-party IPS signature conversion from Panorama. Use the Panorama IPS Signature Converter plugin to gain immediate protection against newly discovered threats by converting third-party IPS rules into Palo Alto Networks custom threat signatures and distributing them to your Panorama-managed firewalls.</p>

Kubernetes

The following table displays the features introduced in each version of the Panorama™ Kubernetes plugin.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Minimum Panorama PAN-OS Version	Maximum Panorama PAN-OS Version	Features
4.0.0	11.0	Latest	Introduces new features like CN-Series Hyperscale Security Fabric, (HSF), Tag Length Enhancement, Shared DAG Support, and Nested DAG Support.
3.0.1	10.2	Latest	Introduces support for shared dynamic address groups.
3.0.0	10.2	Latest	Introduces Retrieving IPv6 Addresses for Multus CNI Setup, Tag Pruning, Service Account Validation, and advanced Dashboard features.
2.0.2	10.1	10.1.x	K8s plugin 2.0.2 creates a new template on Panorama called K8S-Network-Setup-V1-125 . This template creates 250 vwire interfaces and 125 vwires.
2.0.1	10.1	10.1.x	Introduces fixes for known issues.
2.0.0	10.1	10.1.x	Introduces Core-Based Licensing, Multiple Interface Support, and Custom Certificate Chaining.

Plugin Version	Minimum Panorama PAN-OS Version	Maximum Panorama PAN-OS Version	Features
1.0.5	10.0	10.1.x	Introduces fixes for known issues.
1.0.4	10.0	10.1.x	Introduces fixes for known issues.
1.0.3	10.0	10.1.x	Introduces fixes for known issues.
1.0.2	10.0	10.1.x	Introduces fixes for known issues.
1.0.1	10.0	10.1.x	Introduces the ability to disable the creation of service objects on Panorama, and support for offline licensing of CN-Series firewalls with Panorama.
1.0.0	10.0	10.1.x	Manages licenses for the CN-Series firewall and enables you to monitor clusters and leverage Kubernetes labels that you use to organize Kubernetes objects. The plugin communicates with the API server and retrieves metadata, which gives you visibility into applications running within a cluster.

Clustering Plugin

The following table shows the features introduced in Panorama Clustering plugin.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
1.0.0	11.0	Latest	Provides the visibility to the Hyper Scale Security

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
			Fabric (HSF) clusters in CN-Series.

Nutanix

The following table shows the features introduced in each version of the Panorama™ plugin for Nutanix.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.0.1	10.2 (10.2.0)	Latest	Introduces fixes for known issues.
2.0.0	10.2 (10.2.0)	Latest	Introduces enhancements to increase reliability and robustness.
1.0.0	9.0 (9.0.4)	Latest	Enables support for VM Monitoring from Panorama. Configure the Panorama plugin for Nutanix to monitor VM workloads so that you can consistently enforce security policy that automatically adapts to changes within your Nutanix environment.

OpenConfig (Firewall Only)

The following table shows the features introduced in each version of the [OpenConfig](#) plugin.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version (Minimum)	New Features or Changes
1.2.0	10.1	Enables support for protobuf and unbundling.
1.1.0	10.1	Enables support for these standard OpenConfig models: <ul style="list-style-type: none"> • openconfig-ha • openconfig-zones • openconfig-network-instances • openconfig-routing-policy • openconfig-ospfv2
1.0.0	10.1	Enables support for the OpenConfig plugin on PAN-OS firewalls so that you can use standard OpenConfig models to automate configuration and stream telemetry.

Panorama Software Firewall License Plugin

The following table shows the features introduced in each version of the Panorama™ Software Firewall License plugin.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Minimum VM-Series Plugin Version	Features
1.1.1	10.0 (10.0.4)	Latest	2.0.4	Introduces fixes for known issues.
1.1.0	10.0 (10.0.4)	Latest	2.0.4	Introduces fixes for known issues.
1.0.0	10.0 (10.0.4)	Latest	2.0.4	The Panorama Software Firewall License plugin allows you to automatically license a VM-Series firewall

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Minimum VM-Series Plugin Version	Features
				when it connects to Panorama.

Public Cloud—AWS, Azure, and GCP

The following table shows the features introduced in each version of the Panorama™ plugin for Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). The plugins use device groups and templates on Panorama to push the configuration to the managed firewalls.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Public Cloud Platform	AWS Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
AWS	5.1.1	10.2 (10.2.3)	Latest	3.0.0	Introduces enhancements for Cloud NGFW for AWS integration with Panorama.
	5.0.1	10.2 (10.2.3)	Latest	3.0.0	Introduces enhancements for Cloud NGFW for AWS integration with Panorama.
	5.0.0	10.2 (10.2.3)	Latest	3.0.0	Introduces support for Panorama integration with Cloud NGFW for AWS .
	4.1.0	10.2	Latest	3.0.0	Introduces support for nested dynamic address groups and tag pruning.
	4.0.0	10.2	Latest	3.0.0	Introduces enhancements to

Public Cloud Platform	AWS Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
					increase reliability and robustness.
	3.0.3	10.0 (10.0.5)	10.1.x	2.0.6	Introduces shared dynamic address groups support and bug fixes.
	3.0.2	10.0 (10.0.5)	10.1.x	2.0.6	Introduces proxy support and bug fixes.
	3.0.1	10.0 (10.0.5)	10.1.x	2.0.6	Introduces enhancements and bug fixes.
	3.0.0	10.0 (10.0.5)	10.1.x	2.0.6	Introduces Panorama Orchestration and new monitoring parameters.
	2.0.2	10.1 (10.1.0)	10.1.x	2.0.2	Introduces fixes for known issues.
		10.0 (10.0.0)	10.1.x	2.0.0	
		9.1 (9.1.2)	10.1.x	1.0.8	
		9.0 (9.0.6)	10.1.x	1.0.4	
	2.0.1	9.1 (9.1.2)	10.1.x	1.0.4	Introduces a fix for a known issue.
		9.0 (9.0.6)	10.1.x		
	2.0.0	9.1 (9.1.2)	10.1.x	1.0.8	Enables support for: <ul style="list-style-type: none"> VM Monitoring Secure Kubernetes Services in an EKS Cluster
		9.0 (9.0.6)	10.1.x	1.0.4	

Public Cloud Platform	AWS Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
	1.0.1	9.0 (9.0.0) 8.1 (8.1.3)	9.0.x	N/A	Introduces fixes for known issues.
	1.0.0	9.0 (9.0.0) 8.1 (8.1.3)	9.0.x	N/A	Enables support for VM Monitoring to monitor the virtual machine inventory within your AWS VPCs so that you can consistently enforce Security policy that automatically adapts to changes within your AWS deployment.

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
Azure	5.1.0	10.2.4	Latest	4.0.0	Introduces tag pruning feature to increase the scalability and the number of tags collected by the Azure plugin
	5.0.0	10.2.4	Latest	4.0.0	Introduces support for Panorama integration with Cloud NGFW for Azure.
	4.2.0	10.2.3	Latest	3.0.1	Introduces support for Azure Workspace-

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
					based Application Insights.
	4.1.0	10.2	Latest	3.0.1	Increased the number of front-end applications per VM-Series for Azure deployment.
	4.0.0	10.2	Latest	3.0.1	Introduces enhancements to increase reliability and robustness.
	3.2.0	10.0 (10.0.1)	10.1.x	2.0.1	Introduces proxy support and fix for a known issue.
		10.1 (10.1.0)	10.1.x	2.1.0	
	3.1.0	10.0 (10.0.1)	10.1.x	2.0.1	Introduces fixes for a known issue.
		10.1 (10.1.0)	10.1.x	2.1.0	
	3.0.1	10.0 (10.0.1)	10.1.x	2.0.1	Introduces fixes for known issues.
		10.1 (10.1.0)	10.1.x	2.1.0	
	3.0.0	10.0 (10.0.1)	10.1.x	2.0.1	Introduces Panorama Orchestration.
		10.1 (10.1.0)	10.1.x	2.1.0	
	2.0.3	9.0 (9.0.6)	10.1.x	1.0.4	Introduces a fix for a known issue.
		9.1 (9.1.2)	10.1.x	1.0.8	
		10.0 (10.0.0)	10.1.x	2.0.0	
		10.1 (10.1.0)	10.1.x	2.1.0	
	2.0.2	8.1 (8.1.11) 9.0 (9.0.5)	10.1.x	1.0.4	Introduces fixes for known issues.

Public Cloud Platform	Azure Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version (Minimum)	Features
	2.0.1	8.1 (8.1.11) 9.0 (9.0.5)	10.1.x	1.0.4	Introduces fixes for known issues.
	2.0.0	8.1 (8.1.8)	10.1.x	N/A	Enables support for: <ul style="list-style-type: none"> • Auto Scaling—Template v1.0 • Azure Kubernetes Service (AKS) Cluster—Template v1.0
		9.0 (9.0.3)	10.1.x	1.0.4	Enables support for: <ul style="list-style-type: none"> • Auto Scaling—Template v1.0 • Azure Kubernetes Service (AKS) Cluster—Template v1.0
	1.0.0	8.1 (8.1.3) 9.0 (9.0.0)	9.0.x	N/A	Enables support for VM Monitoring from Panorama. Configure the Panorama plugin for Azure to monitor the virtual machine inventory within your Azure subscription.

Public Cloud Platform	GCP Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	VM-Series Plugin Version	Features
GCP	3.0.0	10.2	Latest	3.0.0	Introduces enhancements to increase reliability and robustness.
	2.0.0 (Upgrade from 1.0.0 to 2.0.0 is not supported.)	9.0 (9.0.4)	Latest	1.0.4	<p>Enables you to monitor and secure VMs or GKE clusters deployed in GCP.</p> <ul style="list-style-type: none"> • Deploy auto scaling for VM instance groups or GKE clusters using auto scaling templates for both firewall and application deployments. • VM Monitoring for GCP assets.

SD-WAN

The following table shows the features introduced in each version of the Panorama™ plugin for SD-WAN.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
3.1.2	11.0.2 (11.0.2)	Latest	Bug and performance fixes.
3.1.1	11.0.2 (11.0.2)	Latest	SD-WAN IPv6 Basic Connectivity
3.0.1-h6	11.0.1 (11.0.1)	Latest	Bug and performance fixes.
3.1.0-h6	11.0.0 (11.0.1)	Latest	Enables Advanced Routing Engine support.
3.0.5	10.2.5 (10.2.5)	Latest	Bug and performance fixes.
3.0.4	10.2.4 (10.2.4)	Latest	Bug and performance fixes.
3.0.3	10.2.1 (10.2.1)	Latest	Bug and performance fixes.
3.0.2	10.2.1 (10.2.1)	Latest	Bug and performance fixes.
3.0.1	10.2.1 (10.2.1)	Latest	Copy ToS Header Support.
3.0.0	10.2 (10.2.0)	Latest	Upgrade to the SD-WAN plugin to increase reliability. SD-WAN plugin 3.0 is required to upgrade to PAN-OS 10.2 and is supported only on PAN-OS 10.2 and later releases.
2.2.4	10.1.10 (10.1.10)	Latest	Bug and performance fixes.
2.2.3	10.1.9 (10.1.9)	Latest	Bug and performance fixes.
2.2.2	10.1.5-h1 (10.1.5-h1)	Latest	Bug and performance fixes.

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
2.2.1	10.1.5-h1 (10.1.5-h1)	Latest	Copy ToS Header support.
2.2.0	10.1.4 (10.1.4)	Latest	Prisma Access Hub support.
2.1.1	10.0 (10.0.4)	Latest	Minor bug and performance fixes.
2.1.0	10.0 (10.0.4)	Latest	SD-WAN supports Aggregated Ethernet (AE) interfaces with or without subinterfaces for link redundancy. AE interfaces allow you to tag for different ISP services to achieve end-to-end traffic segmentation. SD-WAN also supports Layer 3 subinterfaces for end-to-end traffic segmentation.
2.0.3	10.0 (10.0.3)	Latest	Minor bug and performance fixes.
2.0.2	10.0 (10.0.3)	Latest	Includes support so you can control whether Auto VPN configuration enables or disables the Remove Private AS setting for all BGP peer groups on a branch or hub.
2.0.1	10.0 (10.0.3)	Latest	Includes support for full mesh VPN cluster with DDNS service, auto-VPN configuration with branch behind NAT, and Direct Internet Access (DIA) AnyPath.
2.0.0	10.0 (10.0.2)	Latest	Maintain high-quality application experience by leveraging Forward

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			Error Correction (FEC) and packet duplication and by accurately measuring SaaS and Cloud applications when you have an SD-WAN firewall with Direct Internet Access (DIA) links.
1.0.6	9.1 (9.1.4)	Latest	Minor bug and performance fixes.
1.0.5	9.1 (9.1.4)	Latest	Minor bug and performance fixes.
1.0.4	9.1 (9.1.4)	Latest	In an SD-WAN VPN cluster that has more than one hub, you must assign a priority to each hub, which determines the primary hub and hub failover order. Panorama maps the priority to a BGP local preference and pushes the local preference to the branches in the cluster.
1.0.3	9.1 (9.1.3)	10.0.0	When the SD-WAN hub is behind a NAT device, the plugin supports an upstream NAT IP address or FQDN for Auto VPN configuration to use as a tunnel endpoint.
1.0.2	9.1 (9.1.2-h1)	9.1.3	Improves ease of use, such as an automatic Security policy rule to allow BGP between branches and hubs, ability to refresh the IKE preshared key for VPN cluster members, specifying VPN tunnel

Plugin Version	PAN-OS Version (Minimum)	Maximum PAN-OS Version	Features
			IP address ranges, and more.
1.0.1	9.1 (9.1.1)	9.1.2	Improves monitoring experience and search filtering, and adds an option to display HA peers consecutively.
1.0.0	9.1 (9.1.0)	9.1.2	Enables support for SD-WAN from Panorama. Configure the Panorama plugin for SD-WAN to provide intelligent and dynamic path selection on top of the industry-leading security that PAN-OS software already delivers. Provide the optimal end user experience by leveraging multiple ISP links to ensure application performance and scale capacity.

VMware NSX

The following table shows the features introduced in each version of the [VM-Series firewall VMware NSX](#) plugin. For additional information about each plugin, see the release notes on the [Customer Support Portal](#).



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM- Series PAN- OS Version (Minimum)	New Features or Changes
5.0.1	<ul style="list-style-type: none"> NSX-V: 10.2.0 (10.2.2) 	<ul style="list-style-type: none"> NSX-V: Latest 10.2.x (10.2.x) NSX-T N/S: Latest 10.2.x (10.2.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) 	Introduces support for PAN-OS and Panorama 10.2.x.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM-Series PAN-OS Version (Minimum)	New Features or Changes
	<ul style="list-style-type: none"> NSX-T N/S: 10.2.0 (10.2.2) NSX-T E/W: 10.2.0 (10.2.2) 	<ul style="list-style-type: none"> NSX-T E/W: Latest 10.2.x (10.2.x) 	<ul style="list-style-type: none"> NSX-T E/W: 9.1 (9.1.0) 	
5.0.0	<ul style="list-style-type: none"> NSX-V: 10.2.0 (10.2.2) NSX-T N/S: 10.2.0 (10.2.2) NSX-T E/W: 10.2.0 (10.2.2) 	<ul style="list-style-type: none"> NSX-V: Latest 10.2.x (10.2.x) NSX-T N/S: Latest 10.2.x (10.2.x) NSX-T E/W: Latest 10.2.x (10.2.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces support for PAN-OS and Panorama 10.2.x.
4.0.3	<ul style="list-style-type: none"> NSX-V: 10.0.0 (10.0.4) NSX-T N/S: 10.0.0 (10.0.4) NSX-T E/W: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces fixes for known issues.
4.0.2	<ul style="list-style-type: none"> NSX-V: 10.0.0 (10.0.4) NSX-T N/S: 10.0.0 (10.0.4) NSX-T E/W: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces fixes for known issues.
4.0.1	<ul style="list-style-type: none"> NSX-V: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) 	Introduces fixes for known issues.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM-Series PAN-OS Version (Minimum)	New Features or Changes
	<ul style="list-style-type: none"> NSX-T N/S: 10.0.0 (10.0.4) NSX-T E/W: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-T E/W: 9.1 (9.1.0) 	
4.0.0	<ul style="list-style-type: none"> NSX-V: 10.0.0 (10.0.4) NSX-T N/S: 10.0.0 (10.0.4) NSX-T E/W: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces Security-Centric Deployment Workflow (East-West) for the VM-Series on VMware NSX-T.
3.2.4	<ul style="list-style-type: none"> NSX-V: 10.0.0 (10.0.4) NSX-T N/S: 10.0.0 (10.0.4) NSX-T E/W: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces fixes for known issues.
3.2.3	<ul style="list-style-type: none"> NSX-V: 10.0.0 (10.0.4) NSX-T N/S: 10.0.0 (10.0.4) NSX-T E/W: 10.0.0 (10.0.4) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces fixes for known issues.
3.2.1	<ul style="list-style-type: none"> NSX-V: 9.0 (9.0.8) NSX-T N/S: 9.0 (9.0.8) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) 	Introduces fixes for known issues.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM-Series PAN-OS Version (Minimum)	New Features or Changes
	<ul style="list-style-type: none"> NSX-T E/W: 9.1 (9.1.0) 	<ul style="list-style-type: none"> NSX-T E/W: 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-T E/W: 9.1 (9.1.0) 	
3.2.0	<ul style="list-style-type: none"> NSX-V: 9.0 (9.0.8) NSX-T N/S: 9.0 (9.0.8) NSX-T E/W: 9.1 (9.1.0) 	<ul style="list-style-type: none"> NSX-V: 10.1.x (10.1.x) NSX-T N/S: Latest 10.1.x (10.1.x) NSX-T E/W: Latest 10.1.x (10.1.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	<p>Introduces Security Policy Extension Between NSX-V and NSX-T and Device Certificate Support on the VM-Series for NSX.</p> <p>The following VM-Series firewall for NSX OVF's require that you enable device certificates.</p> <ul style="list-style-type: none"> 10.0.1 or later 9.1.5 or later 9.0.11 or later 8.1.17 or later
3.1.0	9.1 (9.1.0)	<ul style="list-style-type: none"> NSX-V: Latest 10.0.x NSX-T N/S: Latest (10.2.x) NSX-T E/W: Latest (10.2.x) 	<ul style="list-style-type: none"> NSX-V: 8.1 (8.1.0) NSX-T N/S: 9.0 (9.0.4) NSX-T E/W: 9.1 (9.1.0) 	Introduces the VM-Series firewall on VMware NSX-T for East-West traffic protection.
2.0.6	8.1 (8.1.0)	9.0.x	8.1 (8.1.0)	Introduces fixes for known issues.
2.0.5	8.1 (8.1.0)	9.0.x	8.1 (8.1.0)	Introduces Proxy Bypass Support and Curl Call Timeout features.

Plugin Version	Panorama Version (Minimum)	Panorama Version (Maximum)	Managed VM-Series PAN-OS Version (Minimum)	New Features or Changes
2.0.4	8.1 (8.1.0)	9.0.x	8.1 (8.1.0)	Introduces the Automated Full Dynamic Address Group Sync feature.
2.0.3	8.1 (8.1.0)	9.0.x	8.1 (8.1.0)	Introduces fixes for known issues.
2.0.2	8.1 (8.1.0)	9.0.x	8.1 (8.1.0)	Introduces fixes for known issues.
2.0.1	8.1 (8.1.0)	9.0.x	8.1 (8.1.0)	Introduces fixes for known issues. Minimum required plugin version for Panorama 8.1.

VMware vCenter

The following table shows the features introduced in each version of the Panorama™ plugin for VMware vCenter.



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
2.1.0	10.2 (10.2.0)	Latest	Introduces fixes for known issues.
2.0.0	10.2 (10.2.0)	Latest	Introduces enhancements to increase reliability and robustness.
1.0.0	9.0 (9.0.2)	Latest	Enables support for VM Monitoring from Panorama. Configure

Plugin Version	Panorama PAN-OS Version (Minimum)	Maximum Panorama PAN-OS Version	Features
			the Panorama plugin for VMware vCenter to monitor VM workloads so that you can consistently enforce security policy that automatically adapts to changes within your vCenter environment.

Zero Touch Provisioning (ZTP)

The following table shows the features introduced in each version of the Panorama™ plugin for Zero Touch Provisioning (ZTP).



End-of-life (EoL) software versions are included in this table. Review the [Software End-of-Life Summary website](#) to check whether we are still supporting your software version.

Plugin Version	PAN-OS Version Minimum	Maximum PAN-OS Version	Features
2.0.3	10.2.4 (PAN-OS 10.2 release) 11.0.1 (PAN-OS 11.0 release)	Latest	Minor bug and performance fixes.
2.0.2	10.2.0	Latest	Minor bug and performance fixes.
2.0.1	10.2.0	Latest	Minor bug and performance fixes.
2.0.0	10.2.0	Latest	Upgrade to the ZTP plugin to increase reliability. ZTP plugin 2.0 is required to upgrade to PAN-OS 10.2 and is supported only on PAN-OS 10.2 and later releases.
1.0.2	10.0.3	Latest	Minor bug and performance fixes.

Plugin Version	PAN-OS Version Minimum	Maximum PAN-OS Version	Features
1.0.1	10.0.3	Latest	Minor bug and performance fixes.
1.0.0	9.1.4	Latest	Enables support for ZTP from Panorama. Configure the Panorama plugin for ZTP to simplify and streamline initial firewall deployment by automating the new managed firewall on-boarding without the need for network administrators to manually provision the firewall.

Compatible Plugin Versions for PAN-OS 10.2

To increase reliability and robustness, we enhanced PAN-OS® software starting in PAN-OS® 10.2 with upgraded Panorama™ plugins and by installing the VM-Series plugin by default. However, we did not introduce support for all plugins with the initial release of PAN-OS 10.2.0. Use the following table to determine the minimum plugin versions for use with PAN-OS 10.2 software and, where applicable, the first PAN-OS 10.2 version that supports each plugin. (If no PAN-OS 10.2 version is specified, then the minimum version of the plugin is supported in all PAN-OS 10.2 versions.)



For more information about plugins compatible with PAN-OS 10.2—and all other supported PAN-OS releases, refer to the [Panorama Plugins page](#).

Plugin Name	Minimum Compatible Plugin Version with PAN-OS 10.2
AWS plugin	4.0.0
AIOps for NGFW plugin	1.0.0
Azure plugin	4.0.0
Cloud Services plugin (for use with Cortex Data Lake only)	3.1 (Compatible with PAN-OS 10.2.1 and later)
Cloud Services plugin (for use with Panorama Managed Prisma Access)	<ul style="list-style-type: none"> 3.2 (compatible with PAN-OS 10.2.3 and later PAN-OS 10.2 versions) 3.1 starting with version 3.1.0-h50 (compatible with PAN-OS 10.2.2-h1 and later PAN-OS 10.2 versions) <p>IMPORTANT: Review the PAN-OS and Prisma Access Known Issues that are applicable to Panorama deployments running PAN-OS 10.2.2 with Prisma Access 3.1.</p>
Kubernetes plugin	3.0.0
SW FW Licensing plugin (VM licensing plugin is not a Python-based plugin and the previous version is supported)	1.0.0
Panorama VM-Series plugin	3.0.0
SD-WAN plugin	3.0.0
IPS Signature Converter plugin	2.0.0
ZTP plugin	2.0.0

Plugin Name	Minimum Compatible Plugin Version with PAN-OS 10.2
DLP plugin	3.0.0
OpenConfig plugin	1.1.0
GCP plugin	3.0.0
Cisco ACI plugin	3.0.0
VCenter plugin	2.0.0
Nutanix plugin	2.0.0
Cisco TrustSec plugin	2.0.0



Important considerations for upgrading your plugins



- The plugin versions listed in the above table are the only plugins compatible with PAN-OS 10.2 and later PAN-OS 10.2 versions. If you use any other plugins, you should not upgrade to PAN-OS 10.2 until you upgrade all of your plugins to the minimum supported version for PAN-OS 10.2.
- Starting with PAN-OS 10.2, the VM-Series plugin is installed by default. This option is currently available only in PAN-OS 10.2, which means that Panorama software requires that you download a compatible version of the VM-Series plugin if you downgrade your firewall from PAN-OS 10.2 to a PAN-OS 10.1 or earlier version.



Each upgraded Panorama plugin supports any supported PAN-OS release in addition to PAN-OS 10.2.

Supported Migration Paths for Plugins

Plugin Name	Upgrade/Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN-OS Version	Target Plugin Version
AWS	Upgrade	10.1.x	3.0.x	10.2.0	4.0.0

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN- OS Version	Target Plugin Version
			 You should upgrade AWS plugin 2.x.x to 3.0.x in PAN-OS 10.1.x version before you upgrade to PAN-OS 10.2.		
	Downgrade	10.2.0	4.0.0	10.1.x	3.0.x
Azure plugin	Upgrade	10.1.x	3.1.x	10.2.0	4.0.0
	Downgrade	10.2.0	4.0.0	10.1.x	3.2.X (yet to be released)  Downgrading is not possible until Azure plugin 3.2.x is released.
Kubernetes plugin	Upgrade	10.1.x	2.0.x	10.2.0	3.0.0
	Downgrade	10.2.0	3.0.0	10.1.x	2.0.x

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN- OS Version	Target Plugin Version
					<div> If you have a custom certificate size greater than 32k, the autocommit (which happens after downgrade) will fail. To avoid this, save the config file, add a dummy value in the custom certificate that is less than 16K, and then downgrade to 2.0.x (k8s plugin cannot contact the API server). Then upgrade the</div>

Plugin Name	Upgrade/ Downgrade	Base PAN-OS Version	Base Plugin Version	Target PAN- OS Version	Target Plugin Version
GCP plugin	Upgrade	10.1.x	2.0.0	10.2.0	3.0.0
	Downgrade	10.2.0	3.0.0	10.1.x	2.0.0
Cisco ACI plugin	Upgrade	10.1.x	2.0.x	10.2.0	3.0.0
	Downgrade	10.2.0	3.0.0	10.1.x	2.0.x
VCenter plugin	Upgrade	10.1.x	1.0.x	10.2.0	2.0.0
	Downgrade	10.2.0	2.0.0	10.1.x	1.0.x
Nutanix plugin	Upgrade	10.1.x	1.0.0	10.2.0	2.0.0
	Downgrade	10.2.0	2.0.0	10.1.x	1.0.0

For more information, review how to:

[Upgrade PAN-OS.](#)

[Upgrade Panorama Plugins.](#)

Panorama Management Compatibility

Review the table below to understand which Palo Alto Networks Next-Generation Firewall, Dedicated Log Collector, and WildFire® appliances a Panorama™ management server can manage based on the installed PAN-OS version. Palo Alto Networks recommends management of currently supported [Palo Alto Networks Next-Generation Firewalls](#), Dedicated Log collector, and WildFire appliance running a supported PAN-OS version.

Dedicated Log Collectors must be running the same or later PAN-OS version than managed firewalls from which logs are forwarded. Palo Alto Networks does not support forwarding logs from managed firewalls to a Dedicated Log Collector if the Dedicated Log Collector is running an earlier PAN-OS version than that installed on your managed firewalls. This may lead to log forwarding and ingestion issues.

([PAN-OS 10.1.2 and earlier PAN-OS 10.1 releases](#)) The [device registration authentication key](#) length is increased when you upgrade Panorama to PAN-OS 10.1.3 or later release:

- **Panorama running PAN-OS 10.1.2 or earlier PAN-OS 10.1 releases**— Supports onboarding [firewalls](#), [Dedicated Log Collectors](#), and [WildFire appliances](#) running PAN-OS 10.1.2 or earlier PAN-OS 10.1 release, or running PAN-OS 10.0 or earlier PAN-OS release.
- **Panorama running PAN-OS 10.1.3 or later releases**— Supports onboarding [firewalls](#), [Dedicated Log Collectors](#), and [WildFire appliances](#) running PAN-OS 10.1.3 or later release, or running PAN-OS 10.0 or earlier PAN-OS release.

Despite these onboarding requirements, Panorama supports managing firewalls, Dedicated Log Collectors, and WildFire appliances running the PAN-OS versions described below.



PAN-OS software versions that are [End-of-Life \(EoL\)](#) are not displayed. See the [Palo Alto Networks End of Life Announcements](#) for additional information. EoL PAN-OS versions are supported only for [End-of-Sale \(EoS\)](#) firewall models until they reach EoL.

Management of [End-of-Life \(EoL\)](#) PAN-OS versions may result in unexpected issues, particularly if there is a large gap between the PAN-OS version installed on Panorama and the one installed on the firewall. For example, you may run into unexpected or unknown issues if you attempt to manage a firewall running the EoL PAN-OS 7.1 release from a Panorama running PAN-OS 10.2 or later release.

Panorama Version	Managed Device Version
11.0	11.0
	10.2
	10.1
	9.1
	8.1 (EoS firewalls only)
10.2	10.2
	10.1

Panorama Version	Managed Device Version
	9.1
	8.1 (EoS firewalls only)
10.1	10.1
	9.1
	8.1 (EoS firewalls only)
9.1	9.1
	8.1 (EoS firewalls only)

Panorama Hypervisor Support

Before you deploy a Panorama™ virtual appliance, verify that the hypervisor meets the minimum version requirements to deploy Panorama.

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
PAN-OS 11.0 and PAN-OS 10.2	64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, or 7.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-10. ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.	<ul style="list-style-type: none"> • Ubuntu 18.04 • Ubuntu 16.04 • CentOS/ RHEL 7 • CentOS/ RHEL 8 	<ul style="list-style-type: none"> • Windows Server 2019 with Hyper-V role or Hyper-V 2019 • Windows Server 2016 with Hyper-V role or Hyper-V 2016 	Nutanix AOS Version— 5.10 and later Nutanix AHV Version— 20170830.185 To manage VM-Series firewalls running supported versions of AHV. See VM-Series for Nutanix .	<ul style="list-style-type: none"> • Alibaba Cloud • Amazon AWS • Microsoft Azure • Google Cloud Platform • Amazon AWS GovCloud • Oracle Cloud Infrastructure (OCI)
PAN-OS 10.1	64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, or	<ul style="list-style-type: none"> • Ubuntu 18.04 • Ubuntu 16.04 	<ul style="list-style-type: none"> • Windows Server 2019 with Hyper-V role or 	Nutanix AOS Version— 5.10 and later	<ul style="list-style-type: none"> • Alibaba Cloud • Amazon AWS

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
	<p>7.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on the ESXi server is vmx-10.</p> <p>ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.</p>	<ul style="list-style-type: none"> CentOS/ RHEL 7 CentOS/ RHEL 8 	<p>Hyper-V 2019</p> <ul style="list-style-type: none"> Windows Server 2016 with Hyper-V role or Hyper-V 2016 	<p>Nutanix AHV Version— 20170830.185</p> <p>To manage VM-Series firewalls running supported versions of AHV. See VM-Series for Nutanix.</p>	<ul style="list-style-type: none"> Microsoft Azure Google Cloud Platform Amazon AWS GovCloud Oracle Cloud Infrastructure (OCI)
PAN-OS 9.1	<p>64-bit kernel-based VMware ESXi 6.0, 6.5, 6.7, or 7.0. The supported version of the virtual hardware family type (also known as the VMware virtual hardware version) on</p>	<ul style="list-style-type: none"> Ubuntu 18.04 Ubuntu 16.04 CentOS/ RHEL 7 CentOS/ RHEL 8 	<ul style="list-style-type: none"> Windows Server 2019 with Hyper-V role or Hyper-V 2019 Windows Server 2016 with Hyper-V role or Hyper-V 2016 	<p>Nutanix AOS Version— 5.10 and later</p> <p>Nutanix AHV Version— 20170830.185</p> <p>To manage VM-Series firewalls running supported versions of AHV. See</p>	<ul style="list-style-type: none"> Amazon AWS Microsoft Azure Google Cloud Platform Amazon AWS GovCloud

Panorama Version	VMware ESXi Compatibility	KVM Compatibility	Hyper-V Compatibility	Nutanix AHV Compatibility	Public Cloud/ Partner Integra Compatibility
	the ESXi server is vmx-10. ESXi 6.0 and later versions supports one disk of up to 8TB. Earlier ESXi versions support one disk of up to 2TB.			VM-Series for Nutanix.	

Device Certificate for a Palo Alto Networks Cloud Service

A Palo Alto Networks cloud service is a cloud-hosted service maintained and operated by Palo Alto Networks.

The device certificate must be installed on the firewall, Panorama, and WildFire appliance using the cloud service that is running one of the following releases:

- PAN-OS 11.0.2 or later releases
- PAN-OS 10.2.5 or later releases
- PAN-OS 10.1.10 or late releases
- (EoL) PAN-OS 10.0.5 or later 10.0 releases
- PAN-OS 9.1.8 or later 9.1 releases
- (EoL) PAN-OS 9.0.14 or later 9.0 releases
- (EoL) PAN-OS 8.1.19 or later 8.1 releases

Review the Palo Alto Networks cloud services listed below that require you install a device certificate to function. Panorama management of firewalls, Dedicated Log Collectors, and WildFire appliances, and downloading content and software updates from the Palo Alto Networks Update Server does not require a device certificate. Additionally, communication between a firewall and the WildFire appliance does not require a device certificate.

Cloud Service	Firewall (Individual and Panorama-Managed)	Panorama
AI Ops	Yes	Yes
App-ID Cloud Engine (ACE)	Yes	Yes
Cloud Services (Prisma Access)	N/A	No
Cortex Data Lake	(PAN-OS 10.1 and later) Yes	(PAN-OS 10.1 and later) Yes
Device Telemetry	Yes	Yes
Enterprise DLP	Yes	Yes
Inline Categorization Requires Advanced URL Filtering license	Yes	No

Cloud Service	Firewall (Individual and Panorama-Managed)	Panorama
Inline Cloud Analysis Requires Advanced Threat Protection license	Yes	No
Internet of Things (IoT) security	Yes	Yes
ZTP	No	Yes

MFA Vendor Support

- [MFA Vendor Support](#)

MFA Vendor Support

Palo Alto Networks Next-Generation Firewalls and Panorama™ appliances can integrate with multi-factor authentication (MFA) vendors using RADIUS and SAML. Firewalls can additionally integrate with specific MFA vendors using the API to enforce MFA through Authentication policy.

Authentication Use Case	RADIUS (any vendor)	TACACS + (any vendor)	SAML (any vendor)	MFA Server Profile
Next-Generation Firewall and Panorama Administrator Web Interface	✓	✓	✓	—
Next-Generation Firewall and Panorama Administrator CLI	✓	✓	—	—
GlobalProtect™ Portal and Gateway Authentication	✓	✓	✓	—
Authentication Policy (Formerly Captive Portal Policy)	✓	✓	✓	✓ Vendor / Min. Content Version * <ul style="list-style-type: none"> • RSA SecurID Access / 752 • PingID / 655 • Okta Adaptive / 655 • Duo v2 / 655



* Palo Alto Networks provides support for MFA vendors through Applications content updates, which means that if you use Panorama to push device group configurations to firewalls, you must [install the same Applications release version](#) on managed firewalls as you install on Panorama to avoid mismatches in vendor support.

Supported Cipher Suites

Use this table in the Palo Alto Networks Compatibility Matrix to determine support for cipher suites according to function and PAN-OS® software release.

- [Cloud Identity Engine Cipher Suites](#)
- [Cipher Suites Supported in PAN-OS 11.0](#)
- [Cipher Suites Supported in PAN-OS 10.2](#)
- [Cipher Suites Supported in PAN-OS 10.1](#)
- [Cipher Suites Supported in PAN-OS 9.1](#)
- [Cipher Suites Supported in PAN-OS 8.1](#)

Cloud Identity Engine Cipher Suites

The following cipher suites are supported and required on the Cloud Identity Engine agent host for on-premises directories.

Feature or Function	Required Ciphers
Cloud Identity Engine agent	<ul style="list-style-type: none">• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256• TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Cipher Suites Supported in PAN-OS 11.0

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- [PAN-OS 11.0 GlobalProtect Cipher Suites](#)
- [PAN-OS 11.0 IPsec Cipher Suites](#)
- [PAN-OS 11.0 IKE and Web Certificate Cipher Suites](#)
- [PAN-OS 11.0 Decryption Cipher Suites](#)
- [PAN-OS 11.0 HA1 SSH Cipher Suites](#)
- [PAN-OS 11.0 Administrative Session Cipher Suites](#)
- [PAN-OS 11.0 PAN-OS-to-Panorama Connection Cipher Suites](#)

PAN-OS 11.0 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

- [GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal](#)
- [GlobalProtect App/Agent—IPsec mode](#)
- [GlobalProtect Portal—Browser Access](#)

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	<ul style="list-style-type: none"> • TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	<ul style="list-style-type: none"> • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	<ul style="list-style-type: none"> • AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	<ul style="list-style-type: none"> • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 11.0 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

- [#unique_96/unique_96_Connect_42_id17C8F0X0MAW](#)
- [#unique_96/unique_96_Connect_42_id17C8F0YG02K](#)
- [#unique_96/unique_96_Connect_42_id17C8F0Z06X7](#)

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
IPSec—Encryption	<ul style="list-style-type: none"> • NULL • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	<ul style="list-style-type: none"> • NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	<ul style="list-style-type: none"> • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled • Group 21 (512-bit random elliptic curve group)

PAN-OS 11.0 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 11.0 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

- [IKE Certificate Support](#)
- [IKE—Encryption](#)
- [IKE—Message Authentication](#)
- [IKE—Key Exchange](#)
- [PAN-OS Web Certificates](#)

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
IKE Certificate Support	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
IKE—Encryption	<ul style="list-style-type: none"> • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC <p>Starting with PAN-OS 10.0.3:</p> <ul style="list-style-type: none"> • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	<ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	<p>Diffie-Hellman groups</p> <ul style="list-style-type: none"> • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group) • Group 21 (512-bit random elliptic curve group)
PAN-OS Web Certificates	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—2048-bit, 3072-bit, and 4096-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 11.0 Decryption Cipher Suites


The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

- [SSH Decryption \(SSHv2 only\)—Encryption](#)
- [SSH Decryption \(SSHv2 only\)—Message Authentication](#)
- [SSL/TLS Decryption](#)
- [SSL/TLS Decryption—NIST-approved Elliptical Curves](#)
- [SSL/TLS Decryption—Perfect Forward Secrecy \(PFS\) Ciphers](#)
- [TLS 1.3 Decryption—Signature Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
SSH Decryption (SSHv2 only)—Encryption	<ul style="list-style-type: none"> • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	<ul style="list-style-type: none"> • HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys <div> The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys. </div> <ul style="list-style-type: none"> • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	<ul style="list-style-type: none"> • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption—NIST-approved Elliptical Curves	<ul style="list-style-type: none"> • P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers  <i>If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.</i>	<ul style="list-style-type: none"> • DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	<ul style="list-style-type: none"> • ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1


PAN-OS 11.0 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

- [Administrative Sessions to Web Interface](#)
- [Administrative Sessions to CLI \(SSH\)—Encryption](#)
- [Administrative Sessions to CLI \(SSH\)—Message Authentication](#)
- [Administrative Sessions to CLI \(SSH\)—Server Host Key Types](#)
- [Administrative Sessions to CLI \(SSH\)—Key Exchange Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
Administrative Sessions to Web Interface	<p>TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites</p> <p> <i>TLSv1.3 cipher suites begin with “TLS”.</i></p> <ul style="list-style-type: none"> • RSA-SEED-SHA1 • RSA-CAMELLIA-128-SHA1 • RSA-CAMELLIA-256-SHA1 • RSA-AES-128-SHA1

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
	<ul style="list-style-type: none"> • RSA-AES-256-SHA1 • RSA-AES-256-CBC-SHA1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA1 • ECDHE-ECDSA-AES-256-SHA1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • TLS-AES-128-CCM-SHA256 • TLS-AES-128-GCM-SHA256 • TLS-AES-256-GCM-SHA384 • TLS-CHACHA20-POLY1305-SHA256
Administrative Sessions to CLI (SSH)—Encryption	<ul style="list-style-type: none"> • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	<ul style="list-style-type: none"> • UMAC-64 • UMAC-128 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-SHA-384 • HMAC-SHA2-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	<ul style="list-style-type: none"> • RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	<ul style="list-style-type: none"> • curve25519-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group14-sha384 • diffie-hellman-group16-sha512 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521

PAN-OS 11.0 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 11.0 release in normal (non-FIPS-CC) or FIPS-CC operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
HA1 SSH	<ul style="list-style-type: none"> • AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 11.0 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 11.0 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 11.0 Releases
PAN-OS to Panorama Connection	<ul style="list-style-type: none"> • RSA-RC4-128-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 11.0 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 11.0 release in FIPS-CC mode. The [Cryptographic Algorithm Validation Program](#) has additional details regarding the algorithm implementation.



If your firewall is running in normal (non-FIPS-CC) operational mode, see [Cipher Suites Supported in PAN-OS 11.0](#)

Functions	Standards	Certificates
Asymmetric key generation		
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: #A3453 VMs: #A3454
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: #A3453 VMs: #A3454
Cryptographic Key Generation (for IKE Peer Authentication)		

Functions	Standards	Certificates
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: #A3453 VMs: #A3454
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: #A3453 VMs: #A3454
Cryptographic Key Establishment		
ECC-based key establishment	SP 800-56A Revision 3	Appliances: #A3453 VMs: #A3454
FFC-based key establishment	SP 800-56A Revision 3	Appliances: #A3453 VMs: #A3454
AES Data Encryption/Decryption		
<ul style="list-style-type: none"> • AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128 	<ul style="list-style-type: none"> • AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197 	Appliances: #A3453 VMs: #A3454
Signature Generation and Verification		
RSA (2048 bits or greater)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5,	Appliances: #A3453

Functions	Standards	Certificates
	using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	VMs: #A3454
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	Appliances: #A3453 VMs: #A3454
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	Appliances: #A3453 VMs: #A3454
Keyed-hash message authentication		
<ul style="list-style-type: none"> • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 	ISO/IEC 9797-2:2011 FIPS PUB 198-1	Appliances: #A3453 VMs: #A3454
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	Appliances: #A3453 VMs: #A3454

Cipher Suites Supported in PAN-OS 10.2

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- [PAN-OS 10.2 GlobalProtect Cipher Suites](#)
- [PAN-OS 10.2 IPsec Cipher Suites](#)
- [PAN-OS 10.2 IKE and Web Certificate Cipher Suites](#)
- [PAN-OS 10.2 Decryption Cipher Suites](#)
- [PAN-OS 10.2 HA1 SSH Cipher Suites](#)
- [PAN-OS 10.2 Administrative Session Cipher Suites](#)
- [PAN-OS 10.2 PAN-OS-to-Panorama Connection Cipher Suites](#)

PAN-OS 10.2 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

- [GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal](#)
- [GlobalProtect App/Agent—IPsec mode](#)
- [GlobalProtect Portal—Browser Access](#)

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	<ul style="list-style-type: none"> • TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	<ul style="list-style-type: none"> • AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 10.2 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

- [IPSec—Encryption](#)
- [IPSec—Message Authentication](#)
- [IPSec—Key Exchange](#)

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
IPSec—Encryption	<ul style="list-style-type: none"> • NULL • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	<ul style="list-style-type: none"> • NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled • Group 21 (512-bit random elliptic curve group)

PAN-OS 10.2 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 10.2 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

- [IKE Certificate Support](#)
- [IKE—Encryption](#)
- [IKE—Message Authentication](#)
- [IKE—Key Exchange](#)
- [PAN-OS Web Certificates](#)

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
IKE Certificate Support	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
IKE—Encryption	<ul style="list-style-type: none"> • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC <p>Starting with PAN-OS 10.0.3:</p> <ul style="list-style-type: none"> • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	<ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	<p>Diffie-Hellman groups</p> <ul style="list-style-type: none"> • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 15 (3072-bit modular exponential group) • Group 16 (4096-bit modular exponential group) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group) • Group 21 (512-bit random elliptic curve group)
PAN-OS Web Certificates	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—2048-bit, 3072-bit, and 4096-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 10.2 Decryption Cipher Suites


The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

- [SSH Decryption \(SSHv2 only\)—Encryption](#)
- [SSH Decryption \(SSHv2 only\)—Message Authentication](#)
- [SSL/TLS Decryption](#)
- [SSL/TLS Decryption—NIST-approved Elliptical Curves](#)
- [SSL/TLS Decryption—Perfect Forward Secrecy \(PFS\) Ciphers](#)
- [TLS 1.3 Decryption—Signature Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
SSH Decryption (SSHv2 only)—Encryption	<ul style="list-style-type: none"> • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	<ul style="list-style-type: none"> • HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys <div> <p>The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.</p> </div> <ul style="list-style-type: none"> • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384 • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption—NIST-approved Elliptical Curves	<ul style="list-style-type: none"> • P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers  <i>If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.</i>	<ul style="list-style-type: none"> • DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption—Signature Algorithms	<ul style="list-style-type: none"> • ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256 • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 10.2 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

- [Administrative Sessions to Web Interface](#)
- [Administrative Sessions to CLI \(SSH\)—Encryption](#)
- [Administrative Sessions to CLI \(SSH\)—Message Authentication](#)
- [Administrative Sessions to CLI \(SSH\)—Server Host Key Types](#)
- [Administrative Sessions to CLI \(SSH\)—Key Exchange Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
Administrative Sessions to Web Interface	<ul style="list-style-type: none"> • TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA1 • RSA-CAMELLIA-128-SHA1 • RSA-CAMELLIA-256-SHA1 • RSA-AES-128-SHA1 • RSA-AES-256-SHA1 • RSA-AES-256-CBC-SHA1

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA1 • ECDHE-ECDSA-AES-256-SHA1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	<ul style="list-style-type: none"> • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	<ul style="list-style-type: none"> • UMAC-64 • UMAC-128 • HMAC-SHA1 • HMAC-SHA2-256 • HMAC-SHA2-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	<ul style="list-style-type: none"> • RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	<ul style="list-style-type: none"> • curve25519-sha256 • diffie-hellman-group14-sha1 • diffie-hellman-group14-sha256 • diffie-hellman-group16-sha512 • diffie-hellman-group-exchange-sha256 • ecdh-sha2-nistp256 • ecdh-sha2-nistp384

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> ecdh-sha2-nistp521

PAN-OS 10.2 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 10.2 release in normal (non-FIPS-CC) or FIPS-CC operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
HA1 SSH	<ul style="list-style-type: none"> AES 128-bit cipher with Counter Mode AES 128-bit cipher with GCM (Galois/Counter Mode) AES 192-bit cipher with Counter Mode AES 256-bit cipher with Counter Mode AES 256-bit cipher with GCM CHACHA20-POLY1305

PAN-OS 10.2 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 10.2 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
PAN-OS to Panorama Connection	<ul style="list-style-type: none"> RSA-RC4-128-SHA-1 RSA-SEED-SHA-1 RSA-CAMELLIA-128-SHA-1 RSA-CAMELLIA-256-SHA-1 RSA-AES-128-SHA-1 RSA-AES-128-SHA-256 RSA-AES-256-SHA-1 RSA-AES-256-SHA-256 RSA-AES-128-GCM-SHA-256 RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.2 Releases
	<ul style="list-style-type: none"> DHE-RSA-AES-128-SHA-1 DHE-RSA-AES-256-SHA-1

PAN-OS 10.2 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 10.2 release in FIPS-CC mode. The [Cryptographic Algorithm Validation Program](#) has additional details regarding the algorithm implementation.



If your firewall is running in normal (non-FIPS-CC) operational mode, see [Cipher Suites Supported in PAN-OS 10.2](#)

Functions	Standards	Certificates
Asymmetric key generation		
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	Appliances: #A2906 VMs: #A2907
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: #A2906 VMs: #A2907
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: #A2906 VMs: #A2907
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: #A2906 VMs: #A2907

Functions	Standards	Certificates
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: #A2906 VMs: #A2907
Cryptographic Key Establishment		
ECC-based key establishment	SP 800-56A Revision 3	Appliances: #A2906 VMs: #A2907
FFC-based key establishment	SP 800-56A Revision 3	Appliances: #A2906 VMs: #A2907
AES Data Encryption/Decryption		
<ul style="list-style-type: none"> • AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128 	<ul style="list-style-type: none"> • AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197 	Appliances: #A2906 VMs: #A2907
Signature Generation and Verification		
RSA (2048 bits or greater)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2	Appliances: #A2906 VMs: #A2907

Functions	Standards	Certificates
	or Digital Signature scheme 3	
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	Appliances: #A2906 VMs: #A2907
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	Appliances: #A2906 VMs: #A2907
Keyed-hash message authentication		
<ul style="list-style-type: none"> • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 	ISO/IEC 9797-2:2011 FIPS PUB 198-1	Appliances: #A2906 VMs: #A2907
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	Appliances: #A2906 VMs: #A2907

Cipher Suites Supported in PAN-OS 10.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- [PAN-OS 10.1 GlobalProtect Cipher Suites](#)
- [PAN-OS 10.1 IPSec Cipher Suites](#)
- [PAN-OS 10.1 IKE and Web Certificate Cipher Suites](#)
- [PAN-OS 10.1 Decryption Cipher Suites](#)
- [PAN-OS 10.1 HA1 SSH Cipher Suites](#)
- [PAN-OS 10.1 Administrative Session Cipher Suites](#)
- [PAN-OS 10.1 PAN-OS-to-Panorama Connection Cipher Suites](#)

PAN-OS 10.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal](#)
- [GlobalProtect App/Agent—IPSec mode](#)
- [GlobalProtect Portal—Browser Access](#)

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	<ul style="list-style-type: none"> • TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	<ul style="list-style-type: none"> • AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 10.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [IPSec—Encryption](#)
- [IPSec—Message Authentication](#)
- [IPSec—Key Exchange](#)

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
IPSec—Encryption	<ul style="list-style-type: none"> • NULL • DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	<ul style="list-style-type: none"> • NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 10.1 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 10.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [IKE Certificate Support](#)
- [IKE—Encryption](#)
- [IKE—Message Authentication](#)
- [IKE—Key Exchange](#)
- [PAN-OS Web Certificates](#)

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
IKE Certificate Support	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512
IKE—Encryption	<ul style="list-style-type: none"> • DES • 3DES • AES-128-CBC

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • AES-192-CBC • AES-256-CBC <p>Starting with PAN-OS 10.0.3:</p> <ul style="list-style-type: none"> • AES-128-GCM • AES-256-GCM
IKE—Message Authentication	<ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	<p>Diffie-Hellman groups</p> <ul style="list-style-type: none"> • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group)
PAN-OS Web Certificates	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, 3072-bit, and 4096-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 10.1 Decryption Cipher Suites


The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.




If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [SSH Decryption \(SSHv2 only\)—Encryption](#)

- [SSH Decryption \(SSHv2 only\)—Message Authentication](#)
- [SSL/TLS Decryption](#)
- [SSL/TLS Decryption—NIST-approved Elliptical Curves](#)
- [SSL/TLS Decryption—Perfect Forward Secrecy \(PFS\) Ciphers](#)
- [TLS 1.3 Decryption—Signature Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
SSH Decryption (SSHv2 only)—Encryption	<ul style="list-style-type: none"> • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	<ul style="list-style-type: none"> • HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, and TLSv1.3 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys <p> <i>The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.</i></p> <ul style="list-style-type: none"> • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • TLS_AES_256_GCM_SHA-384

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • TLS_CHACHA20_POLY1305_SHA-256 • TLS_AES_128_GCM_SHA-256
SSL/TLS Decryption— NIST-approved Elliptical Curves	<ul style="list-style-type: none"> • P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1) • P-521 (secp521r1) • (TLS 1.3 only) X25519 • (TLS 1.3 only) X448
SSL/TLS Decryption— Perfect Forward Secrecy (PFS) Ciphers  <i>If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.</i>	<ul style="list-style-type: none"> • DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384 • (TLS 1.3 only) TLS_AES_128_GCM_SHA-256 • (TLS 1.3 only) TLS_AES_256_GCM_SHA-384 • (TLS 1.3 only) TLS_CHACHA20_POLY1305_SHA-256
TLS 1.3 Decryption— Signature Algorithms	<ul style="list-style-type: none"> • ECDSA-SECP256r1-SHA-256 • RSA-PSS-RSAE-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • RSA-PKCS1-SHA-256 • ECDSA-SECP384r1-SHA-384 • RSA-PSS-RSAE-SHA-384 • RSA-PKCS1-SHA-386 • RSA-PSS-RSAE-SHA-512 • RSA-PKCS1-SHA-512 • RSA-PKCS1-SHA-1

PAN-OS 10.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [Administrative Sessions to Web Interface](#)
- [Administrative Sessions to CLI \(SSH\)—Encryption](#)
- [Administrative Sessions to CLI \(SSH\)—Message Authentication](#)
- [Administrative Sessions to CLI \(SSH\)—Server Host Key Types](#)
- [Administrative Sessions to CLI \(SSH\)—Key Exchange Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
Administrative Sessions to Web Interface	<ul style="list-style-type: none"> • TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-3DES-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
	<ul style="list-style-type: none"> • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	<ul style="list-style-type: none"> • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM • CHACHA20-POLY1305
Administrative Sessions to CLI (SSH)—Message Authentication	<ul style="list-style-type: none"> • UMAC-64 • UMAC-128 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	<ul style="list-style-type: none"> • RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	<ul style="list-style-type: none"> • curve25519-SHA-256 • diffie-hellman-group14-SHA-1 • diffie-hellman-group14-SHA-256 • diffie-hellman-group16-SHA-512 • diffie-hellman-group-exchange-SHA-256 • ecdh-SHA-2-nistp256 • ecdh-SHA-2-nistp384 • ecdh-SHA-2-nistp521

PAN-OS 10.1 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 10.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
HA1 SSH	<ul style="list-style-type: none"> • AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM • CHACHA20-POLY1305

PAN-OS 10.1 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 10.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 10.1 Releases
PAN-OS to Panorama Connection	<ul style="list-style-type: none"> • RSA-RC4-128-SHA-1 • RSA-3DES-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 10.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 10.1 release in FIPS-CC mode. The [Cryptographic Algorithm Validation Program](#) has additional details regarding the algorithm implementation.



If your firewall is running in normal (non-FIPS-CC) operational mode, see [Cipher Suites Supported in PAN-OS 10.1](#)

Functions	Standards	Certificates
Asymmetric key generation		
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	Appliances: #A2137 VMs: #A2244
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: #A2137 VMs: #A2244
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: #A2137 VMs: #A2244
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: #A2137 VMs: #A2244
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: #A2137 VMs: #A2244
Cryptographic Key Establishment		
ECDSA-based key establishment	NIST SP 800-56A Revision 2	Appliances: #A2137 VMs:

Functions	Standards	Certificates
		#A2244
FFC-based key establishment	NIST SP 800-56A Revision 2	Appliances: #A2137 VMs: #A2244
AES Data Encryption/Decryption		
<ul style="list-style-type: none"> • AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128 	<ul style="list-style-type: none"> • AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197 	Appliances: #A2137 VMs: #A2244
Signature Generation and Verification		
RSA Digital Signature Algorithm (rDSA) (2048 bits or greater)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Appliances: #A2137 VMs: #A2244
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, P-521 ISO/IEC 14888-3, Section 6.4	Appliances: #A2137 VMs: #A2244

Functions	Standards	Certificates
Cryptographic hashing		
SHA-1, SHA-256, SHA-384 and SHA-512 (digest sizes 160, 256, 384 and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	Appliances: #A2137 VMs: #A2244
Keyed-hash message authentication		
<ul style="list-style-type: none"> • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 	ISO/IEC 9797-2:2011 FIPS PUB 198-1	Appliances: #A2137 VMs: #A2244
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	Appliances: #A2137 VMs: #A2244

Cipher Suites Supported in PAN-OS 9.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- [PAN-OS 9.1 GlobalProtect Cipher Suites](#)
- [PAN-OS 9.1 IPsec Cipher Suites](#)
- [PAN-OS 9.1 IKE and Web Certificate Cipher Suites](#)
- [PAN-OS 9.1 Decryption Cipher Suites](#)
- [PAN-OS 9.1 HA1 SSH Cipher Suites](#)
- [PAN-OS 9.1 Administrative Session Cipher Suites](#)
- [PAN-OS 9.1 PAN-OS-to-Panorama Connection Cipher Suites](#)

PAN-OS 9.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [GlobalProtect App/Agent—SSL](#)
- [GlobalProtect App/Agent—IPsec mode](#)
- [GlobalProtect Portal—Browser Access](#)

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	<ul style="list-style-type: none"> • TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	<ul style="list-style-type: none"> • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	<ul style="list-style-type: none"> • AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	<ul style="list-style-type: none"> • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 9.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [IPSec—Encryption](#)
- [IPSec—Message Authentication](#)
- [IPSec—Key Exchange](#)

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
IPSec—Encryption	<ul style="list-style-type: none"> • NULL • DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	<ul style="list-style-type: none"> • NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	<ul style="list-style-type: none"> • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 9.1 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 9.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [IKE Certificate Support](#)
- [IKE—Encryption](#)
- [IKE—Message Authentication](#)
- [IKE—Key Exchange](#)
- [PAN-OS Web Certificates](#)

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
IKE Certificate Support	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512
IKE—Encryption	<ul style="list-style-type: none"> • DES • 3DES • AES-128-CBC

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	<ul style="list-style-type: none"> • AES-192-CBC • AES-256-CBC
IKE—Message Authentication	<ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups <ul style="list-style-type: none"> • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group)
PAN-OS Web Certificates	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, 3072-bit, and 4096-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 9.1 Decryption Cipher Suites


The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.




If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [SSH Decryption \(SSHv2 only\)—Encryption](#)
- [SSH Decryption \(SSHv2 only\)—Message Authentication](#)
- [SSL/TLS Decryption](#)
- [SSL/TLS Decryption—NIST-approved Elliptical Curves](#)

- [SSL/TLS Decryption—Perfect Forward Secrecy \(PFS\) Ciphers](#)

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
SSH Decryption (SSHv2 only)—Encryption	<ul style="list-style-type: none"> • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	<ul style="list-style-type: none"> • HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys <p> <i>The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 4096-bit RSA keys.</i></p> <ul style="list-style-type: none"> • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384
SSL/TLS Decryption—NIST-approved Elliptical Curves	<ul style="list-style-type: none"> • P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1)

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	<ul style="list-style-type: none"> • P-521 (secp521r1)
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers  <i>If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.</i>	<ul style="list-style-type: none"> • DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 9.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [Administrative Sessions to Web Interface](#)
- [Administrative Sessions to CLI \(SSH\)—Encryption](#)
- [Administrative Sessions to CLI \(SSH\)—Message Authentication](#)
- [Administrative Sessions to CLI \(SSH\)—Server Host Key Types](#)
- [Administrative Sessions to CLI \(SSH\)—Key Exchange Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
Administrative Sessions to Web Interface	<ul style="list-style-type: none"> • TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-3DES-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	<ul style="list-style-type: none"> • 3DES-CBC • ARCFOUR128 • ARCFOUR256 • BLOWFISH-CBC • CAST128-CBC • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
Administrative Sessions to CLI (SSH)—Message Authentication	<ul style="list-style-type: none"> • UMAC-64 • UMAC-128 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	<ul style="list-style-type: none"> • RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	<ul style="list-style-type: none"> • diffie-hellman-group1-SHA-1 • diffie-hellman-group14-SHA-1 • diffie-hellman-group-exchange-SHA-1 • diffie-hellman-group-exchange-SHA-256 • ecdh-SHA-2-nistp256 • ecdh-SHA-2-nistp384 • ecdh-SHA-2-nistp521

PAN-OS 9.1 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 9.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
HA1 SSH	<ul style="list-style-type: none"> • AES 128-bit cipher with Cipher Block Chaining • AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Cipher Block Chaining • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Cipher Block Chaining

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
	<ul style="list-style-type: none"> • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM

PAN-OS 9.1 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 9.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 9.1 Releases
PAN-OS to Panorama Connection	<ul style="list-style-type: none"> • RSA-RC4-128-SHA-1 • RSA-3DES-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 9.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 9.1 release in FIPS-CC mode. The [Cryptographic Algorithm Validation Program](#) has additional details regarding the algorithm implementation. Also, there were no changes made to the Palo Alto Networks crypto module between PAN-OS 9.0 and PAN-OS 9.1 so all FIPS certificates still apply for this PAN-OS 9.1 release.



If your firewall is running in normal (non-FIPS-CC) operational mode, see [Cipher Suites Supported in PAN-OS 9.1](#)

Functions	Standards
Asymmetric key generation	
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4
RSA key generation (2048 bits or greater)	FIPS PUB 186-4
Cryptographic Key Generation (for IKE Peer Authentication)	
RSA key generation (2048 bits or greater)	FIPS PUB 186-4
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4
Cryptographic Key Establishment	
ECDSA-based key establishment	NIST SP 800-56A Revision 2
FFC-based key establishment	NIST SP 800-56A Revision 2
AES Data Encryption/Decryption	
<ul style="list-style-type: none"> • AES CTR 128/192/256 • AES CBC 128/192/256 • AES GCM 128/256 • AES CCM 128 	<ul style="list-style-type: none"> • AES as specified in ISO 18033-3 • CBC/CTR as specified in ISO 10116 • GCM as specified in ISO 19772 • NIST SP 800-38A/C/D/F • FIPS PUB 197
Signature Generation and Verification	
RSA Digital Signature Algorithm (rDSA) (2048 bits or greater)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST

Functions	Standards
	curves" P-256, P-384, ISO/IEC 14888-3, Section 6.4
Cryptographic hashing	
SHA-1, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 256, 384, and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4
Keyed-hash message authentication	
<ul style="list-style-type: none"> • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 	ISO/IEC 9797-2:2011 FIPS PUB 198-1
Random bit generation	
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A

Cipher Suites Supported in PAN-OS 8.1

The following topics list cipher suites that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.

If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

The ciphers supported in normal operation mode are grouped according to feature or functionality in the following sections:

- [PAN-OS 8.1 GlobalProtect Cipher Suites](#)
- [PAN-OS 8.1 IPsec Cipher Suites](#)
- [PAN-OS 8.1 IKE and Web Certificate Cipher Suites](#)
- [PAN-OS 8.1 Decryption Cipher Suites](#)
- [PAN-OS 8.1 HA1 SSH Cipher Suites](#)
- [PAN-OS 8.1 Administrative Session Cipher Suites](#)
- [PAN-OS 8.1 PAN-OS-to-Panorama Connection Cipher Suites](#)

PAN-OS 8.1 GlobalProtect Cipher Suites

The following table lists cipher suites for GlobalProtect™ supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal](#)
- [GlobalProtect App/Agent—IPsec mode](#)
- [GlobalProtect Portal—Browser Access](#)

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
GlobalProtect App/Agent—SSL tunnels and SSL connections to gateway and portal	<ul style="list-style-type: none"> • TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	<ul style="list-style-type: none"> • RSA-AES-256-GCM-SHA-384 • DHE-RSA-SEED-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • EDH-RSA-3DES-SHA-1 • ECDHE-RSA-AES-128-SHA-1 • ECDHE-RSA-AES-256-SHA-1 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-128-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
GlobalProtect App/Agent—IPSec mode (Keys transported through SSL session with gateway)	<ul style="list-style-type: none"> • AES-128-CBC-HMAC-SHA-1 • AES-128-GCM-HMAC-SHA-1 • AES-256-GCM-HMAC-SHA-1
GlobalProtect Portal—Browser Access	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-256-SHA-1 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	<ul style="list-style-type: none"> • EDH-RSA-3DES-SHA-1 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 8.1 IPSec Cipher Suites

The following table lists the cipher suites for IPSec that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [IPSec—Encryption](#)
- [IPSec—Message Authentication](#)
- [IPSec—Key Exchange](#)

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
IPSec—Encryption	<ul style="list-style-type: none"> • NULL • DES • 3DES • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CCM • AES-128-GCM • AES-256-GCM
IPSec—Message Authentication	<ul style="list-style-type: none"> • NONE • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IPSec—Key Exchange	Diffie-Hellman groups with or without perfect forward secrecy (PFS):

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	<ul style="list-style-type: none"> • No PFS—This option specifies that the firewall reuses the same key for IKE phase 1 and phase 2 instead of renewing the key for phase 2. • Group 1 (768-bit keys) with PFS enabled • Group 2 (1024-bit keys) with PFS enabled • Group 5 (1536-bit keys) with PFS enabled • Group 14 (2048-bit keys) with PFS enabled • Group 19 (256-bit elliptic curve group) with PFS enabled • Group 20 (384-bit elliptic curve group) with PFS enabled

PAN-OS 8.1 IKE and Web Certificate Cipher Suites

The following table lists cipher suites for Internet Key Exchange (IKE) and PAN-OS® web certificates that are supported on firewalls running a PAN-OS 8.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [IKE Certificate Support](#)
- [IKE—Encryption](#)
- [IKE—Message Authentication](#)
- [IKE—Key Exchange](#)
- [PAN-OS Web Certificates](#)

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
IKE Certificate Support	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, and 3072-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512
IKE—Encryption	<ul style="list-style-type: none"> • DES • 3DES • AES-128-CBC

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	<ul style="list-style-type: none"> • AES-192-CBC • AES-256-CBC
IKE—Message Authentication	<ul style="list-style-type: none"> • HMAC-MD5 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512
IKE—Key Exchange	Diffie-Hellman groups <ul style="list-style-type: none"> • Group 1 (768-bit keys) • Group 2 (1024-bit keys) • Group 5 (1536-bit keys) • Group 14 (2048-bit keys) • Group 19 (256-bit elliptic curve group) • Group 20 (384-bit elliptic curve group)
PAN-OS Web Certificates	<ul style="list-style-type: none"> • RSA <ul style="list-style-type: none"> • Keys—512-bit, 1024-bit, 2048-bit, 3072-bit, and 4096-bit keys • Digital signature algorithms—SHA-1, SHA-256, SHA-384, or SHA-512 • ECDSA <ul style="list-style-type: none"> • Keys—256-bit and 384-bit keys • Digital signature algorithms—SHA-256, SHA-384, or SHA-512

PAN-OS 8.1 Decryption Cipher Suites


The following table lists cipher suites for decryption that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.




If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [SSH Decryption \(SSHv2 only\)—Encryption](#)
- [SSH Decryption \(SSHv2 only\)—Message Authentication](#)
- [SSL/TLS Decryption](#)
- [SSL/TLS Decryption—NIST-approved Elliptical Curves](#)

- [SSL/TLS Decryption—Perfect Forward Secrecy \(PFS\) Ciphers](#)

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
SSH Decryption (SSHv2 only)—Encryption	<ul style="list-style-type: none"> • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR
SSH Decryption (SSHv2 only)—Message Authentication	<ul style="list-style-type: none"> • HMAC-RIPEMD • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1
SSL/TLS Decryption	<ul style="list-style-type: none"> • SSLv3, TLSv1.0, TLSv1.1, and TLSv1.2 cipher suites • RSA 512-bit, 1024-bit, 2048-bit, 3072-bit, 4096-bit, and 8192-bit keys <p> <i>The firewall can authenticate certificates up to 8192-bit RSA keys from the destination server, however the firewall generated certificate to the client supports only up to 2048-bit RSA keys.</i></p> <ul style="list-style-type: none"> • RSA-RC4-128-MD5 • RSA-RC4-128-SHA-1 • RSA-3DES-EDE-CBC-SHA-1 • RSA-AES-128-CBC-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384
SSL/TLS Decryption—NIST-approved Elliptical Curves	<ul style="list-style-type: none"> • P-192 (secp192r1) • P-224 (secp224r1) • P-256 (secp256r1) • P-384 (secp384r1)

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
	<ul style="list-style-type: none"> • P-521 (secp521r1)
SSL/TLS Decryption—Perfect Forward Secrecy (PFS) Ciphers  <i>If you use the DHE or ECDHE key exchange algorithms to enable PFS support for SSL decryption, you can use a hardware security module (HSM) to store the private keys used for SSL Inbound Inspection.</i>	<ul style="list-style-type: none"> • DHE-RSA-3DES-EDE-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-1 • DHE-RSA-AES-256-CBC-SHA-1 • DHE-RSA-AES-128-CBC-SHA-256 • DHE-RSA-AES-256-CBC-SHA-256 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-CBC-SHA-1 • ECDHE-RSA-AES-256-CBC-SHA-1 • ECDHE-RSA-AES-128-CBC-SHA-256 • ECDHE-RSA-AES-256-CBC-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-CBC-SHA-1 • ECDHE-ECDSA-AES-256-CBC-SHA-1 • ECDHE-ECDSA-AES-128-CBC-SHA-256 • ECDHE-ECDSA-AES-256-CBC-SHA-384 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384

PAN-OS 8.1 Administrative Session Cipher Suites

The following table lists the cipher suites for administrative sessions that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

- [Administrative Sessions to Web Interface](#)
- [Administrative Sessions to CLI \(SSH\)—Encryption](#)
- [Administrative Sessions to CLI \(SSH\)—Message Authentication](#)
- [Administrative Sessions to CLI \(SSH\)—Server Host Key Types](#)
- [Administrative Sessions to CLI \(SSH\)—Key Exchange Algorithms](#)

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
Administrative Sessions to Web Interface	<ul style="list-style-type: none"> • TLSv1.1 and TLSv1.2 cipher suites • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-3DES-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-256-SHA-1 • RSA-AES-256-CBC-SHA-1 • RSA-AES-128-CBC-SHA-256 • RSA-AES-256-CBC-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-3DES-SHA-1 • DHE-RSA-AES-128-GCM-SHA-256 • DHE-RSA-AES-256-GCM-SHA-384 • ECDHE-RSA-AES-128-GCM-SHA-256 • ECDHE-RSA-AES-256-GCM-SHA-384 • ECDHE-ECDSA-AES-128-SHA-1 • ECDHE-ECDSA-AES-256-SHA-1 • ECDHE-ECDSA-AES-128-GCM-SHA-256 • ECDHE-ECDSA-AES-256-GCM-SHA-384
Administrative Sessions to CLI (SSH)—Encryption	<ul style="list-style-type: none"> • 3DES • ARCFOUR128 • ARCFOUR256 • BLOWFISH • CAST128 • AES-128-CBC • AES-192-CBC • AES-256-CBC • AES-128-CTR • AES-192-CTR • AES-256-CTR • AES-128-GCM • AES-256-GCM

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
Administrative Sessions to CLI (SSH)—Message Authentication	<ul style="list-style-type: none"> • UMAC-64 • HMAC-MD5-96 • HMAC-MD5 • HMAC-SHA-1-96 • HMAC-RIPEMD-160 • HMAC-SHA-1 • HMAC-SHA-256 • HMAC-SHA-512
Administrative Sessions to CLI (SSH)—Server Host Key Types	<ul style="list-style-type: none"> • RSA keys—2048-bit, 3072-bit, and 4096-bit keys • ECDSA keys—256-bit, 384-bit, and 521-bit keys
Administrative Sessions to CLI (SSH)—Key Exchange Algorithms	<ul style="list-style-type: none"> • diffie-hellman-group1-SHA-1 • diffie-hellman-group14-SHA-1 • diffie-hellman-group-exchange-SHA-1 • diffie-hellman-group-exchange-SHA-256 • ecdh-SHA-2-nistp256 • ecdh-SHA-2-nistp384 • ecdh-SHA-2-nistp521

PAN-OS 8.1 HA1 SSH Cipher Suites

The following table lists the cipher suites for HA1 control connections using SSH that are supported on firewalls running a PAN-OS® 8.1 release in normal (non-FIPS-CC) or FIPS-CC operational mode.

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
HA1 SSH	<ul style="list-style-type: none"> • AES 128-bit cipher with Cipher Block Chaining • AES 128-bit cipher with Counter Mode • AES 128-bit cipher with GCM (Galois/Counter Mode) • AES 192-bit cipher with Cipher Block Chaining • AES 192-bit cipher with Counter Mode • AES 256-bit cipher with Cipher Block Chaining • AES 256-bit cipher with Counter Mode • AES 256-bit cipher with GCM

PAN-OS 8.1 PAN-OS-to-Panorama Connection Cipher Suites

The following table lists the cipher suites for PAN-OS®-to-Panorama™ connections that are supported on firewalls running a PAN-OS 8.1 release in normal (non-FIPS-CC) operational mode.



If your firewall is running in FIPS-CC mode, see the list of [PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode](#).

Feature or Function	Ciphers Supported in PAN-OS 8.1 Releases
PAN-OS to Panorama Connection	<ul style="list-style-type: none"> • RSA-RC4-128-SHA-1 • RSA-3DES-SHA-1 • RSA-SEED-SHA-1 • RSA-CAMELLIA-128-SHA-1 • RSA-CAMELLIA-256-SHA-1 • RSA-AES-128-SHA-1 • RSA-AES-128-SHA-256 • RSA-AES-256-SHA-1 • RSA-AES-256-SHA-256 • RSA-AES-128-GCM-SHA-256 • RSA-AES-256-GCM-SHA-384 • DHE-RSA-AES-128-SHA-1 • DHE-RSA-AES-256-SHA-1

PAN-OS 8.1 Cipher Suites Supported in FIPS-CC Mode

The following table lists cipher suites that are supported on firewalls running a PAN-OS® 8.1 release in FIPS-CC mode.



If your firewall is running in normal (non-FIPS-CC) operational mode, see [Cipher Suites Supported in PAN-OS 8.1](#).

Functions	Standards	Certificates
Asymmetric key generation		
FFC key pair generation (key size 2048 bits)	FIPS PUB 186-4	Appliances: DSA #1485 VMs: DSA #1497

Functions	Standards	Certificates
ECC key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: ECDSA #1570 VMs: ECDSA #1575
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: RSA #3086 VMs: RSA #3090
Cryptographic Key Generation (for IKE Peer Authentication)		
RSA key generation (2048 bits or greater)	FIPS PUB 186-4	Appliances: RSA #3086 VMs: RSA #3090
ECDSA key pair generation (NIST curves P-256, P-384)	FIPS PUB 186-4	Appliances: ECDSA #1570 VMs: ECDSA #1575
Cryptographic Key Establishment		
ECDSA-based key establishment	NIST SP 800-56A Revision 2	Appliances: CVL #2119 VMs: CVL #2128
FFC-based key establishment	NIST SP 800-56A Revision 2	Appliances: CVL #2119 VMs: CVL #2128
AES Data Encryption/Decryption		
<ul style="list-style-type: none"> AES CTR 128/192/256 AES CBC 128/192/256 	<ul style="list-style-type: none"> AES as specified in ISO 18033-3 	Appliances:

Functions	Standards	Certificates
<ul style="list-style-type: none"> AES GCM 128/256 AES CCM 128 	<ul style="list-style-type: none"> CBC/CTR as specified in ISO 10116 GCM as specified in ISO 19772 NIST SP 800-38A/C/D/F FIPS PUB 197 	AES #5890 VMs: AES #5902
Signature Generation and Verification		
RSA Digital Signature Algorithm (rDSA) (2048 bits or greater)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSAPKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Appliances: RSA #3086 VMs: RSA #3090
ECDSA (NIST curves P-256, P-384, and P-521)	FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" P-256, P-384, ISO/IEC 14888-3, Section 6.4	Appliances: RSA #1570 VMs: RSA #1575
Cryptographic hashing		
SHA-1, SHA-256, SHA-384, and SHA-512 (digest sizes 160, 256, 384, and 512 bits)	ISO/IEC 10118-3:2004 FIPS PUB 180-4	Appliances: SHS #4641 VMs: SHS #4658
Keyed-hash message authentication		
<ul style="list-style-type: none"> HMAC-SHA-1 HMAC-SHA-256 	ISO/IEC 9797-2:2011 FIPS PUB 198-1	Appliances: HMAC #3865

Functions	Standards	Certificates
<ul style="list-style-type: none">HMAC-SHA-384HMAC-SHA-512		VMs: HMAC #3882
Random bit generation		
CTR_DRBG (AES-256)	ISO/IEC 18031:2011 NIST SP 800-90A	Appliances: DRBG #2451 VMs: DRBG #2464

GlobalProtect

The following topics provide support information for the GlobalProtect™ app (originally referred to as the GlobalProtect agent on Windows and Mac).

- [Where Can I Install the GlobalProtect App?](#)
- [Third-Party IPSec Client Support](#)
- [What Features Does GlobalProtect Support?](#)
- [What Features Does GlobalProtect Support for IoT?](#)
- [What GlobalProtect Features Do Third-Party Mobile Device Management Systems Support?](#)

Where Can I Install the GlobalProtect App?

The following sections show operating systems on which you can install each release of the GlobalProtect™ app.



The compatibility lists that follow show compatibility with major versions for each platform only and does specifically call out minor versions. However, support the stated support for the major versions implicitly includes support for all minor versions for the listed major versions.

- [Apple macOS](#)
- [Microsoft Windows](#)
- [Linux](#)
- [Apple iOS and iPadOS](#)
- [Google Android](#)
- [Google Chrome](#)
- [Internet of Things \(IoT\)](#)
- [Hypervisors](#)

Use the OS compatibility information to determine what version of the GlobalProtect app you want your users to run on their endpoints.



Because the version that an end user must download and install to enable successful connectivity to your network depends on your environment, there is no direct download link for the GlobalProtect app on the Palo Alto Networks site. In addition, the way you [deploy the GlobalProtect app to your users](#) depends on the OS of the endpoint.

Apple macOS

The following table shows which macOS versions support which versions of the GlobalProtect app. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), [5.2](#), and [6.0](#), [6.1](#) and [6.2](#).

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
macOS 10.11 (El Capitan)	✓	✓	—	—	—
macOS 10.12 (Sierra)	✓	✓	—	—	—
macOS 10.13 (High Sierra)	✓	✓	—	—	—

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
macOS 10.14 (Mojave)	✓	✓ 5.2.12 & earlier	—	—	—
macOS 10.15 (Catalina)	✓	✓	✓	✓	✓
macOS 11 (Big Sur)	✓ 5.1.7 & later (x86 & ARM-Based MacBooks Using Rosetta Translation)	✓ 5.2.4 & later (x86-based MacBooks) 5.2.5 & later (x86 & ARM-Based MacBooks Using Rosetta Translation) 5.2.6 & later (x86 & ARM-Based MacBooks)	✓	✓	✓
macOS 12 (Monterey)	—	✓ 5.2.10 or later (x86 & ARM-Based MacBooks)	✓	✓	✓
macOS 13 (Ventura)	—	✓ 5.2.12 or later (x86 & ARM-Based MacBooks)	✓ 6.0.3 or later (x86 & ARM-Based MacBooks)	✓	✓

Microsoft Windows

The following table shows which Microsoft Windows versions support which versions of the GlobalProtect app. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), [5.2](#) [6.0](#), [6.1](#), and [6.2](#).

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
Windows 7	√ Service Pack 1	— Upgrades from 5.1.10 to 5.2.x or later are blocked.	—	—	—
Windows 8	—	—	—	—	—
Windows 8.1	√	√	—	—	—
Windows 10	√	√	√ 64-bit (x64), 32-bit (x86), and ARM64 devices	√ 64-bit (x64), 32-bit (x86), and ARM64 devices	√ 64-bit (x64), 32-bit (x86), and ARM64 devices
Windows 10 UWP	√ x86 and ARM devices	√ x86 and ARM devices	√	√	√
Windows 11	—	√ x86 devices only on 5.2.10 & later	√ 64-bit (x64) and ARM64 devices	√ 64-bit (x64) and ARM64 devices	√ 64-bit (x64) and ARM64 devices

Linux

The following table shows compatibility between Linux versions and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), [5.2](#), [6.0](#), and [6.1](#).

Only 64-bit Linux versions are supported. 32-bit versions are not supported.

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
CentOS 7.0	√ CLI-based and GUI-based	√ CLI-based and GUI-based	—	—	—	N/A

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
	GlobalProtect app	GlobalProtect app				
CentOS 7.1	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
CentOS 7.2	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
CentOS 7.3	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
CentOS 7.4	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
CentOS 7.5	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
CentOS 7.6	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
CentOS 7.7	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
CentOS 8.0	✓ CLI-based GlobalProtect app	✓ CLI-based GlobalProtect app	—	—	—	N/A
CentOS 8.3	—	—	✓ CLI-based and GUI-based GlobalProtect app	✓ Supported on GlobalProtect 6.0.4 or earlier versions only CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	N/A
Red Hat Enterprise Linux (RHEL) 7.0 through 8.1	✓ Releases 7.0 through 7.7: CLI-based and GUI-based GlobalProtect app	✓ Releases 7.0 through 7.7: CLI-based and GUI-based GlobalProtect app	—	—	—	N/A
Red Hat Enterprise Linux (RHEL) 8.3	—	—	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	N/A	N/A

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
Red Hat Enterprise Linux (RHEL) 8.4	—	—	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	N/A	N/A
Red Hat Enterprise Linux (RHEL) 8.7	—	—	—	—	✓ (Supported on GlobalProtect 6.1.1 and later.)	N/A
Red Hat Enterprise Linux (RHEL) 9.1	—	—	—	—	✓ (Supported on GlobalProtect 6.1.1 and later.)	N/A
Ubuntu 14.04	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app running 5.3.2 or later	—	—	N/A
Ubuntu 16.04 LTS	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app running 5.3.2 or later	✓ CLI-based and GUI-based GlobalProtect app	✓ CLI-based and GUI-based GlobalProtect app	N/A
Ubuntu 18.04 LTS	✓ CLI-based and GUI-	✓ CLI-based and GUI-	✓ CLI-based and GUI-	✓ CLI-based and GUI-	✓ CLI-based and GUI-	N/A

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
	based GlobalProtect app	based GlobalProtect app	based GlobalProtect app running 5.3.2 or later	based GlobalProtect app	based GlobalProtect app	
Ubuntu 19.04	✓ CLI-based and GUI- based GlobalProtect app	✓ CLI-based and GUI- based GlobalProtect app	✓ CLI-based and GUI- based GlobalProtect app running 5.3.2 or later	✓ CLI-based and GUI- based GlobalProtect app	✓ CLI-based and GUI- based GlobalProtect app	N/A
Ubuntu 20.04	✓ CLI-based GlobalProtect app only	✓ CLI-based GlobalProtect app only	✓ CLI-based GlobalProtect app running 5.3.2 or later	✓ CLI only	✓ CLI-based and GUI- based GlobalProtect app	N/A
Ubuntu 22.04	—	—	—	—	✓ CLI-based and GUI- based GlobalProtect app	N/A

Apple iOS and iPadOS

The following table shows compatibility between iOS versions and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), [5.2](#), and [6.0](#).

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
iOS 10	✓ (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)	N/A	N/A

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
iOS 11	✓ (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)	N/A	N/A
iOS 12	✓ (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)	N/A	N/A
iOS 13	✓ 5.0.8 & later (64-bit devices only)	✓ (64-bit devices only)	✓ (64-bit devices only)	N/A	N/A
iOS 14	—	✓ (64-bit devices only)	✓ (64-bit devices only)	N/A	N/A
iOS 15	—	✓ (64-bit devices only running GlobalProtect app 5.2.12 or later)	✓ (64-bit devices only)	N/A	N/A
iOS 16	—	—	✓ (64-bit devices only running GlobalProtect app 6.0.4 or later)	N/A	N/A

Google Android

The following table shows compatibility between Google Android versions and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), [5.2](#), and [6.0](#).

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
Google Android 6.x	✓	✓	✓	N/A	N/A
Google Android 7.x	✓	✓	✓	N/A	N/A
Google Android 8.x	✓	✓	✓	N/A	N/A
Google Android 9.x	✓	✓	✓	N/A	N/A
Google Android 10.x	✓	✓	✓	N/A	N/A
Google Android 11.x	—	✓	✓	N/A	N/A
Google Android 12.x	—	✓ Starting with GlobalProtect app version 5.2.10	✓	N/A	N/A
Google Android 13.x	—	—	✓ 6.0.3 or later	N/A	N/A
Chrome OS Systems Supporting Android Apps	✓	✓	✓	N/A	N/A

Google Chrome

The following table shows compatibility between Google Chrome OS systems supporting Android apps and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), and [5.2](#), and [6.0](#).

OS	GP App 5.1	GP App 5.2	GP App 6.0	GP App 6.1	GP App 6.2
Chrome OS Systems Supporting Android Apps	✓	✓	✓	N/A	N/A

Internet of Things (IoT)

The following table shows compatibility between IoT platforms and GlobalProtect app versions. For instructions on installing the GlobalProtect app on a macOS endpoint, see the installation instructions for [5.1](#), [5.2](#), [6.0](#), and [6.1](#). See the [supported features list](#) to see which GlobalProtect app features are supported on IoT devices.

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
Android	✓	✓	—	✓	N/A	N/A
Raspbian	✓	✓	—	✓	✓	N/A
Ubuntu	✓	✓	—	✓	✓	N/A
Windows IoT Enterprise	✓	✓	—	✓	✓	N/A

Hypervisors

The following table shows hypervisor support on each GlobalProtect app version.

OS	GP App 5.1	GP App 5.2	GP App 5.3	GP App 6.0	GP App 6.1	GP App 6.2
Citrix Xen Desktop	—	—	—	✓ 6.0.3 and later	✓	✓
VMWare Horizon and Vcenter	✓	✓	✓	✓	✓	✓

Third-Party VPN Client Support

The following topics provide support information for third-party clients:

- [What Third-Party VPN Clients are Supported?](#)
- [What GlobalProtect Features Do Third-Party Clients Support?](#)
- [How Many Third-Party Clients Does Each Firewall Model Support?](#)

What Third-Party VPN Clients are Supported?

The following table lists third-party VPN client support for PAN-OS® software.



For stronger security, higher tunnel capacities, and a greater breadth of [features](#), we recommend that you use the GlobalProtect™ app instead of a third-party VPN client.

Third-Party IPsec Client	Minimum PAN-OS Release Version
iOS built-in IPsec client	9.1
Android built-in IPsec client	9.1
VPNC on Ubuntu Linux 10.04 and later versions and CentOS 6 and later versions	9.1
strongSwan on Ubuntu Linux and CentOS*	9.1

* To set up authentication for strongSwan Ubuntu and CentOS clients for PAN-OS 9.1 and later releases, refer to the [GlobalProtect Administrator's Guide](#) for your release.



Clients emulating GlobalProtect are not supported.

What GlobalProtect Features Do Third-Party Clients Support?

Third-party clients support the following GlobalProtect™ features:

GlobalProtect Feature	iOS Built-In IPSec Client	Android Built-In IPSec Client	VPNC on Ubuntu Linux 10.04 and later versions and CentOS 6 and later versions	strongSwan on Ubuntu Linux and CentOS
Mixed Authentication Method Support for Certificates or User Credentials	✓	✓	✓	✓
IPSec VPN Connections	✓	✓	✓	✓
IPv4 Addressing	✓	✓	✓	✓
Gateway-Level IP Pools	✓	✓	✓	✓
Primary Username Visibility on GlobalProtect Gateways	✓	✓	✓	✓

How Many Third-Party Clients Does Each Firewall Model Support?

The following table lists the maximum number of third-party X-Auth IPSec clients supported by each firewall model.

Palo Alto Networks Firewall Model	Maximum Third-Party X-Auth IPSec Clients
Hardware Firewalls	
PA-7080	2,000
PA-7050	2,000
PA-5450	4,000
PA-5440	4,000
PA-5430	4,000
PA-5420	4,000
PA-5410	4,000
PA-5280	2,500

Palo Alto Networks Firewall Model	Maximum Third-Party X-Auth IPSec Clients
PA-5260	2,500
PA-5250	2,000
PA-5220	1,500
PA-5060*	1,000
PA-5050*	1,000
PA-5020*	1,000
PA-3440	2,000
PA-3430	2,000
PA-3420	1,500
PA-3410	1,500
PA-3260	1,500
PA-3250	1,500
PA-3220	1,000
PA-3050	1,000
PA-1420	1,400
PA-1410	1,400
PA-850	500
PA-820	500
PA-500*	500
PA-460	1,400
PA-450	1,400
PA-445	1,400
PA-440	1,400

Palo Alto Networks Firewall Model	Maximum Third-Party X-Auth IPSec Clients
PA-415	500
PA-410	500
PA-220R	500
PA-220**	500
VM-Series Firewalls	
VM-700	1,000
VM-500	500
VM-300	500
VM-200	500
VM-100	500
VM-50	125

* These appliances are supported only on PAN-OS 8.1 and only until each reaches its [hardware end-of-life \(EoL\) date](#).

** PA-220 firewalls are supported only on PAN-OS 10.2 and earlier PAN-OS versions.

What Features Does GlobalProtect Support?

The following table lists the features supported on GlobalProtect™ by operating system (OS). An entry in the table indicates the first supported release of the feature on the OS (however, you should review the [End-of-Life Summary](#) to ensure you are using a supported release). A dash (“—”) indicates that the feature is not supported. For recommended minimum GlobalProtect app versions, see [Where Can I Install the GlobalProtect App?](#).



For Chromebook and other Chrome OS devices, use Android App 5.0 or later version to get GlobalProtect app features introduced in GlobalProtect app 5.0 and later releases. (Refer also to the [end-of-life \(EoL\) information for the GlobalProtect app.](#))

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Authentication							
Multi-Factor Authentication Policy	—	—	—	4.0.0	—	4.0.0	—
SAML Authentication	4.0.0	4.0.0 (On-Demand connect method only)	4.1.0	4.0.0	—	4.0.0	5.1 (GUI-based GlobalProtect app)
SAML Authentication with Cloud Authentication Service Note: Requires use of Default System Browser	6.0.0	6.0.0 (On Demand connect method only)	6.0.0	6.0.0	—	6.0.0	6.0.0
Default System Browser for SAML Authentication	5.2.0	5.2.0	5.2.0	5.2.0	—	5.2.0	5.2.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Expired Active Directory Password Change for Remote Users	4.1.0	4.1.0 (notifications only) 5.0.0 (full support)	4.1.0	4.1.0	4.1.0	4.1.0	—
Active Directory Password Change Using the GlobalProtect Credential Provider	—	—	—	4.1.0	—	—	—
Mixed Authentication Method Support or Certificates or User Credentials	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
Pre-Logon Followed by Two-Factor Authentication	—	—	—	4.1.0	—	4.1.0	—
Pre-Logon Followed by SAML Authentication	—	—	—	4.1.0	—	4.1.0	—
Single Sign-On (SSO)							
SSO (Credential Provider)	—	—	—	1.2.0	—	—	—
Kerberos SSO	—	—	—	3.0.0	—	4.1.0	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
SAML SSO	5.1.0	5.2.0	5.1.0	5.2.0	—	5.2.0	5.2.0
SSO (Smart Card Authentication)	—	—	—	6.0.0 Windows 10 or later	—	—	—

VPN Connections

IPSec	1.3.0	1.3.0	3.1.1	1.0.0	—	1.0.0	4.1.0
SSL	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	1.0.0	4.1.0
SSL Tunnel Enforcement	5.1.0	5.1.0	—	5.1.0	—	5.1.0	5.0.6 (CLI) 5.1.0 (web interface)
Clientless VPN	— (no client required)	— (no client required)	— (no client required)	— (no client required)	— (no client required)	— (no client required)	— (no client required)

Connect Methods

User-logon (always on)	1.3.0	1.3.0	5.0.0 (through extended support for the GlobalProtect app for Android)	1.0.0	3.1.3 (Always On configured from third-party MDM)	1.0.0	4.1.0
Pre-logon (always-on)	—	—	—	1.1.0	—	1.1.0	—
Pre-logon (then on-demand)	—	—	—	3.1.0	—	3.1.0	—
On-demand	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	1.0.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Connect Before Logon	—	—	—	5.2.0	—	—	—
Conditional Connect Method	—	—	—	6.2.0	6.2.0	6.2.0	—

Connection Priority

External Gateway Priority by Source Region	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1.0
Internal Gateway Selection by Source IP Address	4.0.0 (Except DHCP options)	4.0.0 (Except DHCP options)	—	4.0.0	—	4.0.0	4.1.0

Modes

Internal mode	1.3.0	1.3.0	—	1.0.0	—	1.0.0	4.1
External mode	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	1.0.0	4.1
Prisma Access Explicit Proxy Connectivity in GlobalProtect	—	—	—	6.2.0	6.2.0	6.2.0	—

Networking

IPv4 Addressing	1.3.0	1.3.0	3.1.1	1.0.0	3.1.3	1.0.0	4.1
IPv6 Addressing	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Split Tunnel to Exclude by Access Route	—	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1
Optimized Split Tunneling for GlobalProtect	—	—	—	4.1.0	—	4.1.0	6.1.0 Domain-based split tunneling only; application-based split tunneling not supported
Enhanced Split Tunneling	—	—	—	6.2.0	6.2.0	6.2.0	—
Split DNS	—	—	—	5.2.0	—	5.2.0	6.1.0
Per-App VPN	4.0.0	4.0.0					
No Direct Access to Local Network	—	—	—	4.0.0	—	4.0.0	6.0.0
Endpoint Traffic Policy Enforcement	—	—	—	6.0.0 Windows 10 or later	—	6.0.0 macOS 11 and later	—

Customization

Autonomous DEM Integration for User Experience Management	—	—	—	5.2.6	—	5.2.6	—
---	---	---	---	-------	---	-------	---

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
GlobalProtect App Log Collection for Troubleshooting	5.2.5	5.2.5	5.2.5	5.2.5	—	5.2.5	5.2.5
Configurable Maximum Transmission Unit for GlobalProtect Connections	5.2.4	5.2.4	5.2.4	5.2.4	5.2.4	5.2.4	5.2.4
Connect Before Logon	—	—	—	5.2.0	—	—	—
User-Initiated Pre-Logon Connection	-	-	-	5.0.3	-	-	-
Support for Preferred Gateways	5.0.3	5.0.7	-	5.0.3	-	5.0.3	-
GlobalProtect Gateway Location Configuration	5.0.0	5.0.0	-	5.0.0	-	5.0.0	-
Automatic Launching of Web Browser in Captive Portal Environment	-	-	-	4.1.0	-	4.1.0	-
GlobalProtect Tunnel Preservation On User Logout	-	-	-	4.1.0	-	-	-
Endpoint Tunnel	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Configurations Based on Source Region or IP Address							
Portal Configuration Assignment and HIP-Based Access Control Using New Endpoint Attributes	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
HIP Report Redistribution	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
DNS Configuration Assignment Based on Users or User Groups	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
Tunnel Restoration and Authentication Cookie Usage Restrictions	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
Concurrent Support for IPv4 and IPv6 DNS Servers	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
Support for IPv6-Only GlobalProtect Deployments	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
FIPS-CC	—	—	—	FIPS Validated on 5.1.4 CC Certified on 5.1.5 x86 platforms FIPS-CC available on 6.0.7	—	FIPS Validated on 5.1.4 CC Certified on 5.1.5 x86 platforms FIPS-CC available on 6.0.7	6.0.7
MDM Integration for HIP-Based Policy Enforcement	5.0.0	5.0.0	—	—	—	—	—
Captive Portal Notification Delay	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
Tunnel Connections Over Proxies	—	—	—	4.1.7	—	4.1.7	—
PAC deployment via GlobalProtect app	—	—	—	6.1.0	—	6.1.0	6.1.0
End-user Notification about GlobalProtect Session Logout	—	—	—	6.1.0	—	6.1.0	6.1.0
GlobalProtect Credentials	—	—	—	4.1.0	—	—	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
Provier Pre-Logon Connection Status							
Static IP Address Assignment	—	—	—	4.1.0	—	—	—
Multiple Portal Support	—	—	—	4.1.0	—	4.1.0	—
Customizable Username and Password Labels	4.1.0	4.1.0	—	4.1.0	4.1.0	4.1.0	4.1.0
Gateway-Level IP Pools	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1.0
Resilient VPN	4.0.3	4.0.3	—	4.0.3	—	4.0.3	—
Pre-logon tunnel rename timeout	—	—	—	4.0.2	—	—	—
Restrict Transparent Agent Upgrades to Internal Network Connections	—	—	—	4.0.0	—	4.0.0	—
Enforce GlobalProtect for Network Access	—	—	—	3.1.0	3.1.3 (VPN Lockdown configured from third-	3.1.0	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
					party MDM)		
Enforce GlobalProtect Exclusions	—	—	—	5.1.0	—	5.1.0	—
Enforce GlobalProtect Connections with FQDN Exclusions	—	—	—	5.2.0	—	5.2.0	—
Certificate selection by OID	—	—	—	3.0.0	—	3.0.0	—
Deployment of SSL Forward Proxy CA certificates in the trust store	—	—	—	3.0.0	—	3.0.0	—
HIP reports	1.3.0	1.3.0	3.0.0	1.0.0	3.1.3 (Host information only; Notifications not supported)	1.0.0	4.1.0 (Host information only)
Run scripts before and after sessions	—	—	—	2.3.0	—	2.3.0	—
Allow users to disable GlobalProtect	—	—	—	2.2.0	—	2.2.0	4.1.0
Welcome and help pages	1.3.0	1.3.0	3.0.0	1.0.0	—	1.0.0	—

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
HIP Exceptions for Patch Management	—	—	—	6.2.0	6.2.0	6.2.0	—
HIP Process Remediation	—	—	—	6.2.0	6.2.0	6.2.0	—
Other							
Support for 100 Manual Gateways	5.0.3	5.0.7	-	5.0.3	-	5.0.3	5.0.3
User Location Visibility on GlobalProtect Gateways and Portals	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0	4.1.0
Gateway and Portal Location Visibility for End Users	5.0.0	5.0.0	—	5.0.0	—	5.0.0	—
Primary Username Visibility on GlobalProtect Gateways	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.0.0	4.1.0
Automatic VPN Reconnect for Chromebooks	—	—	4.1.0	—	—	—	—
Identification and Quarantine of Compromised Devices	5.1.0	5.1.0	5.1.0	5.1.0	5.1.0	5.1.0	5.1.0

Feature	Android	iOS	Chrome	Windows	Windows 10 UWP	macOS	Linux
(Deprecates Device Block List)							

What Features Does GlobalProtect Support for IoT?

The following table describes the features supported for GlobalProtect™ IoT by OS:

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
IPSec VPN	✓	✓	✓	✓
SSL VPN	✓	✓	✓	✓
Pre-Logon Connect Mode	—	—	—	✓
User-Logon Connect Mode	✓ Certificate or username and password	✓ Certificate or username and password	✓ Certificate or username and password	✓ Certificate or username and password
On-Demand Connect Mode	—	—	—	✓
External Gateway Priority by Source Region	✓	✓	✓	✓
Internal Gateway Selection by Source IP Address	✓	✓	✓	✓
Internal Mode	✓	✓	✓	✓
External Mode	✓	✓	✓	✓
IPv4 Addressing	✓	✓	✓	✓
IPv6 Addressing	✓	✓	✓	✓
Split Tunnel Based on Access Route	✓	✓	✓	✓
Split Tunnel Based on Destination	—	—	—	✓

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
Domain, Client Process, and Video Streaming Application				
Multiple Portal Support	—	—	—	✓
Resilient VPN	✓	✓	✓	✓
Pre-Logon Tunnel Rename Timeout	—	—	—	✓
Restrict Transparent App Upgrades to Internal Network Connections	✓	—	—	✓
Enforce GlobalProtect for Network Access	✓	—	—	✓
Deployment of SSL Forward Proxy CA Certificates in the Trust Store	✓	✓	✓	✓
HIP Reports	✓	✓	✓	✓
Run Scripts Before and After Sessions	—	✓	✓	✓
Certificate Selection by OID	—	—		✓
Allow Users to Disable GlobalProtect	—	—	—	✓

Feature	Android	Raspbian	Ubuntu	Windows IoT Enterprise
Multi-Factor Authentication (MFA)	—	—	—	√
SAML Authentication	—	—	—	√
Expired Active Directory (AD) Password Change for Remote Users	—	—	—	√
Active Directory (AD) Password Change Using the GlobalProtect Credential Provider	—	—	—	√
SSO (Credential Provider)	—	—	—	√
Kerberos SSO	—	—	—	√
Welcome and Help Pages	—	—	—	√
Headless-Mode Without Icon, Pop-Up, Dialogs, and UI	√	√	√	√

What GlobalProtect Features Do Third-Party Mobile Device Management Systems Support?

The following table lists the GlobalProtect™ features supported on third-party mobile device management (MDM) systems. A dash (“—”) indicates that the feature is not supported.

Feature	Workspace ONE	Microsoft Intune	MobileIron	Google Admin Console	Jamf Pro
GlobalProtect App Deployment	✓	✓	✓	✓	✓ (macOS only; requires GlobalProtect app 6.1 or later)
Always on VPN Configuration	✓ (iOS and Android only)	✓ (Android, iOS, and Windows 10 UWP only)	✓ (iOS and Android only)	✓ (Android only)	—
Remote Access VPN Configuration	✓ (iOS and Android only)	✓ (Android and iOS only)	✓ (iOS only)	✓	—
Per-App VPN Configuration	✓	✓ (Android, iOS, and Windows 10 UWP only)	✓ (iOS only)	—	—
MDM Integration with HIP	✓	—	—	—	—
VPN Lockdown	✓	—	—	—	—

Prisma Access

The following topics provide support information for Prisma™ Access:

- [What Features Does Prisma Access Support?](#)
- [Prisma Access and Panorama Version Compatibility](#)
- [Supported IKE Cryptographic Parameters](#)

What Features Does Prisma Access Support?

Prisma™ Access helps you to deliver consistent security to your remote networks and mobile users. There are two ways that you can deploy and manage Prisma Access:

- **Cloud Managed Prisma Access**—If you aren't using Panorama™ to manage firewall, the Prisma Access app on the hub gives you a simplified way to onboard and manage Prisma Access.
- **Panorama Managed Prisma Access**—If you are already using Panorama to manage your next-generation firewalls, you can use Panorama to deploy Prisma Access and leverage your existing configurations. You'll need the [Cloud Services plugin](#) to use Panorama for Prisma Access.

The features and IPSec parameters supported for Prisma Access vary depending on the management interface you're using—Panorama or the Prisma Access app. You cannot switch between the management interfaces after you activate your Prisma Access license. This means you must decide how you want to manage Prisma Access before you begin setting up the product. Review the [Prisma Access Feature Support](#) information to help you select your management interface.

For a description of the features supported in GlobalProtect™, see the [features that GlobalProtect supports](#).

- [Prisma Access Feature Support](#)
- [Integration with Other Palo Alto Networks Products](#)
- [Multitenancy Unsupported Features and Functionality](#)

Prisma Access Feature Support

The following sections provide you with the supported features and network settings for Prisma Access (both Panorama Managed and Cloud Managed).

- [Management](#)
- [Remote Networks](#)
- [Service Connections](#)
- [Mobile Users—GlobalProtect](#)
- [Mobile Users—Explicit Proxy](#)
- [Security Services](#)
- [Network Services](#)
- [Identity Services](#)
- [Policy Objects](#)
- [Logs](#)
- [Reports](#)
- [Integration with Other Palo Alto Networks Products](#)
- [Multitenancy Unsupported Features and Functionality](#)

Management

Feature	Prisma Access (Cloud Managed)	Prisma Access (Panorama Managed)
Best Practice Checks	✓ Learn more	—
Default Configurations Default settings enable you to get started quickly and securely	✓ Examples include: <ul style="list-style-type: none"> • Default DNS settings • Default GlobalProtect settings, including for the Prisma Access portal • Default Prisma Access infrastructure settings 	—
Built-in Best Practice Rules So you're as secure as possible, enable your users and applications based on best practice templates. With best practices as your basis, you can then refine policy based on your enterprise needs.	✓ Features with best practice rules include: <ul style="list-style-type: none"> • Security rules • Security profiles • Decryption • M365 	—
Onboarding Walkthroughs for First-Time Setup	✓ Learn more Guided walkthroughs include: <ul style="list-style-type: none"> • Onboard Remote Networks • Onboard Mobile Users (GlobalProtect) • Onboard Your HQ or Data Centers • Turn on Decryption 	—
Centralized Management Dashboards Can includes Best Practice scores and usage information	✓ Dashboards are available for features including: <ul style="list-style-type: none"> • Security Policy • Security Profiles • Decryption 	—

Feature	Prisma Access (Cloud Managed)	Prisma Access (Panorama Managed)
	<ul style="list-style-type: none"> • Authentication • Certificates • SaaS Application Management 	
Hit Counts	✓ Hit counts for security profiles include counts that measure the profile's effectiveness, and these can depend on the profile (for example, unblocked critical and high severity vulnerabilities, or WildFire submission types).	✓ Learn more
Policy Rule Usage	✓	✓ Learn more
Policy Optimizer	—	—
Profile Groups	✓ Learn more	✓
Configuration Table Export	—	✓

Remote Networks

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
IPSec Tunnels See Supported IKE Cryptographic Parameters for a list of the supported IKE crypto parameters. FQDNs for peer IPSec addresses are not supported; use an IP address for the peer address instead.	✓	✓
Secure Inbound Access	✓ Learn more	✓ Learn more
Tunnel Monitoring		

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Dead Peer Detection (DPD)	✓	✓
ICMP	✓	✓
Bidirectional Forwarding Detection (BFD)	—	—
SNMP Use Tunnel Monitoring instead of SNMP to monitor the tunnels in Prisma Access.	—	—

Service Connections

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
IPSec Tunnels See Supported IKE Cryptographic Parameters for a list of the supported IKE crypto parameters.	✓	✓ FQDNs for peer IPSec addresses are not supported; use an IP address for the peer address instead.
Tunnel Monitoring		
Dead Peer Detection (DPD)	✓	✓
ICMP	✓	✓
Bidirectional Forwarding Detection (BFD)	—	—
SNMP Use Tunnel Monitoring instead of SNMP to monitor the tunnels in Prisma Access.	—	—
Traffic Steering (using policy-based forwarding rules to forward	✓ Learn more	✓ Learn more Introduced in version 1.7.

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
internet-bound traffic to service connections)		

Mobile Users—GlobalProtect

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Using On-Premise Gateways (Hybrid Deployments)		
On-premise gateway integration with Prisma Access	✓	✓ Using on-premise gateways with Prisma Access gateways is supported.
Priorities for Prisma Access and On-Premise Gateways	✓	✓ Supported for deployments that have on-premise GlobalProtect gateways. You can set a priority separately for on-premise gateways and collectively for all gateways in Prisma Access. You can also specify source regions for on-premise gateways.
Manual Gateway Selection Users can manually select a cloud gateway from their client machines using the GlobalProtect app.	✓ Learn more	✓ Learn more
GlobalProtect Gateway Modes		
External Mode	✓	✓
Internal Mode You cannot configure Prisma Access gateways as internal gateways; however, you can add one or more on-premise	—	—

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
gateways and configure them as internal gateways.		
GlobalProtect App Connect Methods		
User-Logon (always on)	✓	✓
Pre-Logon (always on)	✓	✓
Pre-Logon (then on-demand)	✓	✓
On-Demand	✓	✓
Clientless VPN		
Clientless VPN	✓ Learn more	✓ Learn more
Mobile User—GlobalProtect Features		
Support for Multiple Username Formats	✓	✓
Mobile Device Management (MDM)	—	✓ Learn more
MDM Integration with HIP Prisma Access does not support AirWatch MDM HIP service integration; however, you can use the GlobalProtect App for iOS and Android MDM Integration for HIP-Based Policy Enforcement	✓	✓
Optimized Split Tunneling for GlobalProtect	✓	✓
Administratively Log Out Mobile Users	✓	✓ Learn more Introduced in version 1.4.
DHCP Prisma Access uses the IP address pools you specify during mobile user setup	—	—


Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
to assign IP addresses to mobile users and does not use DHCP.		
GlobalProtect App Version Controls	✓ One-click configuration for GlobalProtect agent log collection	✓ Learn more

Mobile Users—Explicit Proxy

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Explicit Proxy Support	✓ Learn more	✓ Learn more Introduced in 2.0 Innovation.
Explicit Proxy Connectivity in GlobalProtect for Always-On Internet Security	✓ Learn more Introduced in Prisma Access 4.0 Preferred with GlobalProtect app version 6.2	✓ Learn more Introduced in Prisma Access 4.0 Preferred with GlobalProtect app version 6.2

Security Services

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Security Policy	✓	✓
DoS Protection The Prisma Access infrastructure manages DoS protection.	✓	✓
SaaS Application Management	✓ Learn more Supported for:	—

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
	<ul style="list-style-type: none"> Microsoft 365 apps  <i>Includes a guided walkthrough to safely enable M365</i> <ul style="list-style-type: none"> Google apps Dropbox YouTube 	
Security Profiles		
Supported Profile Types	✓ <ul style="list-style-type: none"> Anti-Spyware DNS Security Vulnerability Protection WildFire and Antivirus URL Filtering File Blocking Data Loss Prevention (DLP) HTTP Header Insertion 	✓ <ul style="list-style-type: none"> Anti-Spyware DNS Security (enabled via an Anti-Spyware profile) Vulnerability Protection Antivirus WildFire URL Filtering File Blocking Data Loss Prevention (DLP)
Dashboards for Security Profiles	✓ Learn more Dashboards are tailored to each profile, and give you: <ul style="list-style-type: none"> centralized management for security service features visibility into profile usage and effectiveness access to cloud databases (search for threat coverage, for example) 	—
Best Practice Scores for Security Profiles	✓ Learn more	—

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Response pages	✓	✓ HTTP response pages are supported for mobile users and users at remote networks. To use HTTPS response pages, open a CLI session in the Panorama that manages Prisma Access, enter the set template Mobile_User_Template config deviceconfig settingssl-decrypt url-proxyyes command in configuration mode, and commit your changes.
HTTP Header Insertion		
HTTP Header Insertion Profiles	✓	✓
Decryption		
Decryption Policies	✓	✓
Decryption Profiles	✓	✓
Automatic SAN Support for SSL Decryption	✓	✓
Guided Walkthrough: Turn on Decryption	✓	—

Network Services

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Network Services		
Quality of Service (QoS)	✓	✓

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Prisma Access uses the same QoS policy rules and QoS profiles and supports the same Differentiated Services Code Point (DSCP) markings as Palo Alto Networks next-generation firewalls.		QoS for Remote network deployments that allocate bandwidth by compute location is introduced in version 3.0 Preferred.
Application Override	✓	✓
IPv4 Addressing	✓	✓
IPv6 Addressing You can access internal (private) apps that use IPv6 addressing . Introduced in version 2.2 preferred.	✓	✓
Split Tunnel Based on Access Route	✓	✓
Split Tunnel Based on Destination Domain, Client Process, and Video Streaming Application	✓	✓
NetFlow	—	—
NAT Prisma Access automatically manages outbound NAT; you cannot configure the settings.	✓	✓
SSL VPN Connections	✓	✓
Routing Features		
Static Routing	✓	✓
Dynamic Routing (BGP)	✓	✓
Dynamic Routing (OSPF)	—	—

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
High Availability		
High availability	Availability maintained by Palo Alto Networks.	✓
SMTP	✓ Prisma Access may block SMTP port 25 for security reasons and to mitigate the risk from known vulnerabilities that exploit non-secure SMTP. Palo Alto Networks recommends using ports 465, 587 or an alternate port 2525 for SMTP.	✓ Prisma Access may block SMTP port 25 for security reasons and to mitigate the risk from known vulnerabilities that exploit non-secure SMTP. Palo Alto Networks recommends using ports 465, 587 or an alternate port 2525 for SMTP.

Identity Services

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Authentication Types		
SAML	✓	✓
Cloud Identity Engine	✓ Requires 3.0 Innovation or a later Innovation release.	✓ Requires 3.0 Innovation or a later Innovation release.
TACACS+	✓	✓
RADIUS	✓	✓
LDAP	✓	✓ On-Premises LDAP Authentication
Kerberos	✓ Kerberos is supported for Windows clients only.	✓ Kerberos SSO
MFA	✓	✓

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
		Multi-Factor Authentication (MFA)
Local Database Authentication	✓	✓
Authentication Features		
Authentication Rules	✓	✓
Authentication Portal	✓	✓
Certificate-Based Authentication	✓ Supported for both IPSec and mobile users with GlobalProtect.	✓ Supported for both IPSec and mobile users with GlobalProtect.
RADIUS Vendor-Specific Attributes (VSAs)	—	—
Framed-IP-Address retrieval from RADIUS server	—	—
Extensible Authentication Protocol (EAP) Support for RADIUS	✓	✓
Single Sign-On (SSO)	✓	✓
Terminal Server (TS) Agent	✓ Supported for the following platforms: <ul style="list-style-type: none"> • Citrix XenApp 7.x • Windows Server 2019 • Windows 10 Enterprise Multi-session A maximum of 400 TS Agents are supported.	✓ Supported for the following platforms: <ul style="list-style-type: none"> • Windows Server 2019 • Windows 10 Enterprise Multi-session A maximum of 400 TS Agents are supported.
Cloud Identity Engine (Directory Sync Component)		
Directory Sync for User and Group-Based Policy	✓	✓

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
	Supports on-premises Active Directory and Azure Active Directory. <ul style="list-style-type: none"> • Learn more 	You can retrieve user and group information using the Directory Sync component of the Cloud Identity Engine . Prisma Access supports on-premises Active Directory, Azure Active Directory, and Google IdP. Introduced in version 1.6. Support for Azure Active Directory introduced in 2.0 Preferred. Support for Google IdP introduced in 3.0 Preferred and Innovation.
Identity Redistribution <ul style="list-style-type: none"> • IP-address-to-username mappings • HIP • Device Quarantine • IP-Tag • User-Tag 	✓	✓
Ingestion of IP-address-to-username mappings from 3rd party integration (NAC)	—	✓
Include username in HTTP header insertion entries	✓	✓ Introduced in version 1.7. Requires Panorama running 9.1.1 or later.

Policy Objects

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Addresses	✓	✓
Address Groups	✓	✓

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Dynamic Address Groups (DAGs) and Auto-Tags	✓	✓
XML API - Based DAG Updates	—	✓
Regions	✓	✓
Dynamic User Groups (DUGs)	✓	✓
App-ID (Applications)	✓	✓
Simplified Application Dependency Workflow (App Dependency tab for commits)	✓	— Commit warnings are not supported for Prisma Access.
Service-Based Session Timeouts	✓	✓ Learn more
Application Groups	✓	✓
Application Filters	✓	✓
Services	✓	✓
Service Groups	✓	✓
Tags	✓	✓
Streamlined Application-Based Policy (Tag-based application filters)	✓	✓ Introduced in version 1.7. Requires Panorama running 9.1.1 or later.
Auto-Tag Actions	✓	✓
HIP Objects		
HIP	✓	✓
HIP Match Log	✓	✓
HIP-Based Security Policy	✓	✓

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
HIP Notifications	✓	✓
HIP Report Submission	✓	✓
HIP Checks	✓	✓
HIP Report Viewing	—	✓ Introduced in version 1.5.
HIP Redistribution	✓	✓ Introduced in version 1.5.
HIP Objects and Profiles	✓	✓
External Dynamic Lists	✓	✓
Certificate Management		
Custom Certificates	✓	✓
Palo Alto Networks Issued Certificates	✓	✓
Certificate Profiles	✓	✓
Custom Certificates	✓	✓
SSL/TLS Service Profiles	✓	✓
SSL SSL is supported only for Mobile Users, not for site-to-site VPNs	✓	✓
SCEPs	✓	✓
OCSP Responders	✓	✓
Default Trusted Certificate Authorities	✓	✓

Logs

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Enhanced Application Logging	✓	✓
Cortex™ Data Lake Log Storage	✓	✓
Log Forwarding App Forward logs stored in Cortex Data Lake to syslog and email destinations	✓	✓
Log Forwarding Profiles	✓ Default log forwarding profile	✓ HTTP, SNMP, auto-tagging in Built-in Actions not supported
Enhanced Mobile Users Visibility for Administrators (GlobalProtect logs)	✓	✓ Introduced in version 1.7. Requires Panorama 9.1.1 or a later version. If you use Panorama running a 9.0 version, you can still see traffic and HIP logs from Panorama but you need to use the Explore app from the Hub to see the remaining logs.

Reports

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Reports	✓ Learn more	✓ Learn more Introduced in Prisma Access 1.8. Prisma Access supports running scheduled and

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
		<p>custom reports on Panorama with the following caveats:</p> <p>Run the scheduled or custom report under the All device group. Running a scheduled or custom report under a specific Device Group retrieves a blank report.</p> <p>You cannot search or sort the records in a report by specific device groups.</p>
App Report	✓ Learn more	<p>✓ Learn more</p> <p>This feature has the following Cortex Data Lake-based limitation:</p> <p>SaaS Application Usage report (Monitor > PDF Reports > SaaS Application Usage)—Cannot filter the logs for user groups (the Include user group information in the report choice is not supported)</p>
Usage Report	✓ Learn more	✓ Learn more
User Activity Report	✓ Learn more	✓ Learn more
Best Practices Report	✓	✓
WildFire Reports	✓	<p>✓</p> <p>Supported starting 2.0 Innovation.</p>
Reporting Engine Enhancements	—	✓

Integration with Other Palo Alto Networks Products

Feature	Prisma Access (Cloud-Managed)	Prisma Access (Panorama-Managed)
Cortex XSOAR integration	—	✓ Source IP-based allow lists and malicious user activity detection is supported.
Enterprise Data Loss Prevention (DLP) integration	✓	✓
Cortex XDR integration	✓ Prisma Access is compatible with the Cortex XDR version of Cortex Data Lake . Cortex XDR receives Prisma Access log information from Cortex Data Lake.	✓ Prisma Access is compatible with the Cortex XDR version of Cortex Data Lake . Cortex XDR receives Prisma Access log information from Cortex Data Lake.
Prisma SaaS integration	✓ SaaS visibility with Cortex Data Lake and VPN reverse SAML proxy are supported.	✓ SaaS visibility with Cortex Data Lake and VPN reverse SAML proxy are supported.
IoT Security Integration	—	✓ Introduced in version 2.0 Innovation.

Multitenancy Unsupported Features and Functionality

The following Prisma Access (Panorama Managed) features are not supported in a [multitenant deployment](#):

- [IoT Security](#)

In addition, a Panorama Managed multitenant deployment has changes to the following functionality:

- You cannot view your Panorama Managed tenants under [Common Services: Tenant Management](#).
- For Panorama-managed Prisma Access, continue to use Panorama for managing Prisma Access and the admin access that is controlled locally on Panorama. You cannot manage users, roles, and services accounts using [Common Services: Identity and Access](#) for Panorama-managed Prisma Access. However, you can use Common Services: Identity and Access for managing other apps such as ADEM and Insights.

- You cannot use the [Prisma Access APIs](#) in `pan-dev`.

The following Prisma Access components and add-ons have the following caveats when used in a multitenant deployment:

- For Prisma Access—Explicit Proxy deployments, if you have an existing Prisma Access non-multitenant deployment and [convert it to a multitenant deployment](#), only the first tenant (the tenant you migrated) supports Explicit Proxy. Any subsequent tenants you create for the multitenant deployment after the first do not support Explicit Proxy.
- [SaaS Security](#) and Enterprise Data Loss Prevention ([Enterprise DLP](#)) support multitenancy with the following restrictions:
 - Only a Superuser on Panorama can create DLP profiles and patterns and can associate DLP profiles to security policies for tenants.
 - A Superuser must commit all changes to Panorama whenever they make changes in DLP profiles and patterns.
 - All tenants share a single copy of profiles and pattern configurations; therefore, any changes done to them will be reflected across all tenants.
 - Since security policies can be different across tenants, each tenant can have different data filtering profiles associated with security policies.
- [Prisma SD-WAN](#) integration and [Configuring multiple portals in Prisma Access](#) can only be used with one tenant per multitenant deployment.
- If you enable High Availability (HA) with active and passive Panorama appliances in a multi-tenant deployment, you cannot change the HA pair association after you enable multi-tenancy.

Prisma Access and Panorama Version Compatibility

This section provides you with the minimum and maximum versions of Panorama™ to use with Prisma™ Access, along with the end-of-service (EoS) dates for Panorama software versions with Prisma Access.

- [Minimum Required Panorama Software Versions](#)
- [End-of-Support \(EoS\) Dates for Panorama Software Version Compatibility with Prisma Access](#)


Minimum Required Panorama Software Versions




The Cloud Services plugins require the following minimum Panorama™ software versions.





Due to the fast-paced release of Prisma Access and the Cloud Services plugin, the software [end-of-support \(EoS\) dates](#) for Panorama appliances used to manage Prisma Access can differ from the software end-of-life (EoL) dates for PAN-OS and Panorama releases. Note that these exceptions apply only to Panorama version compatibility with Prisma Access.

For FedRAMP deployment required Panorama versions, see [Panorama Managed Prisma Access FedRAMP Requirements](#).

Cloud Services Plugin Version	Minimum Required Panorama Version
4.0 and 4.1. Preferred	<ul style="list-style-type: none"> • PAN-OS 11.0.0 or a later PAN-OS 11.0 version • PAN-OS 10.2.3 or a later PAN-OS 10.2 version • PAN-OS 10.1.7 or a later PAN-OS 10.1 version <p>You must have a Panorama appliance running 10.2 to take advantage of the 10.2 features in Prisma Access.</p>
3.2.1 Preferred	<ul style="list-style-type: none"> • PAN-OS 11.0.0 or a later PAN-OS 11.0 version • PAN-OS 10.2.3 or a later PAN-OS 10.2 version <p> Only Cloud Services plugin versions 3.2 and 3.1.0-h50 or later support a Panorama running 10.2.3 or later. Do not upgrade your Panorama to PAN-OS 10.2.3 until after you upgrade your Cloud Services plugin to these minimum versions. No 10.2 Panorama versions earlier than 10.2.3 are supported.</p> <ul style="list-style-type: none"> • 10.1.7 or a later 10.1 version
3.2.1 Innovation	<ul style="list-style-type: none"> • PAN-OS 11.0 • PAN-OS 10.2.3 or a later PAN-OS 10.2 version.

Cloud Services Plugin Version	Minimum Required Panorama Version
	<ul style="list-style-type: none"> 10.1.7 or a later 10.1 version
3.2 Preferred	<ul style="list-style-type: none"> PAN-OS 10.2.3 or a later PAN-OS 10.2 version. <p> Only Cloud Services plugin versions 3.2 and 3.1.0-h50 or later support a Panorama running 10.2.3 or later. Do not upgrade your Panorama to PAN-OS 10.2.3 until after you upgrade your Cloud Services plugin to these minimum versions. No 10.2 Panorama versions earlier than 10.2.3 are supported.</p> <ul style="list-style-type: none"> 10.1.7 (10.1.8 recommended) or a later 10.1 version <p> While Panoramas running 10.1.7 are supported for use with 3.2, Palo Alto Networks recommends that you upgrade your Panorama to a minimum 10.1 version of 10.1.8 to support a future Panorama Managed Prisma Access release, to be released after the first quarter of calendar year 2023.</p>
3.2 Innovation	<ul style="list-style-type: none"> PAN-OS 10.2.3 or a later PAN-OS 10.2 version. 10.1.7 or a later 10.1 version
3.1 Preferred	<ul style="list-style-type: none"> PAN-OS 10.2.2-h1 or a later PAN-OS 10.2 version (minimum Cloud Services plugin version of 3.1.0-h50 required). <p> Only Cloud Services plugin version 3.1.0-h50 or later support a Panorama running 10.2.2-h1 or later. Do not upgrade your Panorama to PAN-OS 10.2.2-h1 until after you upgrade your Cloud Services plugin to this minimum version. No 10.2 Panorama versions earlier than 10.2.2-h1 are supported.</p> <p>Review the PAN-OS and Prisma Access Known Issues that are applicable to deployments with Panorama running PAN-OS 10.2.2 with Prisma Access 3.1.2.</p> <ul style="list-style-type: none"> PAN-OS 10.1.3 or a later PAN-OS 10.1 version. <p>You should upgrade your PAN-OS software to PAN-OS 10.1.4 or a later PAN-OS 10.1 version to incorporate an addressed issue (CYR-19816) that</p>

Cloud Services Plugin Version	Minimum Required Panorama Version
	<p>resolves a known issue found in earlier PAN-OS 10.1 versions.</p> <ul style="list-style-type: none"> PAN-OS 10.0.7 or a later PAN-OS 10.0 version.
3.1 Innovation	<p>PAN-OS 10.2.3 or a later PAN-OS 10.2 version.</p> <p>PAN-OS 10.1.3 or a later PAN-OS 10.1 version.</p> <p>If using a PAN-OS 10.1 version, you should upgrade your PAN-OS software to PAN-OS 10.1.4 or a later PAN-OS 10.1 version to incorporate an addressed issue (CYR-19816) that resolves a known issue found in earlier PAN-OS 10.1 versions.</p>
3.0	<ul style="list-style-type: none"> PAN-OS 10.1.2 or a later PAN-OS 10.1 version. <p> <i>FedRAMP Prisma Access deployments require Panorama running PAN-OS 10.1.8. Enabling the Processing Standard and Common Criteria (FIPS-CC mode) on the Panorama that manages Prisma Access is the recommended best practice aligned with FedRAMP controls.</i></p> <p>You should upgrade your PAN-OS software to PAN-OS 10.1.4 or a later PAN-OS 10.1 version to incorporate an addressed issue (CYR-19816) that resolves a known issue found in earlier PAN-OS 10.1 versions.</p> <ul style="list-style-type: none"> PAN-OS 10.0.7 or a later PAN-OS 10.0 version.
2.2 Preferred	<ul style="list-style-type: none"> PAN-OS 10.1. <p> <i>FedRAMP Prisma Access deployments require Panorama running PAN-OS 10.1.8. Enabling the Processing Standard and Common Criteria (FIPS-CC mode) on the Panorama that manages Prisma Access is the recommended best practice aligned with FedRAMP controls.</i></p> <p>You should upgrade your PAN-OS software to PAN-OS 10.1.4 or a later PAN-OS 10.1 version to incorporate an addressed issue (CYR-19816) that resolves a known issue found in earlier PAN-OS 10.1 versions.</p> <ul style="list-style-type: none"> PAN-OS 10.0.5 or a later PAN-OS 10.0 version.

End-of-Support (EoS) Dates for Panorama Software Version Compatibility with Prisma Access

When Prisma™ Access upgrades its infrastructure and dataplane after a major release, the upgrades can become incompatible with earlier Panorama™ versions. Because of the fast-paced release of Prisma Access and the Cloud Services plugin, the software compatibility end-of-support (EoS) dates for Panorama can differ from the software end-of-life dates for Panorama releases and apply to Panorama version compatibility with Prisma Access only.

If the Panorama appliance that manages Prisma Access is running a software version that is incompatible (not supported) with the upgrades, you must upgrade Panorama to a compatible version to take full advantage of the capabilities of the infrastructure and dataplane upgrades. It is our goal to make this process as seamless as possible and, for this reason, we make every effort to provide you with adequate notice of Panorama and Prisma Access version compatibility requirements.

Use the dates in the following table to learn when a Panorama software version that manages Prisma Access is no longer compatible with Prisma Access so that you can plan an upgrade to a supported version prior to the EoS date.



Due to the fast-paced release of Prisma Access and the Cloud Services plugin, the software compatibility end-of-support (EoS) dates for Panorama appliances used to manage Prisma Access can differ from the software end-of-life (EoL) dates for PAN-OS and Panorama releases. Note that these exceptions apply only to Panorama version compatibility with Prisma Access.



*To find the latest EoS compatibility information for your Panorama software with Prisma Access, log in to the Panorama appliance that manages Prisma Access, select the Service Setup page (**Panorama > Cloud Services > Configuration > Service Setup**), and view the **Panorama Alert** information. (See [Notifications and Alerts for Panorama, Cloud Services Plugin, and PAN-OS Dataplane Versions](#) for details.)*

Panorama Software Version	EoS Dates for Prisma Access Deployments
PAN-OS 10.0	March 1, 2023
PAN-OS 9.1	<p>August 1st, 2022</p> <p>Before this date, you must upgrade your Panorama to PAN-10.0 or a later supported (with Prisma Access) PAN-OS version.</p> <p>PAN-OS 10.1 is supported only after you upgrade to 2.2 Preferred or to the following 2.1 plugins:</p> <ul style="list-style-type: none"> • 2.1.0-h24 Preferred • 2.1.0-h16 Innovation

The Panorama upgrade is required regardless of the Cloud Services plugin version you are running at the EoS date. You cannot continue using an earlier version of the Cloud Services plugin with an earlier unsupported version of Panorama software.

The following Panorama software versions are already EoS and you cannot use them with Prisma Access:

- **PAN-OS 9.0**—EoS on February 1, 2021

Supported IKE Cryptographic Parameters

The following table documents the IKE cryptographic settings that are supported with Prisma™ Access.

Component	Phase 1 Supported Crypto Parameters	Phase 2 Supported Crypto Parameters
Encryption	3DES AES-128 AES-192 AES-256	Null (not recommended) DES 3DES AES-128-CBC AES-192-CBC AES-256-CBC AES-128-GCM AES-192-GCM AES-256-GCM
Authentication/Integrity	MD5 SHA-1 If you use IKEv2 with certificate-based authentication, only SHA1 is supported in IKE crypto profiles (Phase 1). SHA-256 SHA-384 SHA-512	None (supported with Galois/Counter Mode (GCM)) MD5 SHA-1 SHA-256 SHA-384 SHA-512
DH Group	Group 1 Group 2 Group 5 Group 14 Group 19 Group 20	No PFS (not recommended) Group 1 Group 2 Group 5 Group 14 Group 19 Group 20

Component	Phase 1 Supported Crypto Parameters	Phase 2 Supported Crypto Parameters
Security Association (SA) Lifetime	Configurable	Configurable
SA Lifebytes	N/A	Configurable

User-ID Agent

You install the User-ID™ agent on a domain server that is running a supported operating system (OS) and then connect the User-ID agent to exchange or directory servers.

- [Where Can I Install the User-ID Agent?](#)
- [Which Servers Can the User-ID Agent Monitor?](#)
- [Where Can I Install the User-ID Credential Service?](#)

Where Can I Install the User-ID Agent?

The following table shows the operating systems on which you can install each release of the Windows-based User-ID™ agent. The system must also meet the minimum requirements (see the [User-ID agent release notes](#)).

Operating System	Release 8.1*	Release 9.1	Release 10.0**	Release 10.1	Release 10.2	Release 11.0
Windows Server 2012 and 2012 R2	✓	✓	✓	✓	✓	✓
Windows Server 2016	✓	✓	✓	✓	✓	✓
Windows Server 2019	—	✓	✓	✓	✓	✓

* PAN-OS 8.1 is supported only on PA-200, PA-500, and PA-5000 Series firewalls (and the M-100 appliance) and only until each reaches its [hardware end-of-life \(EoL\) date](#).

** PAN-OS 10.0 is supported only on PA-7000 Series firewalls with PA-7000-20G-NPC or PA-7000-20GQ-NPC cards and only until these cards reach their [hardware end-of-life \(EoL\) date](#).

Which Servers Can the User-ID Agent Monitor?

The following are the exchange and directory servers you can monitor with the PAN-OS® integrated and Windows-based User-ID™ agents:



You can install only specific [releases](#) of the Windows-based User-ID agent on supported Microsoft Windows servers.

Server	Versions Supported
Microsoft Exchange Server	<ul style="list-style-type: none"> • 2019—Only with Windows User-ID agent 9.0.2 and later releases or with PAN-OS integrated User-ID agents running the following PAN-OS releases: <ul style="list-style-type: none"> • PAN-OS 11.0 (all releases) • PAN-OS 10.2 (all releases) • PAN-OS 10.1 (all releases) • PAN-OS 10.0 (all releases)* • PAN-OS 9.1 (all releases) • PAN-OS 8.1.8 and later PAN-OS 8.1 releases* • 2016—Only with Windows User-ID agent or with PAN-OS integrated User-ID agents running the following PAN-OS releases: <ul style="list-style-type: none"> • PAN-OS 11.0 (all releases) • PAN-OS 10.2 (all releases) • PAN-OS 10.1 (all releases) • PAN-OS 10.0 (all releases)* • PAN-OS 9.1 (all releases) • PAN-OS 8.1 (all releases)* • 2013
Microsoft Windows Server	<ul style="list-style-type: none"> • 2019—Only with Windows User-ID agent 9.0.2 and later releases or with PAN-OS integrated User-ID agents running the following PAN-OS releases: <ul style="list-style-type: none"> • PAN-OS 11.0 (all releases) • PAN-OS 10.2 (all releases) • PAN-OS 10.1 (all releases) • PAN-OS 10.0 (all releases)* • PAN-OS 9.1 (all releases) • PAN-OS 8.1.8 and later PAN-OS 8.1 releases*

Server	Versions Supported
	<ul style="list-style-type: none">• 2016—Only with Windows User-ID agent or with PAN-OS integrated User-ID agents running the following PAN-OS releases:<ul style="list-style-type: none">• PAN-OS 11.0 (all releases)• PAN-OS 10.2 (all releases)• PAN-OS 10.1 (all releases)• PAN-OS 10.0 (all releases)*• PAN-OS 9.1 (all releases)• PAN-OS 8.1 (all releases)*• 2012 and 2012 R2
Novell eDirectory Server	8.8

* PAN-OS 8.1 is supported only on PA-200, PA-500, and PA-5000 Series firewalls (and the M-100 appliance) and only until each reaches its [hardware end-of-life \(EoL\) date](#).

* PAN-OS 10.0 is supported only on PA-7000 Series firewalls with PA-7000-20G-NPC or PA-7000-20GQ-NPC cards and only until these cards reach their [hardware end-of-life \(EoL\) date](#).

Where Can I Install the User-ID Credential Service?

The following table shows the Read-Only Domain Controller (RODC) on which you can install each release of the Windows User-ID™ agent with the User-ID credential service to [detect credential submissions](#). The credential service is an add-on for the Windows User-ID agent; you must install the add-on separately.

Server	PAN-OS Version Supported	Windows User-ID Agent Version Supported
Windows Server 2019	<ul style="list-style-type: none">• 11.0• 10.2.3• 10.1.7• 10.0.11-h1*• 9.1.15	<ul style="list-style-type: none">• 11.0• 10.2.1• 10.0.6• 10.1.1• 9.1.4

* PAN-OS 10.0 is supported only on PA-7000 Series firewalls with PA-7000-20G-NPC or PA-7000-20GQ-NPC cards and only until these cards reach their [hardware end-of-life \(EoL\) date](#).

Terminal Server (TS) Agent

You install the Terminal Server (TS) agent on a domain server that is running a supported operating system (OS) and then report username-to-port mapping information to PAN-OS® firewalls.

- [Where Can I Install the Terminal Server \(TS\) Agent?](#)
- [How Many TS Agents Does My Firewall Support?](#)

Where Can I Install the Terminal Server (TS) Agent?

The following table shows the operating systems on which you can install each release of the Terminal Server (TS) agent.

Operating System	TS Agent 8.1 *	TS Agent 9.1	TS Agent 10.0**	TS Agent 10.1	TS Agent 10.2	TS Agent 11.0
Windows Server 2012 R2	✓	✓	✓	✓	✓	✓
Windows Server 2016	✓ 8.1.1 & later	✓	✓	✓	✓	✓
Windows Server 2019	—	✓	✓	✓	✓	✓
Windows 10 Enterprise Multi-session	—	✓ 9.1.1 & later	✓ 10.0.1 & later	✓	✓	✓
Citrix Metaframe Presentation Server 4.x	✓	✓	✓	✓	✓	✓
Citrix XenApp 5.x	✓	✓	✓	✓	✓	✓
Citrix XenApp 6.x	✓	✓	✓	✓	✓	✓
Citrix XenApp 7.x	✓	✓	✓	✓	✓	✓

* PAN-OS 8.1 is supported only on PA-200, PA-500, and PA-5000 Series firewalls (and the M-100 appliance) and only until each reaches its [hardware end-of-life \(EoL\) date](#).

** PAN-OS 10.0 is supported only on PA-7000 Series firewalls with PA-7000-20G-NPC or PA-7000-20GQ-NPC cards and only until these cards reach their [hardware end-of-life \(EoL\) date](#).

How Many TS Agents Does My Firewall Support?

The following table shows how many Terminal Server (TS) agents each hardware-based and VM-Series firewall supports. To confirm which PAN-OS® releases are supported on your firewall, review the [Supported PAN-OS releases for each model](#).



For optimal configuration, install the TS agent version that matches the PAN-OS version running on the firewall. If there is not a TS agent version that matches the PAN-OS version, install the latest version that is closest to the PAN-OS version.

Firewall or VM Model	PAN-OS 9.1	PAN-OS 10.0*	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Hardware Firewalls					
PA-7000 Series	2,000	2,000	2,000	2,000	2,000
PA-7000 Series with SMC-B	2,500	2,500	2,500	2,500	2,500
PA-5450	—	—	2,500	2,500	2,500
PA-5440	—	—	—	—	2,500
PA-5430	—	—	—	400	400
PA-5420					
PA-5410					
PA-5200 Series	2,500	—	2,500	2,500	2,500
PA-3440	—	—	—	2,000	2,000
PA-3430					
PA-3420	—	—	—	400	400
PA-3410					
PA-3200 Series	2,000	—	2,000	2,000	2,000
PA-3000 Series	400	—	—	—	—
PA-1400 Series	—	—	—	—	400
PA-800 Series	1,000	—	1,000	1,000	1,000
PA-460	—	—	1,000	1,000	1,000

Firewall or VM Model	PAN-OS 9.1	PAN-OS 10.0*	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
PA-450	—	—	400	400	400
PA-445	—	—	—	—	800
PA-440	—	—	800	800	800
PA-415	—	—	—	—	400
PA-410	—	—	400 10.1.2 & later	400	400
PA-220R	400	—	400	400	400
PA-220	400	—	400	400	—

VM-Series Firewalls

VM-700	2,500	—	2,500	2,500	2,500
VM-500	2,000	—	2,000	2,000	2,000
VM-300	400	—	400	400	400
VM-100	400	—	400	400	400
VM-50 Lite	400	—	400	400	400

* PAN-OS 10.0 is supported only on PA-7000 Series firewalls with PA-7000-20G-NPC or PA-7000-20GQ-NPC cards and only until these cards reach their [hardware end-of-life \(EoL\) date](#).

Cortex Data Lake

- [Cortex Data Lake Software Compatibility](#)


Cortex Data Lake Software Compatibility

To forward firewall log data to Cortex® Data Lake, you must ensure that your firewalls are running a supported PAN-OS® version. The PAN-OS version you need depends on whether you [use Panorama™ to onboard several firewalls simultaneously](#) or you [onboard firewalls individually](#).

To onboard firewalls to Cortex Data Lake using Panorama, you must also install a supported version of the Cloud Services plugin. If you use the Cloud Services plugin to enable Prisma™ Access, ensure that your Panorama is running [supported versions](#) of PAN-OS and the Cloud Services plugin.

Version Requirements for Panorama-Managed Firewalls

Software versions required to integrate a Panorama-managed deployment with Cortex Data Lake.

Software	Version	Description
PAN-OS*	Minimum: <ul style="list-style-type: none"> Americas and Europe: PAN-OS 8.1; PAN-OS 8.1.3 or later recommended Other regions: PAN-OS 9.1 	<p>To forward logs from Panorama-managed firewalls to Cortex Data Lake in the Americas or Europe regions, both Panorama and the firewalls must run PAN-OS 8.1 or a later version. Forwarding logs to any other region requires Panorama to be running PAN-OS 9.1 or a later supported PAN-OS version.</p> <p>For enhanced application logging and more reliable service, upgrade to PAN-OS 8.1.3 or a later PAN-OS 8.1* version or to PAN-OS 9.1 or a later supported version.</p>
Cloud Services plugin	Minimum: <ul style="list-style-type: none"> Americas and Europe: 1.4.0 Other regions: 1.5.0-h6 Recommended: the latest version	<p>The Cloud Services plugin enables you to send log data from Panorama-managed firewalls. To download the plugin, see the step describing how to install the plugin when you configure Panorama for Cortex Data Lake.</p> <p> <i>Ensure that your Panorama is running a PAN-OS version that supports your Cloud Services plugin version. Failure to do so can result in a loss of data.</i></p>

* PAN-OS 8.1 is supported only on PA-200, PA-500, and PA-5000 Series firewalls (and the M-100 appliance) and only until each reaches its [hardware end-of-life \(EoL\) date](#).

Version Requirements for Individually Managed Firewalls

Software	Version	Description
PAN-OS	Minimum: PAN-OS 9.1	Individually managed firewalls must run PAN-OS 9.1 or a later supported PAN-OS version to authenticate to Cortex Data Lake.

Software	Version	Description
Content Version	Minimum: 8274	Install the latest content updates to ensure your firewall can authenticate to Cortex Data Lake.

Cortex XDR



Compatibility information for Cortex XDR® has a new home. Going forward, when you click the links below, you will be redirected to the [Palo Alto Networks docs-cortex website](#).

- [Where Can I Install the Cortex XDR Agent?](#)
- [Cortex XDR Supported Kernel Module Versions by Distribution](#)
- [Cortex XDR and Traps Compatibility with Third-Party Security Products](#)

Where Can I Install the Cortex XDR Agent?

The Traps™ agent is now the Cortex XDR® agent in Cortex XDR agent release 7.0 and later releases.



Compatibility information for Cortex XDR (and Traps) has a new home. Going forward, you can determine [where you can install the Cortex XDR agent](#) by going to the [Palo Alto Networks docs-cortex website](#).

Cortex XDR Supported Kernel Module Versions by Distribution

On Linux endpoints, to perform malware analysis of Executable and Linkable Format (ELF) files and to collect data for endpoint detection and response (EDR) and behavioral threat analysis, the Cortex XDR® agent requires Linux kernel 3.4 or a later version. If you deploy the Cortex XDR agent on a Linux server that is not running one of the kernel versions required for these additional protection capabilities, the agent will operate in *asynchronous mode*. Go to the [Palo Alto Networks docs-cortex website](#) to learn more about [Cortex XDR supported kernel module versions](#).

Cortex XDR and Traps Compatibility with Third-Party Security Products

We renamed the Traps™ agent as the Cortex XDR® agent in Cortex XDR agent release 7.0 and later releases.

You can review [considerations related to third-party security software integration with Cortex XDR and Traps software](#) by visiting the [Palo Alto Networks docs-cortex website](#).

Endpoint Security Manager (ESM)

You can install the Traps™ agent, now known as the Cortex XDR® agent, and the Endpoint Security Manager (ESM) Components (comprised of the ESM Console, one or more ESM Servers, and the database) only on servers and endpoints that are running a supported operating system (OS).

- [Where Can I Install the Endpoint Security Manager \(ESM\)?](#)
- [Where Can I Install the Cortex XDR Agent?](#)

Where Can I Install the Endpoint Security Manager (ESM)?

The Endpoint Security Manager (ESM) comprises the ESM Console, one or more ESM Servers, and a database. You can install the ESM components on dedicated servers or install them on the same server as long as you install them on a supported operating system (OS).

Server Operating System	ESM 4.2
Windows Server 2008 R2	✓
Windows Server 2012	✓
Windows Server 2012 R2	✓
Windows Server 2016	✓
Windows Server 2019	✓ *4.2.6 & later

Where Can I Install the Cortex XDR Agent?

The Traps™ agent is now the Cortex XDR® agent in Cortex XDR agent release 7.0 and later releases.



Compatibility information for Cortex XDR (and Traps) has a new home. Going forward, you can determine [where you can install the Cortex XDR agent](#) by going to the [Palo Alto Networks docs-cortex website](#).

IPv6 Support by Feature

- [IPv6 Support by Feature](#)

IPv6 Support by Feature

Use the following table to review PAN-OS® features (listed by category) that support IPv6 traffic.

- [Security](#)
- [Management & Panorama](#)
- [Networking](#)
- [VPN](#)
- [Host Dynamic Address Configuration](#)
- [Device](#)
- [User-ID](#)

PAN-OS Feature	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Security					
WildFire® Appliance	—	—	✓	✓	✓
App-ID™ and Firewalling in Layer 2 and Layer 3	✓	✓	✓	✓	✓
User-ID™	✓	✓	✓	✓	✓
Content-ID™	✓	✓	✓	✓	✓
Block IPv6 in IPv4 Tunneling (via App-ID)	✓	✓	✓	✓	✓
Zone Protection	✓	✓	✓	✓	✓
Packet-Based Attack Protection	✓	✓	✓	✓	✓
Reconnaissance Protection	✓	✓	✓	✓	✓
URL Filtering	✓	✓	✓	✓	✓
SSL Decryption	✓	✓	✓	✓	✓
SSH Decryption	✓	✓	✓	✓	✓
DoS Rulebase	✓	✓	✓	✓	✓
IPv6 Access to PAN-DB	✓	✓	✓	✓	✓

PAN-OS Feature	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
DNS Sinkhole	✓	✓	✓	✓	✓
External Dynamic List (EDL)	✓	✓	✓	✓	✓
Management & Panorama™					
SSH Management (dedicated MGMT port)	✓	✓	✓	✓	✓
Web Interface Management (dedicated MGMT port)	✓	✓	✓	✓	✓
Interface Management (ping, telnet, ssh, http, https - all ports)	✓	✓	✓	✓	✓
Device to Panorama SSL TCP Connection	✓	✓	✓	✓	✓
Panorama HA Connection Between Peers	✓	✓	✓	✓	✓
DNS	✓	✓	✓	✓	✓
Dynamic DNS Support for Firewall Interfaces (DHCP-based interfaces)	—	✓	✓	✓	✓
RADIUS	✓	✓	✓	✓	✓
LDAP	✓	✓	✓	✓	✓
SYSLOG	✓	✓	✓	✓	✓
SNMP	✓	✓	✓	✓	✓
NTP	✓	✓	✓	✓	✓
Device DNS (device only)	✓	✓	✓	✓	✓
DNS Proxy	✓	✓	✓	✓	✓
Reporting and Visibility in to IPv6	✓	✓	✓	✓	✓
IPv6 Address Objects	✓	✓	✓	✓	✓
IPv6 FQDN Address Objects	✓	✓	✓	✓	✓

PAN-OS Feature	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Networking					
IPv6 Static Routes	✓	✓	✓	✓	✓
PBF	✓	✓	✓	✓	✓
PBF Next-Hop Monitor (v6 endpoint)	✓	✓	✓	✓	✓
OSPFv3	✓	✓	✓	✓	✓
MP-BGP	✓	✓	✓	✓	✓
GRE Tunneling Support	—	✓	✓	✓	✓
ECMP	✓	✓	✓	✓	✓
Dual Stack Support for L3 Interfaces	✓	✓	✓	✓	✓
QoS Policy	✓	✓	✓	✓	✓
QoS Marking	✓	✓	✓	✓	✓
DSCP (session based)	✓	✓	✓	✓	✓
Neighbor Discovery and Duplicate Address Detection	✓	✓	✓	✓	✓
Tunnel Content Inspection	✓	✓	✓	✓	✓
Virtual Wires	✓	✓	✓	✓	✓
NPTv6 (stateless prefix translation)	✓	✓	✓	✓	✓
NAT64 (IP-IPv6 protocol translation)	✓	✓	✓	✓	✓
LLDP (Link Layer Discovery Protocol)	✓	✓	✓	✓	✓
Bidirectional Forwarding Detection (BFD)	✓	✓	✓	✓	✓
VPN					

PAN-OS Feature	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
GlobalProtect™	✓	✓	✓	✓	✓
IKE/IPSec	✓	✓	✓	✓	✓
IKEv2	✓	✓	✓	✓	✓
IPv6 over IPv4 IPSec Tunnel	✓	✓	✓	✓	✓
Large Scale VPN (LSVPN)	✓	✓	✓	✓	✓
Host Dynamic Address Configuration					
DHCPv6 Relay	✓	✓	✓	✓	✓
DHCPv6 Client with Prefix Delegation (Dataplane Interface only)	—	—	—	—	✓
SLAAC (Router Advertisements)	✓	✓	✓	✓	✓
SLAAC (Router Preference)	✓	✓	✓	✓	✓
SLAAC (RDNSS)	✓	✓	✓	✓	✓
Device					
High Availability (HA)—Active/Active	✓	✓	✓	✓	✓
HA—Active/Passive	✓	✓	✓	✓	✓
HA—IPv6 transport for HA1 & HA2	✓	✓	✓	✓	✓
HA Path Monitoring (IPv6 Endpoint)	✓	✓	✓	✓	✓
HA Clustering	—	—	✓	✓	✓
User-ID					
Map IPv6 Address to Users	✓	✓	✓	✓	✓
Captive Portal for IPv6	✓	✓	✓	✓	✓

PAN-OS Feature	PAN-OS 8.1*	PAN-OS 9.1	PAN-OS 10.1	PAN-OS 10.2	PAN-OS 11.0
Connection to User-ID Agents over IPv6	✓	✓	✓	✓	✓
User-ID XML API for IPv6	✓	✓	✓	✓	✓
Terminal Server Agent IPv6	✓	✓	✓	✓	✓

* PAN-OS 8.1 is supported only on PA-200, PA-500, and PA-5000 Series firewalls and the M-100 appliance and only until each reaches its [hardware end-of-life \(EoL\) date](#).

Mobile Network Infrastructure Feature Support

Specific Palo Alto Networks firewall models support GTP and SCTP security and 3GPP Technical Standards:

- [PAN-OS Releases by Model that Support GTP, SCTP, and 5G Security](#)
- [3GPP Technical Standard References](#)

PAN-OS Releases by Model that Support GTP, SCTP, and 5G Security

The following table lists which firewall models support GTP Security, SCTP Security, and 5G Security.

Firewall Model	PAN-OS 9.1 (GTP and SCTP)	PAN-OS 10.1 (GTP, SCTP, and 5G)	PAN-OS 10.2 (GTP, SCTP, and 5G)	PAN-OS 11.0 (GTP, SCTP, and 5G)
VM-Series firewalls	✓	✓	✓	✓
PA-7000 Series firewalls that use three of the following cards*: <ul style="list-style-type: none"> PA-7000-100G-NPC card; PA-7000-LFC-A card; and PA-7050-SMC-B card OR PA-7080-SMC-B card	✓	✓	✓	✓
PA-5450 firewalls	—	✓	✓	✓
PA-5400 Series firewalls	—	—	✓	✓
PA-5200 Series firewalls	✓	✓	✓	✓
PA-3430 and PA-3440 firewalls	—	—	✓	✓
CN-Series firewalls	—	✓	✓	✓

* To verify that your PA-7000 Series firewall is installed with the cards that support GTP and SCTP, use the **show chassis inventory** CLI command. However, it is possible that cards are installed but not functional if not all dependencies are met. Refer to the [PA-7000 Series Firewall Hardware Reference](#) for installation instructions and to review the dependencies for each card.



CN-Series Daemonset mode supports GTP, SCTP, and 5G security in PAN-OS 10.1 and later versions. CN-Series firewalls running PAN-OS 10.2 support GTP, SCTP, and 5G security on K8s cloud-native network (CNF) mode and Daemonset mode.

3GPP Technical Standard References

3GPP Technical Standards references of mobile network security features for PAN-OS® releases on [firewalls that support GTP security](#).

- [3GPP TS References for GTP Security](#)
- [3GPP TS References for 5G Security](#)
- [3GPP TS References for 5G Multi-Edge Security](#)

3GPP TS References for GTP Security

3GPP TS references for GTP security on [firewalls that support GTP security](#).

	Protocol	3GPP TS	3GPP TS Release
PAN-OS 10.2	GTPv2-C	29.274	Up to 15.2
PAN-OS 10.1	GTPv1-C	29.060	Up to 15.5.0
	GTP-U	29.281	Up to 15.0.0
	—	43.129	15.0.0
	—	23.401	15.12.0
PAN-OS 9.1	GTPv2-C	29.274	Up to 15.2
	GTPv1-C	29.060	Up to 15.1
	GTP-U	29.281	Up to 15.0.0
PAN-OS 8.1 (only where supported)	GTPv2-C	29.274	Up to 13.4
	GTPv1-C	29.060	Up to 13.4
	GTP-U	29.281	Up to 13.0

3GPP TS References for 5G Security

3GPP Technical Standards references for 5G network slice, 5G subscriber ID, and 5G equipment ID security on [firewalls that support GTP security](#).

- Procedures for the 5G System (5GS)
- 5GS Session Management Services

	3GPP TS	3GPP TS Release
PAN-OS 10.2	23.502	Up to 15.5.0
PAN-OS 10.1	29.502	Up to 15.4.0

3GPP TS References for 5G Multi-Edge Security

[5G Multi-Edge Security](#) supports Packet Forwarding Control Protocol (PFCP) messages over N4 interfaces for the following technical specifications in the 3GPP TS release:

- Interface between the Control Plane and the User Plane nodes

3GPP Technical Standards reference for 5G Multi-Edge Security on firewalls that support 5G MEC Security:

	3GPP TS	3GPP TS Release
PAN-OS 10.2	29.244	Up to 16.5.0
PAN-OS 10.1		

3GPP TS References for UE-to-IP Address Correlation with PFCP in 4G

The below table provides the 3GPP Technical Standards reference for firewalls that leverage User Equipment (UE)-to-IP Address Correlation using the Packet Forwarding Control Protocol (PFCP) for 4G network traffic.

	3GPP TS	3GPP TS Release
PAN-OS 11.0	23.214	Up to 16.2.0
	29.244	Up to 16.9.1