

# **VM-Series Deployment Guide**

Version 8.0

## Contact Information

Corporate Headquarters:

Palo Alto Networks

4401 Great America Parkway

Santa Clara, CA 95054

[www.paloaltonetworks.com/company/contact-support](http://www.paloaltonetworks.com/company/contact-support)

## About this Guide

This guide describes how to set up and license the VM-Series firewall; it is intended for administrators who want to deploy the VM-Series firewall.

For more information, refer to the following sources:

- For information on the additional capabilities of and instructions for configuring the features on your firewall, refer to <https://www.paloaltonetworks.com/documentation>.
- For access to the knowledge base, complete documentation set, discussion forums, and videos, refer to <https://live.paloaltonetworks.com>.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to <https://www.paloaltonetworks.com/support/tabs/overview.html>.
- For the most current PAN-OS 8.0 release notes, go to <https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os-release-notes.html>.

To provide feedback on the documentation, please write to us at: [documentation@paloaltonetworks.com](mailto:documentation@paloaltonetworks.com).

Palo Alto Networks, Inc.

[www.paloaltonetworks.com](http://www.paloaltonetworks.com)

© 2017 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies.

**Revision Date: June 12, 2017**



# Table of Contents

---

About the VM-Series Firewall .....	9
VM-Series Models .....	10
VM-Series System Requirements .....	10
CPU Oversubscription .....	11
VM-Series Deployments .....	13
VM-Series in High Availability .....	15
Upgrade the VM-Series Firewall .....	16
Upgrade the PAN-OS Software Version (Standalone Version) .....	16
Upgrade the PAN-OS Software Version (VM-Series for NSX) .....	17
Upgrade the VM-Series Model .....	19
Upgrade the VM-Series Model in an HA Pair .....	21
Upgrade Panorama 7.1 to Panorama 8.0 .....	22
Enable Jumbo Frames on the VM-Series Firewall .....	23
Hypervisor Assigned MAC Addresses .....	24
 License the VM-Series Firewall .....	 25
License Types—VM-Series Firewalls .....	26
VM-Series Firewall for NSX Licenses .....	26
VM-Series Firewall in Amazon Web Services (AWS) and Azure Licenses .....	26
Serial Number and CPU ID Format for the VM-Series Firewall .....	28
Create a Support Account .....	29
Register the VM-Series Firewall .....	30
Register the VM-Series Firewall (with auth code) .....	30
Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code) .....	31
Switch Between the BYOL and the PAYG Licenses .....	33
Activate the License .....	35
Activate the License for the VM-Series Firewall (Standalone Version) .....	35
Activate the License for the VM-Series Firewall for VMware NSX .....	36
Deactivate the License(s) .....	39
Install a License Deactivation API Key .....	39
Deactivate a Feature License or Subscription Using the CLI .....	40
Deactivate VM .....	41
Licensing API .....	45
Manage the Licensing API Key .....	45
Use the Licensing API .....	46
Licensing API Error Codes .....	49
Licenses for Cloud Security Service Providers (CSSPs) .....	50
Get the Auth Codes for CSSP License Packages .....	50
Register the VM-Series Firewall with a CSSP Auth Code .....	51
Add End-Customer Information for a Registered VM-Series Firewall .....	52

<b>Set Up a VM-Series Firewall on an ESXi Server .....</b>	<b>55</b>
Supported Deployments on VMware vSphere Hypervisor (ESXi) .....	56
VM-Series on ESXi System Requirements and Limitations .....	57
Requirements .....	57
Limitations .....	58
Install a VM-Series firewall on VMware vSphere Hypervisor (ESXi) .....	59
Plan the Interfaces for the VM-Series for ESXi .....	59
Provision the VM-Series Firewall on an ESXi Server .....	60
Perform Initial Configuration on the VM-Series on ESXi .....	63
Add Additional Disk Space to the VM-Series Firewall .....	64
Use VMware Tools on the VM-Series Firewall on ESXi and vCloud Air .....	65
Troubleshoot ESXi Deployments .....	68
Basic Troubleshooting .....	68
Installation Issues .....	68
Licensing Issues .....	70
Connectivity Issues .....	71
Performance Tuning of the VM-Series for ESXi .....	73
Install the NIC Driver on ESXi .....	73
Enable DPDK on ESXi .....	75
Enable SR-IOV on ESXi .....	75
Enable Multi-Queue Support for NICs on ESXi .....	76
 <b>Set Up the VM-Series Firewall on vCloud Air .....</b>	 <b>77</b>
About the VM-Series Firewall on vCloud Air .....	78
Deployments Supported on vCloud Air .....	79
Deploy the VM-Series Firewall on vCloud Air .....	80
 <b>Set Up a VM-Series Firewall on the Citrix SDX Server .....</b>	 <b>87</b>
About the VM-Series Firewall on the SDX Server .....	88
System Requirements and Limitations .....	89
Requirements .....	89
Limitations .....	89
Supported Deployments—VM Series Firewall on Citrix SDX .....	91
Scenario 1—Secure North-South Traffic .....	91
Scenario 2—Secure East-West Traffic (VM-Series Firewall on Citrix SDX) .....	94
Install the VM-Series Firewall on the SDX Server .....	95
Upload the Image to the SDX Server .....	95
Provision the VM-Series Firewall on the SDX Server .....	95
Secure North-South Traffic with the VM-Series Firewall .....	97
Deploy the VM-Series Firewall Using L3 Interfaces .....	97
Deploy the VM-Series Firewall Using Layer 2 (L2) or Virtual Wire Interfaces .....	101
Deploy the VM-Series Firewall Before the NetScaler VPX .....	103
Secure East-West Traffic with the VM-Series Firewall .....	106



<b>Set Up the VM-Series Firewall on VMware NSX .....</b>	<b>109</b>
VM-Series for NSX Firewall Overview .....	110
What are the Components of the VM-Series for NSX Solution? .....	110
How Do the Components in the VM-Series Firewall for NSX Solution Work Together? .....	113
What are the Benefits of the NSX VM-Series firewall for NSX Solution? .....	118
What is Multi-Tenant Support on the VM-Series Firewall for NSX? .....	119
VM-Series Firewall for NSX Deployment Checklist .....	121
Install the VMware NSX Plugin .....	123
Register the VM-Series Firewall as a Service on the NSX Manager .....	124
Enable Communication Between the NSX Manager and Panorama .....	124
Create Template(s) and Device Group(s) on Panorama .....	126
Create the Service Definitions on Panorama .....	127
Create Steering Rules .....	133
Deploy the VM-Series Firewall .....	137
Enable SpoofGuard .....	137
Define an IP Address Pool .....	138
Prepare the ESXi Host for the VM-Series Firewall .....	139
Deploy the Palo Alto Networks NGFW Service .....	140
Apply Policies to the VM-Series Firewall .....	145
Enable Large Receive Offload .....	148
Steer Traffic from Guests that are not Running VMware Tools .....	150
Dynamically Quarantine Infected Guests .....	151
Use Case: Shared Compute Infrastructure and Shared Security Policies .....	156
Use Case: Shared Security Policies on Dedicated Compute Infrastructure .....	161
Dynamic Address Groups—Information Relay from NSX Manager to Panorama .....	168
<b>Set Up the VM-Series Firewall on AWS .....</b>	<b>175</b>
About the VM-Series Firewall on AWS .....	176
VM-Series Firewall on AWS GovCloud .....	176
AWS Terminology .....	176
Management Interface Mapping for Use with Amazon ELB .....	178
Deployments Supported on AWS .....	180
Deploy the VM-Series Firewall on AWS .....	183
Obtain the AMI .....	183
Review System Requirements and Limitations for VM-Series on AWS .....	185
Planning Worksheet for the VM-Series in the AWS VPC .....	185
Launch the VM-Series Firewall on AWS .....	187
Use the VM-Series Firewall CLI to Swap the Management Interface .....	194
Enable CloudWatch Monitoring on the VM-Series Firewall .....	195
High Availability for VM-Series Firewall on AWS .....	198
Overview of HA on AWS .....	198
IAM Roles for HA .....	199
HA Links .....	200
Heartbeat Polling and Hello Messages .....	200
Device Priority and Preemption .....	201
HA Timers .....	201

Configure Active/Passive HA on AWS . . . . .	202
Use Case: Secure the EC2 Instances in the AWS Cloud . . . . .	207
Use Case: Use Dynamic Address Groups to Secure New EC2 Instances within the VPC. . . . .	219
Use Case: Deploy the VM-Series Firewalls to Secure Highly Available Internet-Facing Applications on AWS	223
Solution Overview—Secure Highly Available Internet-Facing Applications . . . . .	223
Deploy the Solution Components for Highly Available Internet-Facing Applications on AWS	225
Set Up the VPC . . . . .	226
Deploy the VM-Series Firewalls in the VPC. . . . .	228
Launch the VM-Series Firewalls and the NetScaler VPX. . . . .	229
Configure the VM-Series Firewall for Securing Outbound Access from the VPC. . . . .	232
Configure the Firewalls that Secure the Web Farm . . . . .	234
Configure the Firewall that Secures the RDS. . . . .	236
Deploy the Web Farm in the VPC . . . . .	237
Set Up the Amazon Relational Database Service (RDS). . . . .	239
Configure the Citrix NetScaler VPX. . . . .	241
Set up Amazon Route 53. . . . .	243
Verify Traffic Enforcement . . . . .	244
Port Translation for Service Objects . . . . .	245
Use Case: VM-Series Firewalls as GlobalProtect Gateways on AWS . . . . .	247
Components of the GlobalProtect Infrastructure . . . . .	248
Deploy GlobalProtect Gateways on AWS . . . . .	248
Auto Scale VM-Series Firewalls with the Amazon ELB . . . . .	250
What Components Does the VM-Series Auto Scaling Template for AWS Deploy? . . . . .	251
How Does the VM-Series Auto Scaling Template for AWS Enable Dynamic Scaling? . . . . .	253
Plan the VM-Series Auto Scaling Template for AWS . . . . .	254
Launch the VM-Series Auto Scaling Template for AWS . . . . .	261
Customize the Bootstrap.xml File . . . . .	275
Use the GitHub Bootstrap Files as Seed. . . . .	275
Create a new Bootstrap File from Scratch . . . . .	276
NAT Policy Rule and Address Objects in the Auto Scaling Template . . . . .	278
Stack Update with VM-Series Auto Scaling Template for AWS (v1.2) . . . . .	279
Modify Administrative Account and Update Stack. . . . .	283
Troubleshoot the VM-Series Auto Scaling Template for AWS. . . . .	283
List of Attributes Monitored on the AWS VPC. . . . .	290
IAM Permissions Required for Monitoring the AWS VPC. . . . .	290
<b>Set Up the VM-Series Firewall on KVM. . . . .</b>	<b>293</b>
VM-Series on KVM— Requirements and Prerequisites. . . . .	294
System Requirements . . . . .	294
Options for Attaching the VM-Series on the Network . . . . .	295
Prerequisites for VM-Series on KVM . . . . .	295
Supported Deployments on KVM. . . . .	298
Secure Traffic on a Single Host . . . . .	298
Secure Traffic Across Linux hosts . . . . .	298
Install the VM-Series Firewall on KVM . . . . .	300
Enable the Use of a SCSI Controller . . . . .	306

Verify PCI-ID for Ordering of Network Interfaces on the VM-Series Firewall .....	306
Use an ISO File to Deploy the VM-Series Firewall .....	307
Performance Tuning of the VM-Series for KVM .....	311
Install KVM and Open vSwitch on Ubuntu 16.04.1 LTS .....	311
Enable Open vSwitch on KVM .....	311
Integrate Open vSwitch with DPDK .....	312
Enable SR-IOV on KVM .....	316
Enable Multi-Queue Support for NICs on KVM .....	317
Isolate CPU Resources in a NUMA Node on KVM .....	317
<b>Set Up the VM-Series Firewall on Hyper-V .....</b>	<b>321</b>
Supported Deployments on Hyper-V .....	322
Secure Traffic on a Single Hyper-V Host .....	322
Secure Traffic Across Multiple Hyper-V Hosts .....	322
System Requirements on Hyper-V .....	324
Linux Integration Services .....	324
Install the VM-Series Firewall on Hyper-V .....	325
Before You Begin .....	325
Performance Tuning of the VM-Series Firewall on Hyper-V .....	326
Provision the VM-Series Firewall on a Hyper-V host with Hyper-V Manager .....	326
Provision the VM-Series Firewall on a Hyper-V host with PowerShell .....	328
Perform Initial Configuration on the VM-Series Firewall .....	329
<b>Set up the VM-Series Firewall on Azure .....</b>	<b>333</b>
About the VM-Series Firewall on Azure .....	334
Azure Networking and VM-Series .....	334
VM-Series Firewall Templates on Azure .....	335
Minimum System Requirements for the VM-Series on Azure .....	335
Deployments Supported on Azure .....	337
Deploy the VM-Series Firewall from the Azure Marketplace (Solution Template) .....	338
Use the ARM Template to Deploy the VM-Series Firewall .....	344
Deploy the VM-Series and Azure Application Gateway Template .....	348
VM-Series and Azure Application Gateway Template .....	349
Start Using the VM-Series & Azure Application Gateway Template .....	350
Deploy the Template to Azure .....	350
VM-Series and Azure Application Gateway Template Parameters .....	354
Sample Configuration File .....	355
Adapt the Template .....	356
<b>Set Up the VM-Series Firewall on OpenStack .....</b>	<b>357</b>
VM-Series Firewall for OpenStack .....	358
Components of the VM-Series for OpenStack Solution .....	358
Orchestration with the Heat Template .....	359
VM-Series Firewall on OpenStack Deployment Checklist .....	362
Install the VM-Series Firewall in OpenStack .....	363

<b>Bootstrap the VM-Series Firewall .....</b>	<b>367</b>
VM-Series Firewall Bootstrap Workflow .....	368
Bootstrap Package .....	369
Bootstrap Configuration Files .....	371
Generate the VM Auth Key on Panorama .....	372
Create the init-cfg.txt File .....	374
Create the bootstrap.xml File .....	377
Prepare the Licenses for Bootstrapping .....	378
Prepare the Bootstrap Package .....	379
Bootstrap the VM-Series Firewall on ESXi .....	380
Bootstrap the VM-Series Firewall on ESXi with an ISO .....	380
Bootstrap the VM-Series Firewall on ESXi with a Block Storage Device .....	380
Bootstrap the VM-Series Firewall on Hyper-V .....	382
Bootstrap the VM-Series Firewall on Hyper-V with an ISO .....	382
Bootstrap the VM-Series Firewall on Hyper-V with a Block Storage Device .....	382
Bootstrap the VM-Series Firewall on KVM .....	384
Bootstrap the VM-Series Firewall on KVM with an ISO .....	384
Bootstrap the VM-Series Firewall on KVM With a Block Storage Device .....	385
Bootstrap the VM-Series Firewall on KVM in OpenStack .....	385
Bootstrap the VM-Series Firewall in AWS .....	389
Bootstrap the VM-Series Firewall in Azure .....	391
Verify Bootstrap Completion .....	393
Bootstrap Errors .....	394



# About the VM-Series Firewall

---

The Palo Alto Networks VM-Series firewall is the virtualized form of the Palo Alto Networks next-generation firewall. It is positioned for use in a virtualized or cloud environment where it can protect and secure east-west and north-south traffic.

- ▲ [VM-Series Models](#)
- ▲ [VM-Series Deployments](#)
- ▲ [VM-Series in High Availability](#)
- ▲ [Upgrade the VM-Series Firewall](#)
- ▲ [Enable Jumbo Frames on the VM-Series Firewall](#)
- ▲ [Hypervisor Assigned MAC Addresses](#)

## VM-Series Models

The VM-Series firewall is available in the following models—VM-50, VM-100, VM-200, VM-300, VM-500, VM-700, and VM-1000-HV.

All models can be deployed as guest virtual machines on VMware ESXi and vCloud Air, Citrix NetScaler SDX, Amazon Web Services, KVM and KVM in OpenStack, and Microsoft Hyper-V and Azure; on VMware NSX, only the VM-100, VM-200, VM-300, VM-500, and VM-1000-HV firewalls are supported. The software package (.xva, .ova, or .vhdx file) that is used to deploy the VM-Series firewall is common across all models.

When you apply the capacity [license](#) on the VM-Series firewall, the model number and the associated capacities are implemented on the firewall. Capacity is defined in terms of the number of sessions, rules, security zones, address objects, IPsec VPN tunnels, and SSL VPN tunnels that the VM-Series firewall is optimized to handle. To make sure that you purchase the correct model for your network requirements, use the following table to understand the maximum capacity for each model and the capacity differences by model:

Model	Sessions	Security Rules	Dynamic IP Addresses	Security Zones	IPsec VPN Tunnels	SSL VPN Tunnels
VM-50	50,000	250	1,000	15	250	250
VM-100 VM-200	250,000	1,500	2,500	40	1,000	500
VM-300 VM-1000-HV	800,000	10,000	100,000	40	2,000	2,000
VM-500	2,000,000	10,000	100,000	200	4,000	6,000
VM-700	10,000,000	20,000	100,000	200	8,000	12,000

For information on the platforms on which you can deploy the VM-Series firewall, see [VM-Series Deployments](#). For more information about the VM-Series firewall models, see the Palo Alto Networks Firewall [comparison tool](#). You can also review general information [About the VM-Series Firewall](#).

- ▲ [VM-Series System Requirements](#)
- ▲ [CPU Oversubscription](#)

## VM-Series System Requirements

Each instance of the VM-Series firewall requires a minimum resource allocation—number of CPUs, memory, and disk space, on its host server. Use the table below to verify that you allocate the necessary hardware resources for your VM-Series model.



When upgrading to 8.0 or the VM-Series model license, you may be required to allocate additional hardware resources before completing your upgrade.



VM-Series Model	Supported Hypervisors	Supported vCPUs	Minimum Memory	Minimum Hard Drive
VM-50	ESXi, KVM, Hyper-V	2	4.5GB	32GB (60GB at boot)
VM-100 VM-200	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2	6.5GB	60GB
VM-300 VM-1000-HV	ESXi, KVM, Hyper-V, AWS, Azure, NSX, SDX	2, 4	9GB	60GB
VM-500	ESXi, KVM, Hyper-V, AWS, Azure, NSX	2, 4, 8	16GB	60GB
VM-700	ESXi, KVM, Hyper-V, AWS, Azure	2, 4, 8, 16	56GB	60GB



To achieve the best performance, all of the needed cores should be available on a single CPU socket.



For operation, the VM-50 firewall requires minimum 32GB of hard drive space. However, because the VM-Series base image is common to all models, you must allocate 60GB of hard drive space until you license the VM-50.

The number of vCPUs assigned to the management plane and those assigned to the dataplane differs depending on the total number of vCPUs assigned to the VM-Series firewall. If you assign more vCPUs than those officially supported by the license, any additional vCPUs are assigned to the management plane.

Total vCPUs	Management Plane vCPUs	Dataplane vCPUs
2	1	1
4	2	2
8	2	6
16	4	12

## CPU Oversubscription

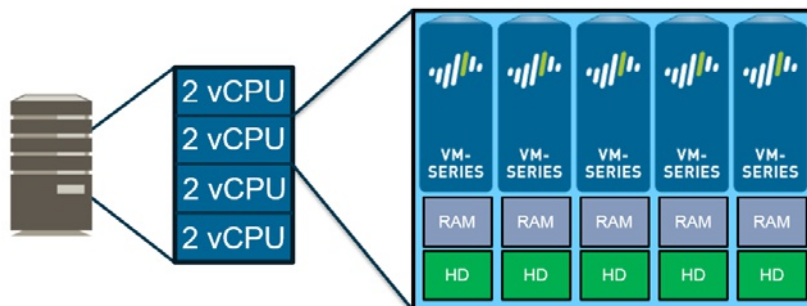
The VM-Series firewall supports CPU oversubscription on all models. CPU oversubscription allows you deploy a higher density of VM-Series firewalls on hypervisors running on x86 architecture. You can deploy two (2:1) to five (5:1) VM-Series firewalls per required allocation of CPUs. When planning your deployment, use the following formula to calculate the number of VM-Series firewalls your hardware can support.

$(\text{Total CPUs} \times \text{Oversub Ratio}) / \text{CPUs per firewall} = \text{total number of VM-Series firewalls}$

For example, at a 5:1 ratio, a host machine with 16 physical CPU and at least 180GB of memory ( $40 \times 4.5\text{GB}$ ) can support up to 40 instances to the VM-50. Each VM-50 requires two vCPUs and five VM-50s can be associated to each pair of vCPUs.

$(16 \text{ CPUs} \times 5) / 2 = 40 \text{ VM-50 firewalls}$

Beyond meeting the minimum [VM-Series System Requirements](#), no additional configuration is required to take advantage of oversubscription. Deploy VM-Series firewalls normally and resource oversubscription occurs automatically. When planning your deployment, consider other functions, such as virtual switches, and guest machines on the host that require hardware resources of their own.

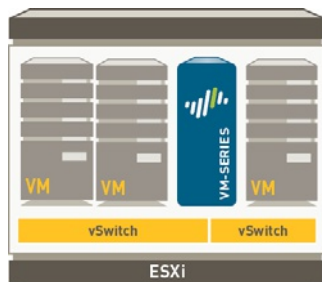


## VM-Series Deployments

The VM-Series firewall can be deployed on the following platforms:

❑ **VM-Series for VMware vSphere Hypervisor (ESXi) and vCloud Air**

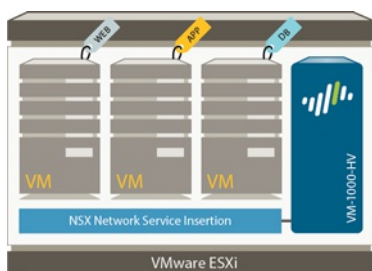
You can deploy any VM-Series model as a guest virtual machine on VMware ESXi; ideal for cloud or networks where virtual form factor is required.



For details, see [Set Up a VM-Series Firewall on an ESXi Server](#) and [Set Up the VM-Series Firewall on vCloud Air](#).

❑ **VM-Series for VMware NSX**

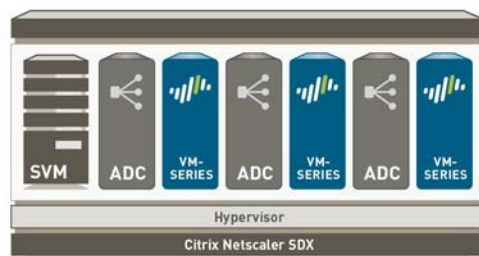
The VM-100, VM-200, VM-300, VM-500, or VM-1000-HV is deployed as a network introspection service with VMware NSX, and Panorama. This deployment is ideal for east-west traffic inspection, and it also can secure north-south traffic.



For details, see [Set Up the VM-Series Firewall on VMware NSX](#)

❑ **VM-Series for Citrix SDX**

VM-100, VM-200, VM-300, or VM-1000-HV is deployed as guest virtual machine on Citrix NetScaler SDX; consolidates ADC and security services for multi-tenant and Citrix XenApp/XenDesktop deployments.



For details, see [Set Up a VM-Series Firewall on the Citrix SDX Server](#)

❑ **VM-Series for Amazon Web Services (AWS)**

You can deploy any VM-Series model, except the VM-50, on EC2 instances on the AWS Cloud.

For details, see [Set Up the VM-Series Firewall on AWS](#).

❑ **VM-Series for Kernel Virtualization Module (KVM)**

You can deploy any VM-Series model on a Linux server that is running the KVM hypervisor. For details, see [Set Up the VM-Series Firewall on KVM](#).

❑ **VM-Series for Microsoft Hyper-V**

You can deploy any VM-Series model on a Windows Server 2012 R2 server with the Hyper-V role add-on enabled or a standalone Hyper-V 2012 R2 server. For details, see [Set Up the VM-Series Firewall on Hyper-V](#).

❑ **VM-Series for Microsoft Azure**

You can deploy any VM-Series model, except the VM-50, on the Azure VNet.

For details, see [Set up the VM-Series Firewall on Azure](#).

❑ **VM-Series for OpenStack**

You can deploy any VM-Series model on KVM in your OpenStack environment. For details, see [Set Up the VM-Series Firewall on OpenStack](#).

## VM-Series in High Availability

High availability (HA) is a configuration in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up the firewalls in a two-device cluster provides redundancy and allows you to ensure business continuity. In an HA configuration on the VM-Series firewalls, both peers must be deployed on the same type of hypervisor, have identical hardware resources (such as CPU cores/network interfaces) assigned to them, and have the set same of licenses/subscriptions. For general information about HA on Palo Alto Networks firewalls, see [High Availability](#).

The VM-Series firewalls support stateful active/passive or active/active high availability with session and configuration synchronization. The only exceptions are the following:

- The VM-Series firewall on the Amazon Web Services (AWS) cloud supports active/passive HA only. For details, see [High Availability for VM-Series Firewall on AWS](#).
- HA is not relevant for the [VM-Series firewall for VMware NSX](#).



The active/active deployment is supported in virtual wire and Layer 3 deployments, and is only recommended for networks with asymmetric routing.

Features/ Links Supported	ESX	KVM	SDX	AWS	NSX	Hyper-V	Azure
Active/Passive HA	Yes	Yes	Yes	Yes	No	Yes	No
Active/Active HA	Yes	Yes	Yes	No	No	Yes	No
HA 1	Yes	Yes	Yes	Yes	No	Yes	No
HA2—(session synchronization and keepalive)	Yes	Yes	Yes	Yes	No	Yes	No
HA3	Yes	Yes	Yes	No	No	Yes	No

For instructions on configuring the VM-Series firewall as an HA pair, see [Configure Active/Passive HA](#) and [Configure Active/Active HA](#).

# Upgrade the VM-Series Firewall

- ▲ [Upgrade the PAN-OS Software Version \(Standalone Version\)](#)
- ▲ [Upgrade the PAN-OS Software Version \(VM-Series for NSX\)](#)
- ▲ [Upgrade the VM-Series Model](#)
- ▲ [Upgrade the VM-Series Model in an HA Pair](#)
- ▲ [Upgrade Panorama 7.1 to Panorama 8.0](#)

For instructions on installing your VM-Series firewall, see [VM-Series Deployments](#).

## Upgrade the PAN-OS Software Version (Standalone Version)

Now that the VM-Series firewall has network connectivity and the base PAN-OS software is installed, consider upgrading to the latest version of PAN-OS. Use the following instructions for firewalls that are not deployed in a high availability (HA) configuration. For firewalls deployed in HA, refer to the [PAN-OS 8.0 New Features Guide](#).

### Upgrade PAN-OS Version (Standalone Version)

- 
- Step 1** Verify that there enough hardware resources available to the VM-Series firewall. Refer to the [VM-Series System Requirements](#) to see the new resource requirements for each VM-Series model. Allocate additional hardware resources before continuing the upgrade process. The process for assigning additional hardware resources differs on each hypervisor.
- 
- Step 2** From the web interface, navigate to **Device > Licenses** and make sure you have the correct VM-Series firewall license and that the license is activated.  
On the VM-Series firewall standalone version, navigate to **Device > Support** and make sure that you have activated the support license.
- 
- Step 3** (Required for a firewall that is in production) Save a backup of the current configuration file.
1. Select **Device > Setup > Operations** and click **Export named configuration snapshot**.
  2. Select the XML file that contains your running configuration (for example, **running-config.xml**) and click **OK** to export the configuration file.
  3. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.
- 
- Step 4** Check the Release Notes to verify the Content Release version required for the PAN-OS version. The firewalls you plan to upgrade must be running the Content Release version required for the PAN-OS version.
1. Select **Device > Dynamic Updates**.
  2. Check the **Applications and Threats** or **Applications** section to determine what update is currently running.
  3. If the firewall is not running the required update or later, click **Check Now** to retrieve a list of available updates.
  4. Locate the desired update and click **Download**.
  5. After the download completes, click **Install**.
-



### Upgrade PAN-OS Version (Standalone Version)

**Step 5** Upgrade the PAN-OS version on the VM-Series firewall.

1. Select **Device > Software**.
2. Click **Refresh** to view the latest software release and also review the **Release Notes** to view a description of the changes in a release and to view the migration path to install the software.
3. Click **Download** to retrieve the software then click **Install**.

**Step 6** If you are upgrading from PAN-OS 7.1 to PAN-OS 8.0, transition your VM-Series firewall from a 40GB hard disk to a 60GB hard disk.

1. On your hypervisor, attach a new 60GB hard drive to the VM-Series firewall. This new disk must be 60GB. The firewall will return an error if another value is assigned.
2. Access the firewall CLI.
3. Use the following CLI command to create a new disk partition to copy the data from the original system disk to the new system disk.  

```
> request system clone-system-disk target sdb
```
4. Return to your hypervisor and power off the VM-Series firewall.
5. Remove the original system disk.
6. Power on the VM-Series firewall.

## Upgrade the PAN-OS Software Version (VM-Series for NSX)

For the VM-Series Firewall NSX edition, use Panorama to upgrade the software version on the firewalls.

### Upgrade VM-Series NSX Edition Firewalls Using Panorama

**Step 1** Allocate additional hardware resources to your VM-Series firewall.

Verify that there are enough hardware resources available to the VM-Series firewall. Refer to the [VM-Series System Requirements](#) to see the new resource requirements for each VM-Series model. Allocate additional hardware resources before continuing the upgrade process. The process for assigning additional hardware resources differs on each hypervisor.

**Step 2** Save a backup of the current configuration file on each managed firewall that you plan to upgrade.



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

1. Select **Device > Setup > Operations** and click **Export Panorama and devices config bundle**. This option is used to manually generate and export the latest version of the configuration backup of Panorama and of each managed device.
2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

## Upgrade VM-Series NSX Edition Firewalls Using Panorama (Continued)

**Step 3** Check the Release Notes to verify the Content Release version required for the PAN-OS version.

The firewalls you plan to upgrade must be running the Content Release version required for the PAN-OS version.

1. Select **Panorama > Device Deployment > Dynamic Updates**.
2. Check for the latest updates. Click **Check Now** (located in the lower left-hand corner of the window) to check for the latest updates. The link in the **Action** column indicates whether an update is available. If a version is available, the **Download** link displays.



3. Click **Download** to download a selected version. After successful download, the link in the **Action** column changes from **Download** to **Install**.
4. Click **Install** and select the devices on which you want to install the update. When the installation completes, a check mark displays in the **Currently Installed** column.

**Step 4** Deploy software updates to selected firewalls.



If your firewalls are configured in HA, make sure to clear the **Group HA Peers** check box and upgrade one HA peer at a time.

1. Select **Panorama > Device Deployment > Software**.
2. Check for the latest updates. Click **Check Now** (located in the lower left-hand corner of the window) to check for the latest updates. The link in the **Action** column indicates whether an update is available.
3. Review the **File Name** and click **Download**. Verify that the software versions that you download match the firewall models deployed on your network. After successful download, the link in the **Action** column changes from **Download** to **Install**.
4. Click **Install** and select the devices on which you want to install the software version.
5. Select **Reboot device after install**, and click **OK**.
6. If you have devices configured in HA, clear the **Group HA Peers** check box and upgrade one HA peer at a time.

**Step 5** Verify the software and Content Release version running on each managed device.

1. Select **Panorama > Managed Devices**.
2. Locate the device(s) and review the content and software versions on the table.

		Status						
Device Group	Device Name	Conn...	Template	Software Version	Apps and Threat	Antivirus	URL Filtering	GlobalProtect Client
▼ Branch (1/1 Devices Connected)								
Branch	SupportFW-07	<input checked="" type="checkbox"/>	In sync	5.0.0	347-1647	862-1186	4061	1.1.3
								15901-23121

## Upgrade the VM-Series Model

The licensing process for the VM-Series firewall uses the UUID and the CPU ID to generate a unique serial number for each VM-Series firewall. Hence, when you generate a license, the license is mapped to a specific instance of the VM-Series firewall and cannot be modified.

Use the instructions in this section, if you are:

- Migrating from an evaluation license to a production license.
- Upgrading the model to allow for increased capacity. For example you want to upgrade from the VM-100 to the VM-300 license.

Upgrade the VM-Series Capacity	
<b>Step 1</b> Enable automatic VM-Series license deactivation.	Before upgrading your VM-Series firewall capacity, <a href="#">Install a License Deactivation API Key</a> .

## Upgrade the VM-Series Capacity (Continued)

**Step 2** Upgrade the license on the Customer Support portal.



Skip this step if you are upgrading the capacity with an authorization code.

1. Log in to the Palo Alto Networks [Customer Support](#) portal.
2. Select **Assets > Devices** and search for your firewall by the serial number.
3. Select the Action icon to open the Device Licenses window.
4. Select **Activate Upgrade License** and enter the authorization code for the higher capacity VM.

5. Select **Agree and Submit**.
6. (Optional) If your VM-Series firewall does not have direct internet access, download the capacity upgrade license key.
  - a. Select **Assets > Devices** and search for your firewall by the serial number.
  - b. Under the License column, select the download icon next to PA-VM to download the license key.
  - c. Save the license key to a location the VM-Series firewall can access.

**Step 3** Allocate additional hardware resources to your VM-Series firewall.

Before initiating the capacity upgrade, you must verify that enough hardware resources are available to the VM-Series firewall to support the new capacity. The process for assigning additional hardware resources differs on each hypervisor.

To check the hardware requirements for your new VM-Series model, see [VM-Series Models](#).

Although the capacity upgrade does not require a reboot of the VM-Series firewall, you need to power down the virtual machine to change the hardware allocation.

## Upgrade the VM-Series Capacity (Continued)

<b>Step 4</b> Upgrade the capacity.	Select <b>Device &gt; Licenses &gt; Upgrade Capacity</b> and then activate your licenses and subscriptions in one of the following ways: <ul style="list-style-type: none"> <li>• <b>Retrieve license keys from license server</b>—Use this option if you activated your license on the <a href="#">Customer Support</a> portal.</li> <li>• <b>Manually upload license key</b>—Use this option if your firewall does not have connectivity to the <a href="#">Palo Alto Networks Customer Support web site</a>. In this case, you must download a license key file from the support site on an Internet connected computer and then upload to the firewall.</li> <li>• <b>Use an authorization code</b>—Use this option to upgrade the VM-Series capacity using an authorization code for licenses that have not been previously activated on the support portal. When prompted, enter the <b>Authorization Code</b> and then click <b>OK</b>.</li> </ul>
<b>Step 5</b> Verify that your firewall capacity license upgrade is successful.	On the <b>Device &gt; Licenses</b> page, verify that the license was successfully activated.

## Upgrade the VM-Series Model in an HA Pair

Because a license upgrade requires some critical processes to restart, pairing firewalls into HA mode is recommended to minimize the impact to service. This process is similar to that of upgrading the PAN-OS version of an HA pair. During the upgrade process, session synchronization continues, if you have it enabled.



Configuration sync is automatically disabled when a capacity mismatch is detected and remains disabled until the mismatch is resolved. Therefore, configuration changes during the upgrade process are not recommended. If the firewalls in the HA pair have different major software versions (such as 7.1 and 8.0) and different capacities, both devices will enter the Suspend state. Therefore, it is recommended that you make sure both firewalls are running the same version of PAN-OS before upgrading the capacity.

## Upgrade the Capacity License in an Active-Passive HA Pair

<b>Step 1</b> Upgrade the capacity license of the passive firewall.	Follow the procedure to <a href="#">Upgrade the VM-Series Capacity</a> . After critical processes restart on passive device, it will be the new VM-Series model. This upgraded firewall enters the non-functional state due to the capacity mismatch between it and the active firewall.
<b>Step 2</b> Upgrade the capacity license of the active firewall.	Follow the procedure to <a href="#">Upgrade the VM-Series Capacity</a> . When the capacity upgrade of the active firewall is complete, the passive firewall then becomes active. After the critical processes restart, the previously active firewall enters the initial state and becomes the passive pair member with its new capacity.

## Upgrade Panorama 7.1 to Panorama 8.0

When you upgrade Panorama in your VMware NSX deployment from 7.1 to 8.0, all your existing configuration is maintained. However, that configuration will remain in pre-8.0 formats and any configuration you create after upgrading will be in post-8.0 formats. Complete the following procedure to move your pre-8.0 configuration into post 8.0 formats.

Move Pre-8.0 Configuration to Post-8.0 Configuration	
<b>Step 1</b> Upgrade Panorama.	The VMware NSX plugin is automatically installed upon upgrade to 8.0.
<b>Step 2</b> Update the match criteria format in your dynamic address groups.	<ol style="list-style-type: none"> <li>1. Select <b>Objects &gt; Address Groups</b> and click the link name for your first dynamic address group.</li> <li>2. Delete the existing match criteria entry.</li> <li>3. Enter the new match criteria in the following format: <code>'_nsx_&lt;dynamic-address-group-name&gt;'</code></li> <li>4. Click <b>OK</b>.</li> <li>5. Repeat this process for each dynamic address group.</li> </ol>
<b>Step 3</b> Change security policy used as NSX steering rules to intrazone.	<ol style="list-style-type: none"> <li>1. Select <b>Policies &gt; Security &gt; Pre Rules</b> and click the link name for your first security policy rule.</li> <li>2. On the General tab, change the <b>Rule Type</b> to intrazone.</li> <li>3. Click <b>OK</b>.</li> <li>4. Repeat this process for each security policy rule.</li> </ol>
<b>Step 4</b> Generate new steering rules.	<ol style="list-style-type: none"> <li>1. Select <b>Panorama &gt; VMware NSX &gt; Steering Rules</b>.</li> <li>2. Click <b>Auto-Generate Steering Rules</b>.</li> </ol>
<b>Step 5</b> Commit your changes.	<p>When you commit your changes, Panorama pushes updates to NSX Manager.</p> <ol style="list-style-type: none"> <li>1. Verify that NSX Manager created new security groups. <ol style="list-style-type: none"> <li>a. Login to vCenter and select <b>Networking &amp; Security &gt; Security Groups</b>.</li> <li>b. The new security groups (mapped to the updated dynamic address groups) should appear in the following format: <code>&lt;service-definition-name&gt; - &lt;dynamic-address-group-name&gt;</code></li> </ol> </li> <li>2. Verify that NSX Manager created new steering rules. <ol style="list-style-type: none"> <li>a. Select <b>Networking &amp; Security &gt; Firewall &gt; Configuration &gt; Partner security services</b>.</li> <li>b. The new steering rules (mapped to the security policy rules you create on Panorama) are listed above the old steering rules.</li> </ol> </li> </ol>
<b>Step 6</b> Delete the old steering rules from vCenter.	<ol style="list-style-type: none"> <li>1. Select <b>Networking &amp; Security &gt; Firewall &gt; Configuration &gt; Partner security services</b>.</li> <li>2. Delete the old steering rules.</li> </ol>
<b>Step 7</b> Delete the old security groups from vCenter.	<ol style="list-style-type: none"> <li>1. Select <b>Networking &amp; Security &gt; Security Groups</b>.</li> <li>2. Delete the old security groups.</li> </ol>




## Enable Jumbo Frames on the VM-Series Firewall

By default, the maximum transmission unit (MTU) size for packets sent on a Layer 3 interface is 1500 bytes. This size can be manually set to any size from 512 to 1500 bytes on a per-interface basis. Some configurations require Ethernet frames with an MTU value greater than 1500 bytes. These are called jumbo frames.

To use jumbo frames on a firewall you must specifically enable jumbo frames at the global level. When this is enabled, the default MTU size for all Layer 3 interfaces is set to a value of 9192 bytes. This default value can then be set to any value in the range of 512 to 9216 bytes.

After setting a global jumbo frame size it becomes the default value for all Layer 3 interfaces that have not explicitly had an MTU value set at the interface configuration level. This can become a problem if you only want to exchange jumbo frames on some interfaces. In these situations, you must set the MTU value at every Layer 3 interface that you do not want to use the default value.

The following procedure describes how to enable jumbo frames on a firewall, set the default MTU value for all Layer 3 interfaces and to then set a different value for a specific interface.

Enable Jumbo Frames and Set MTU Values	
<p><b>Step 1</b> Enable jumbo frames and set a default global MTU value.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Session</b> and edit the Session Settings section.</li> <li>2. Select <b>Enable Jumbo Frame</b>.</li> <li>3. Enter a value for <b>Global MTU</b>. The default value is 9192. The range of acceptable values is: 512 - 9216.</li> <li>4. Click <b>OK</b>. A message is displayed that informs you that enabling or disabling Jumbo Frame mode requires a reboot and that Layer 3 interfaces inherit the <b>Global MTU</b> value.</li> <li>5. Click <b>Yes</b>. A message is displayed to inform you that Jumbo Frame support has been enabled and reminds you that a device reboot is required for this change to be activated.</li> <li>6. Click <b>OK</b>.</li> <li>7. Click <b>Commit</b>.</li> </ol>
<p><b>Step 2</b> Set the MTU value for a Layer 3 interface and reboot the firewall.</p> <p> The value set for the interface overrides the global MTU value.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Network &gt; Interfaces</b>.</li> <li>2. Select an interface of the Layer3 <b>Interface type</b>.</li> <li>3. Select <b>Advanced &gt; Other Info</b>.</li> <li>4. Enter a value for <b>MTU</b>. The default value is 9192. The range of acceptable values is: 512 - 9216.</li> <li>5. Click <b>OK</b>.</li> <li>6. Click <b>Commit</b>.</li> <li>7. Select <b>Device &gt; Setup &gt; Operations</b> and select <b>Reboot Device</b>.</li> </ol>

## Hypervisor Assigned MAC Addresses

By default, the VM-Series firewall uses the MAC address assigned to the physical interface by the host/hypervisor and use that MAC address on the VM-Series firewall deployed with Layer 3 interfaces. The firewall can then use the hypervisor assigned MAC address in its ARP responses. This capability allows non-learning switches, such as the VMware vSwitch to forward traffic to the dataplane interface on the firewall without requiring that promiscuous mode be enabled on the vSwitch. If neither promiscuous mode nor the use of hypervisor assigned MAC address is enabled, the host will drop the frame when it detects a mismatch between the destination MAC address for an interface and the host-assigned MAC address.



There is no option to enable or disable the use of hypervisor assigned MAC addresses on AWS and Azure. It is enabled by default for both platforms and cannot be disabled.

If you are deploying the VM-Series firewall in Layer 2, virtual wire, or tap interface modes, you must enable promiscuous mode on the virtual switch to which the firewall is connected. The use of hypervisor assigned MAC address is only relevant for Layer 3 deployments where the firewall is typically the default gateway for the guest virtual machines.

When you enable hypervisor assigned MAC address functionality on the VM-Series firewall, make note of the following requirements:

- **IPv6 Address on an Interface**—In an active/passive [HA configuration](#), Layer 3 interfaces using IPv6 addresses must not use the EUI-64 generated address as the interface identifier (Interface ID). Because the EUI-64 uses the 48-bit MAC address of the interface to derive the IPv6 address for the interface, the IP address is not static. This results in a change in the IP address for the HA peer when the hardware hosting the VM-Series firewall changes on failover, and leads to an HA failure.
- **Lease on an IP Address**—When the MAC address changes, DHCP client, DHCP relay and PPPoE interfaces might release the IP address because the original IP address lease could terminate.
- **MAC address and Gratuitous ARP**—VM-Series firewalls with hypervisor assigned MAC addresses in a high-availability configuration behave differently than the hardware appliances with respect to MAC addressing. Hardware firewalls use self-generated floating MAC addresses between devices in an HA pair, and the unique MAC address used on each dataplane interface (say eth 1/1) is replaced with a virtual MAC address that is common to the dataplane interface on both HA peers. When you enable the use of the hypervisor assigned MAC address on the VM-Series firewall in HA, the virtual MAC address is not used. The dataplane interface on each HA peer is unique and as specified by the hypervisor.

Because each dataplane interface has a unique MAC address, when a failover occurs, the now active VM-Series firewall must send a gratuitous ARP so that neighboring devices can learn the updated MAC/IP address pairing. Hence, to enable a stateful failover, the internetworking devices must not block or ignore gratuitous ARPs; make sure to disable the anti-ARP poisoning feature on the internetworking devices, if required.

### Disable Use of Hypervisor Assigned MAC Address

To allow the VM-Series firewall to use the interface MAC addresses provided by the host/hypervisor:

**Step 1** Select **Device > Management > Setup**.

**Step 2** Disable (clear) the option to **Use Hypervisor Assigned MAC Address**.

When the MAC address change occurs, the firewall generates a system log to record this transition and the interface generates a gratuitous ARP.

**Step 3** **Commit** the change on the firewall. You do not need to reboot the firewall.



# License the VM-Series Firewall

---

Before you can start using your VM-Series firewall to secure east-west and north-south traffic on your network, you must activate the licenses for the services you purchased to secure your network.

If you are an authorized CSSP partner, see [Licenses for Cloud Security Service Providers \(CSSPs\)](#) for information that pertains to you.

For details on creating a support account and activating the licenses:

- ▲ [License Types—VM-Series Firewalls](#)
- ▲ [Serial Number and CPU ID Format for the VM-Series Firewall](#)
- ▲ [Create a Support Account](#)
- ▲ [Register the VM-Series Firewall](#)
- ▲ [Switch Between the BYOL and the PAYG Licenses](#)
- ▲ [Activate the License](#)
- ▲ [Deactivate the License\(s\)](#) (to release the licenses attributed to a firewall)
- ▲ [Licensing API](#)
- ▲ [Licenses for Cloud Security Service Providers \(CSSPs\)](#)

## License Types—VM-Series Firewalls

The following licenses and subscriptions are available for the VM-Series firewall:

- **Capacity License**—The VM-Series firewall requires a base license, also called a *capacity license*, to enable the model number (VM-100, VM-200, VM300, or VM-1000-HV) and the associated capacities on the firewall. Capacity licenses can be perpetual or term-based:
  - **Perpetual License**—A license with no expiration date, it allows you to use the VM-Series firewall at the licensed capacity, indefinitely. Perpetual licenses are available for the VM-Series capacity license only.
  - **Term-Based License**—A term-based license allows you to use the VM-Series firewall for a specified period of time. It has an expiration date and you will be prompted to renew the license before it expires. Term-based licenses are available for the capacity licenses, support entitlements, and subscriptions.

Further, capacity licenses are available as an Individual version or an Enterprise version. The Individual version is in multiples of 1. The orderable SKU, for example PA-VM-300, includes an auth code to license one instance of the VM-Series firewall. The Enterprise version is available in multiples of 25. For example, the orderable SKU PAN-VM-100-ENT has a single auth code that allows you to register 25 instances of the VM-100.

- **Support**—In addition to the capacity license, you need a support entitlement that provides access to technical support and software updates.
- **Subscriptions**—Optionally, you may purchase one or more subscription licenses for Threat Prevention, PAN-DB URL Filtering, AutoFocus™, GlobalProtect™, and WildFire™. These subscriptions allow you to enforce policies that safely enable applications and content on the network. For example, the Threat Prevention subscription, allows you to obtain content updates that include the most up-to-date threat information for malware detection.

## VM-Series Firewall for NSX Licenses

In order to automate the provisioning and licensing of the VM-Series firewall for NSX in the VMware integrated NSX solution, two license bundles are available:

- One bundle includes the VM-Series capacity license (VM-100, VM-200, VM-300, VM-500, or VM-1000-HV only), Threat Prevention license and a premium support entitlement.
- Another bundle includes the VM-Series capacity license (VM-100, VM-200, VM-300, VM-500, or VM-1000-HV only) with the complete suite of licenses that includes Threat Prevention, GlobalProtect, WildFire, PAN-DB URL Filtering, and a premium support entitlement.

## VM-Series Firewall in Amazon Web Services (AWS) and Azure Licenses

You can license the VM-Series firewall in AWS and Azure in two ways:

- **Bring Your Own License (BYOL)**—A license that is purchased from a partner, reseller, or directly from Palo Alto Networks. Capacity license, support license, and subscription licenses are supported for BYOL. With this option, you must apply the license after you deploy the VM-Series firewall.

- **Usage-Based License**—Also called a *pay-per-use* or *pay-as-you-go* (PAYG) license. This type of license can be purchased from the AWS Marketplace and the Azure public Marketplace. Usage-based licenses are not available on the Azure Government Cloud Marketplace.

AWS supports hourly and annual PAYG options; Azure supports the hourly PAYG option only.

With the usage-based licenses, the firewall is prelicensed and ready for use as soon as you deploy it; you do not receive an auth code. When the firewall is stopped or terminated on the AWS or Azure console, the usage-based licenses are suspended or terminated.

Usage-based licenses are available in the following pricing bundles:

- Bundle 1: Includes the VM-Series capacity license (VM-300 only), Threat Prevention license that includes IPS, AV, malware prevention, and a premium support entitlement.
- Bundle 2: Includes the VM-Series capacity license (VM-300 only), Threat Prevention (includes IPS, AV, malware prevention), GlobalProtect, WildFire, PAN-DB URL Filtering licenses, and a premium support entitlement.



If you have an evaluation copy of the VM-Series firewall and would like to convert it to a fully licensed (purchased) copy, clone your VM-Series firewall and use the instructions to register and license the purchased copy of your VM-Series firewall. For instructions, see [Upgrade the VM-Series Firewall](#).

You cannot switch between the PAYG and the BYOL licenses. To move from PAYG to BYOL, contact your Palo Alto Networks channel partner or sales representative to purchase a BYOL license and get a BYOL auth code that you can use to license your firewall. If you have deployed your firewall and want to switch the license, see [Switch Between the BYOL and the PAYG Licenses](#).

## Serial Number and CPU ID Format for the VM-Series Firewall

When you launch an instance of the VM-Series firewall, each instance of the firewall is uniquely identified using the CPU ID and serial number of the firewall. The format of the CPU ID and the serial number include information on the hypervisor and the license type for each instance of the VM-Series firewall.

- With the usage-based licensing model of the VM-Series firewalls, at launch the firewall generates a serial number and CPU ID, and you use these details to [Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure \(no auth code\)](#).
- With the BYOL model, you must [Register the VM-Series Firewall \(with auth code\)](#) on the Customer Support portal (CSP). For a firewall with direct internet access, you can apply the auth code on the firewall to generate a license file that includes the serial number. For a firewall that is offline, you must use the CSP to input the CPU ID, UUID, and the auth code to generate a license file that includes the serial number and install the license on the firewall.

License Type	Serial Number	CPU ID
BYOL	15 digits, all numeric Example: 0071 51 345678909	<Hypervisor>:<ActualCPUID> Example: <b>ESX</b> :12345678
PAYG	15 digits, alphanumeric Example: 4 DE0YTAYOGMYTNN	<Hypervisor>:<Instance-ID>:<CloudProductCode>:<CloudRegion> Example: <b>AWSMP</b> :1234567890abcdef0:6kxdw3bbmdeda3o6i 1ggqt4km:us-west1



## Create a Support Account

A support account is required to access software updates and to get technical support or open a case with Palo Alto Networks technical support.

For all licensing options except for usage-based licenses that are currently only available in AWS, you require a support account so that you can download the software package required to install the VM-Series firewall. The support account also allows you to view and manage all assets—appliances, licenses, and subscriptions—that you have registered with Palo Alto Networks.

If you have an existing support account, continue with [Register the VM-Series Firewall](#).

### Create a Support Account

**Step 1** Go to <https://www.paloaltonetworks.com/support/tabs/overview.html>.

**Step 2** Click the **Register** link (bottom of the page), and enter the corporate email address to associate with the support account.

**Step 3** Pick one of the following options and fill in the details in the user registration form:

- (For the usage-based license in AWS)
  1. Click **Register your Amazon Web Services VM-Series Instance**
  2. On the AWS Management Console, find the AWS Instance ID, AWS Product Code, and the AWS Zone in which you deployed the firewall.
  3. Fill in the other details.
- (For all other licenses)
  1. Click **Register device using Serial Number or Authorization Code**
  2. Enter the capacity auth code and the sales order number or customer ID.
  3. Fill in the other details.

**Step 4** **Submit** the form. You will receive an email with a link to activate the user account; complete the steps to activate the account.

After your account is verified and the registration is complete, you can log in to the support portal.

---

## Register the VM-Series Firewall

When you purchase a VM-Series firewall, you receive an email that includes an auth code for a capacity license for the VM-Series model, a support entitlement auth code (for example, PAN-SVC-PREM-VM-100 SKU), and one or more auth codes for the subscription licenses. To use the auth code(s), you must register the code to the support account on the [Palo Alto Networks Customer Support web site](#). In the case of the VMware integrated NSX solution, the email contains a single authorization code that bundles the capacity license for one or more instances of the VM-1000-HV model, the support entitlement, and one or more subscription licenses.

For the usage-based licenses in AWS, you do not receive an auth code. However, in order to activate your premium support entitlement with Palo Alto Networks, you must create a support account and register the VM-Series firewall on the [Palo Alto Networks Customer Support web site](#).

Use the instructions in this section to register the capacity auth code or firewall with your support account:

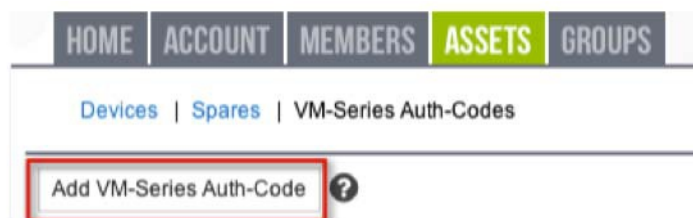
- ▲ [Register the VM-Series Firewall \(with auth code\)](#)
- ▲ [Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure \(no auth code\)](#)

### Register the VM-Series Firewall (with auth code)

#### Register the VM-Series Firewall (with auth code)

**Step 1** Log in to the [Palo Alto Networks Customer Support web site](#) with your account credentials. If you need a new account, see [Create a Support Account](#).

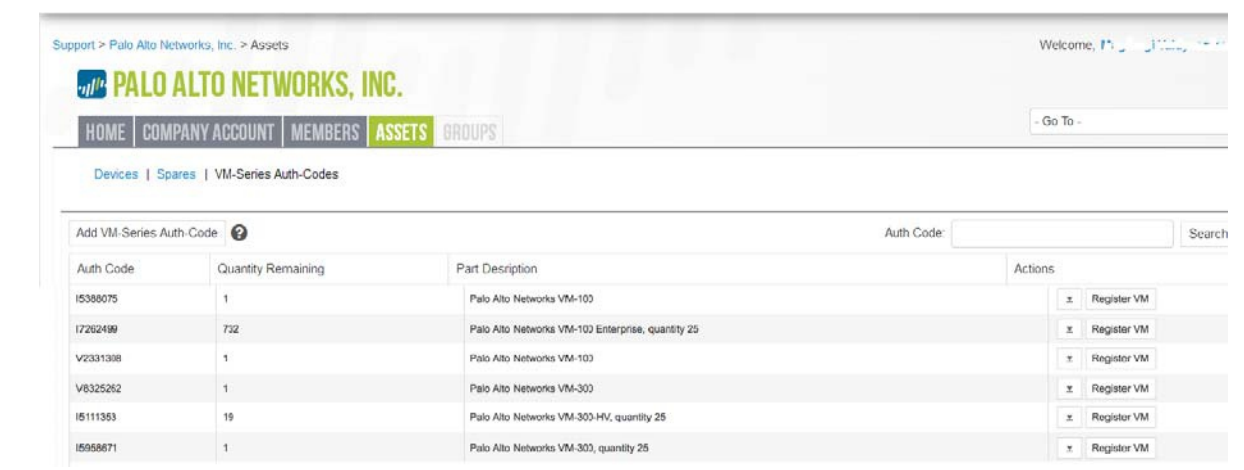
**Step 2** Select **Assets** and click **Add VM-Series Auth-Codes**.



### Register the VM-Series Firewall (with auth code)

**Step 3** In the **Add VM-Series Auth-Code** field, enter the capacity auth code you received by email, and click the checkmark on the far right to save your input. The page will display the list of auth codes registered to your support account.

You can track the number of VM-Series firewalls that have been deployed and the number of licenses that are still available for use against each auth code. When all the available licenses are used, the auth code does not display on the VM-Series Auth-Codes page. To view all the assets that are deployed, select **Assets > Devices**.



The screenshot shows the Palo Alto Networks Customer Support web site. The user is logged in as 'Support > Palo Alto Networks, Inc. > Assets'. The navigation bar includes 'HOME', 'COMPANY ACCOUNT', 'MEMBERS', 'ASSETS', and 'GROUPS'. Below the navigation bar, there are links for 'Devices', 'Spares', and 'VM-Series Auth-Codes'. The main content area is titled 'Add VM-Series Auth-Code' and features a search bar for 'Auth Code'. Below this is a table with the following data:

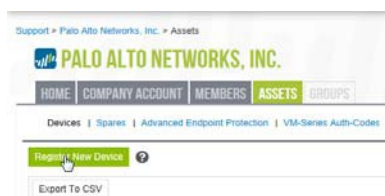
Auth Code	Quantity Remaining	Part Description	Actions
15388075	1	Palo Alto Networks VM-100	<input type="checkbox"/> Register VM
17262499	732	Palo Alto Networks VM-100 Enterprise, quantity 25	<input type="checkbox"/> Register VM
V2331398	1	Palo Alto Networks VM-100	<input type="checkbox"/> Register VM
V8325262	1	Palo Alto Networks VM-300	<input type="checkbox"/> Register VM
15111353	19	Palo Alto Networks VM-300-HV, quantity 25	<input type="checkbox"/> Register VM
15958671	1	Palo Alto Networks VM-300, quantity 25	<input type="checkbox"/> Register VM

## Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code)

Before you begin the registration process, log in to the VM-Series firewall and jot down the serial number and the CPU ID (UUID is optional) from the dashboard.

### Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code)

**Step 1** On the **Assets** tab (after you log in to the [Palo Alto Networks Customer Support web site](#)), click **Register New Device**.



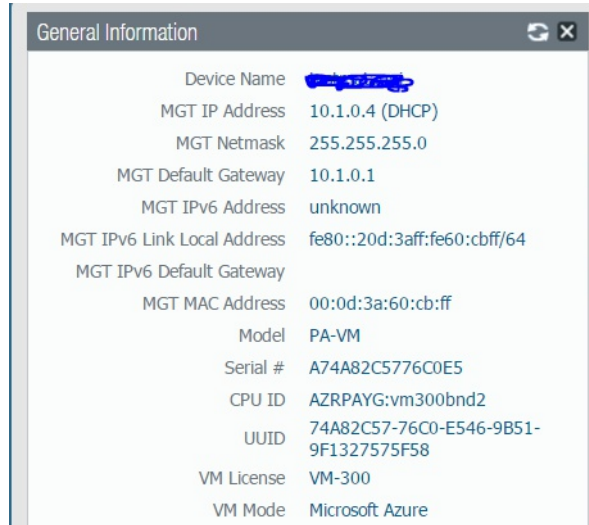
**Step 2** Select **Register usage-based VM-Series models (hourly/annual) purchased from public cloud Marketplace**.

**Step 3** Select your **Cloud Marketplace** vendor and **Submit**.

### Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code) (Continued)

**Step 4** Enter the **Serial #**, the **CPU ID**, and the **UUID** of the VM-Series firewall.

For example, from the Dashboard of the VM-Series firewall on Azure you will see the following information.



If you plan to use the firewall offline, please select the **Offline** checkbox and enter the PAN-OS version you plan to use.

---

**Step 5** **Agree and Submit** to accept the EULA and register the firewall.

---

**Step 6** Verify that the details on the licenses you purchased are displayed on the **Assets** page of the support portal.

---

## Switch Between the BYOL and the PAYG Licenses

There is no migration path between the BYOL and PAYG licensing options. If you have already deployed and configured a VM-Series firewall with the PAYG or BYOL option in AWS or Azure, and now want to switch to the other option, use the following instructions to save and export the configuration on your existing firewall, deploy a new firewall, and then restore the configuration on the new firewall.

Switch Between the PAYG License and the BYOL License	
<p><b>Step 1</b> Save a backup of the current configuration file and store it to an external server.</p>	<ol style="list-style-type: none"> <li>1. Select <b>Device &gt; Setup &gt; Operations</b> and <b>Export named configuration snapshot</b>.</li> <li>2. Select the XML file that contains your running configuration (for example, running-config.xml) and click <b>OK</b> to export the configuration file.</li> <li>3. Save the exported file to a location external to the firewall.</li> </ol>
<p><b>Step 2</b> Deploy a new firewall and register or activate the license, as appropriate.</p>	<p>For a new PAYG instance:</p> <ol style="list-style-type: none"> <li>1. In the AWS or Azure Marketplace, select the software image for the PAYG licensing bundle you want to deploy.</li> <li>2. Deploy a new VM-Series firewall in the AWS or Azure public cloud. See <a href="#">Set Up the VM-Series Firewall on AWS</a> or <a href="#">Set up the VM-Series Firewall on Azure</a>.</li> <li>3. <a href="#">Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure (no auth code)</a>.</li> </ol> <p>For a new BYOL instance:</p> <ol style="list-style-type: none"> <li>1. Contact your sales representative or reseller to purchase a BYOL license, and get a BYOL auth code that you can use to license your firewall.</li> <li>2. <a href="#">Register the VM-Series Firewall (with auth code)</a>.</li> <li>3. Deploy a new VM-Series firewall in the AWS or Azure public cloud. See <a href="#">Set Up the VM-Series Firewall on AWS</a> or <a href="#">Set up the VM-Series Firewall on Azure</a>.</li> <li>4. <a href="#">Activate the License for the VM-Series Firewall (Standalone Version)</a>.</li> </ol>

**Switch Between the PAYG License and the BYOL License**

- |   |  |
|---|--|
| <p><b>Step 3</b> On the newly deployed firewall, restore the configuration that you exported.</p> | <ol style="list-style-type: none"><li>1. Access the web interface of the newly deployed firewall.</li><li>2. Select <b>Device &gt; Setup &gt; Operations</b>, click <b>Import named configuration snapshot</b>, Browse to the configuration file on the external host, and click <b>OK</b>.</li><li>3. Click <b>Load named configuration snapshot</b>, select the <b>Name</b> of the configuration file you just imported, and click <b>OK</b>.</li><li>4. Click <b>Commit</b> to overwrite the running configuration with the snapshot you just imported.</li><li>5. Verify that the configuration on the new firewall matches the firewall that you are replacing, before you delete the firewall or deactivate the licenses on the replaced firewall.</li></ol> |
|---|--|

## Activate the License

To activate the license on your VM-Series firewall, you must have deployed the VM-Series firewall and completed initial configuration. To deploy the firewall, see [VM-Series Deployments](#).

Use the instructions in this section for all the BYOL models including AWS and Azure; for usage-based licensing in AWS and Azure, you do not need to activate the license. For the usage-based licenses, you must [Register the Usage-Based Model of the VM-Series Firewall in AWS and Azure \(no auth code\)](#) in order to activate your premium support entitlement.



For usage-based models of the VM-Series firewall in the AWS Marketplace, instances with short and long AWS instance IDs are supported.

Until you activate the license on the VM-Series firewall, the firewall does not have a serial number, the MAC address of the dataplane interfaces are not unique, and only a minimal number of sessions are supported. Because the MAC addresses are not unique until the firewall is licensed, to prevent issues caused by overlapping MAC addresses, make sure that you do not have multiple, unlicensed VM-Series firewalls.

When you activate the license, the licensing server uses the UUID and the CPU ID of the virtual machine to generate a unique serial number for the VM-Series firewall. The capacity auth code in conjunction with the serial number is used to validate your entitlement.



After you license a VM-Series firewall, if you need to delete and redeploy the VM-Series firewall, make sure to [Deactivate the License\(s\)](#) on the firewall. Deactivating the license allows you to transfer the active licenses to a new instance of the VM-Series firewall without help from technical support.

- ▲ [Activate the License for the VM-Series Firewall \(Standalone Version\)](#)
- ▲ [Activate the License for the VM-Series Firewall for VMware NSX](#)

### Activate the License for the VM-Series Firewall (Standalone Version)

To activate the license on your VM-Series firewall, you must have deployed the VM-Series firewall and completed initial configuration.

Activate the License	
<ul style="list-style-type: none"> <li>If your VM-Series firewall has direct internet access. To activate the license, the firewall must be configured with an IP address, netmask, default gateway, and DNS server IP address.</li> </ul>	<ol style="list-style-type: none"> <li>Select <b>Device &gt; Licenses</b> and select the <b>Activate feature using authentication code</b> link.</li> <li>Enter the capacity auth code that you registered on the support portal. The firewall will connect to the update server (updates.paloaltonetworks.com), and download the license and reboot automatically.</li> <li>Log back in to the web interface and confirm that the <b>Dashboard</b> displays a valid serial number. If the term <i>Unknown</i> displays, it means the device is not licensed.</li> <li>On <b>Device &gt; Licenses</b>, verify that <b>PA-VM</b> license is added to the device.</li> </ol>

### Activate the License (Continued)

- If your VM-Series firewall does not have internet access.

1. Select **Device > Licenses** and click the **Activate Feature using Auth Code** link.
2. Click **Download Authorization File**, and download the *authorizationfile.txt* on the client machine.
3. Copy the *authorizationfile.txt* to a computer that has access to the internet and log in to the support portal. Click **My VM-Series Auth-Codes** link and select the applicable auth code from the list and click the **Register VM** link.
4. On the **Register Virtual Machine** tab upload the authorization file. Select the PAN-OS version and the hypervisor on which you have deployed the firewall, to complete the registration process. The serial number of your VM-Series firewall will be attached to your account records.

5. Navigate to **Assets > My Devices** and search for the VM-Series device just registered and click the **PA-VM** link. This will download the VM-Series license key to the client machine.
6. Copy the license key to the machine that can access the web interface of the VM-Series firewall and navigate to **Device > Licenses**.
7. Click **Manually Upload License** link and enter the license key. When the capacity license is activated on the firewall, a reboot occurs.
8. Log in to the device and confirm that the **Dashboard** displays a valid serial number and that the **PA-VM** license displays in the **Device > Licenses** tab.

## Activate the License for the VM-Series Firewall for VMware NSX

Panorama serves as the central point of administration for the VM-Series firewalls for VMware NSX and the license activation process is automated when Panorama has direct internet access. Panorama connects to the Palo Alto Networks update server to retrieve the licenses, and when a new VM-Series firewall for NSX is deployed, it communicates with Panorama to obtain the license. If Panorama is not connected to the internet, you need to manually license each instance of the VM-Series firewall so that the firewall can connect to Panorama. For an overview of the components and requirements for deploying the VM-Series firewall for NSX, see [VM-Series for NSX Firewall Overview](#).



For this integrated solution, the auth code (for example, PAN-VM-1000-HV-SUB-BND-NSX2) includes licenses for threat prevention, URL filtering and WildFire subscriptions and premium support for the requested period.

In order to activate the license, you must have completed the following tasks:

- Registered the auth code to the support account. If you don't register the auth code, the licensing server will fail to create a license.
- Entered the auth code in the Service Definition on Panorama. On Panorama, select **VMware Service Manager** to add the **Authorization Code** to the **VMware Service Definition**.




If you have purchased an evaluation auth code, you can license up to 5 VM-Series firewalls with the VM-1000-HV capacity license for a period of 30 or 60 days. Because this solution allows you to deploy one VM-Series firewall per ESXi host, the ESXi cluster can include a maximum of 5 ESXi hosts when using an evaluation license.

The following process of activating the licenses is manual. If you have a custom script or an orchestration service, you can use the [Licensing API](#) to automate the process of retrieving the licenses for the VM-Series firewalls.

Activate the Licenses on the VM-Series Firewall for NSX	
When Panorama has internet access (Online)	
<b>Step 1</b> Verify that the VM-Series firewall is connected to Panorama.	<ol style="list-style-type: none"> <li>1. Log in to Panorama.</li> <li>2. Select <b>Panorama &gt; Managed Devices</b> and check that the firewall displays as Connected.</li> </ol>
<b>Step 2</b> Verify that each firewall is licensed.	<p>Select <b>Panorama &gt; Device Deployment &gt; Licenses</b> and verify that Panorama has matched the auth code and applied the licenses to each firewall.</p> <p>If you do not see the licenses, click <b>Refresh</b>. Select the VM-Series firewalls for which to retrieve subscription licenses and click <b>OK</b>.</p>
When Panorama does not have internet access (Offline)	
<b>Step 1</b> Locate the CPU ID and UUID of the VM-Series firewall.	<ol style="list-style-type: none"> <li>1. From the vCenter server obtain the IP address of the firewall.</li> <li>2. Log into the web interface and select <b>Dashboard</b>.</li> <li>3. Get the <b>CPU ID</b> and the <b>UUID</b> for the firewall from the General Information widget.</li> </ol>
<b>Step 2</b> Activate the auth code and generate the license keys.	<ol style="list-style-type: none"> <li>1. Log in to the <a href="#">Palo Alto Networks Customer Support web site</a> with your account credentials. If you need a new account, see <a href="#">Create a Support Account</a>.</li> <li>1. Select <b>Assets &gt; VM-Series Auth Codes</b>, click <b>Add VM-Series Auth Codes</b> to enter the auth code.</li> <li>2. Select <b>Register VM</b> in the row that corresponds to the auth code that you just registered, enter the CPU ID and the UUID of the firewall and click <b>Submit</b>. The portal will generate a serial number for the firewall.</li> <li>3. Select <b>Assets &gt; Devices</b> and search for the serial number.</li> <li>4. Click the link the Actions column to download each key locally to your laptop. In addition to the subscription license key, you must get the capacity license and the support license keys.</li> </ol>

### Activate the Licenses on the VM-Series Firewall for NSX

<p><b>Step 3</b> Upload the keys to the firewall.</p>	<ol style="list-style-type: none"> <li>1. Log in to the firewall web interface.</li> <li>2. Select <b>Device &gt; Licenses</b>, and select <b>Manually upload license key</b>.</li> <li>3. <b>Browse</b> to select a key and click <b>OK</b> to install the license on the firewall.   Install the capacity license key file (pa-vm.key) first. When you apply the capacity license key, the VM-Series firewall will reboot. On reboot, the firewall will have a serial number that you can use to register the firewall as a managed device on Panorama.</li> <li>4. Repeat the process to install each key on the firewall.</li> <li>5. Select <b>Dashboard</b> and verify that you can see the <b>Serial #</b> in the General Information widget.</li> </ol>
<p><b>Step 4</b> Add the serial number of the firewall on Panorama.</p>	<p>Select <b>Panorama &gt; Managed Devices</b> and click <b>Add</b> to enter the serial number for the VM-Series firewall for NSX. The firewall should now be able to connect with Panorama so that it can obtain its configuration and policy rules.</p>

## Deactivate the License(s)

The license deactivation process enables you to self-manage licenses. Whether you want to remove one or more active licenses or subscriptions attributed to a firewall (hardware-based or VM-Series firewall) or you want to deactivate the VM-Series firewall and unassign all active licenses and subscriptions, begin the deactivation process on the firewall or Panorama (not on the Palo Alto Networks Customer Support web site).

To successfully deactivate a license, you must install a license deactivation API key and enable verification of the update server identity (enabled by default). PAN-OS uses this deactivation API key to authenticate with all update a license services. The deactivation API is key is not required for manual license deactivation, where there is not connectivity between the firewall and license server.

If the firewall/Panorama has internet access and can communicate with the Palo Alto Networks Licensing servers, the license removal process completes automatically with a click of a button. If the firewall/Panorama does not have internet access, you must complete the process manually in a two-step process. In the first step, from the firewall or Panorama, you generate and export a license token file that includes information on the deactivated keys. In the second step, while logged in to the [Palo Alto Networks Customer Support web site](#), upload the token file to dissociate the license keys from the firewall.

- ▲ [Install a License Deactivation API Key](#)
- ▲ [Deactivate a Feature License or Subscription Using the CLI](#)
- ▲ [Deactivate VM](#)

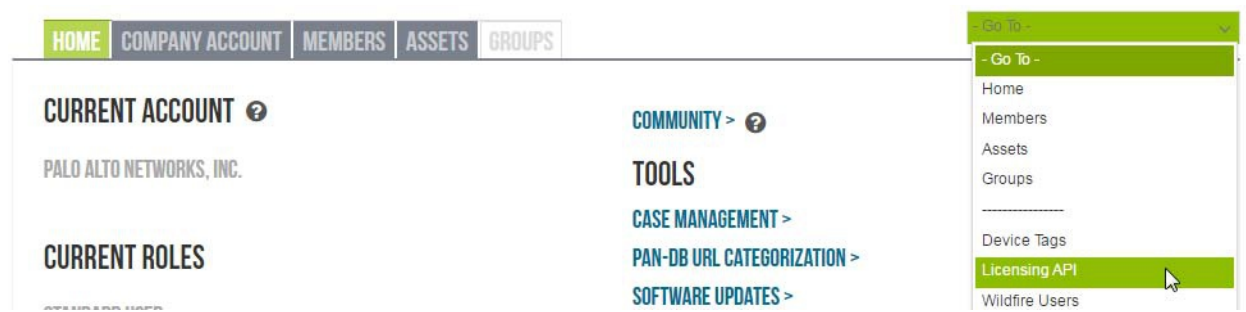
## Install a License Deactivation API Key

Retrieve your license API key from the Customer Support Portal and install it using the CLI on the firewall and Panorama. You must have superuser privileges on the firewall or Panorama to install the license API key. When you install a license API key on Panorama, Panorama pushes the API key to its managed devices. If the managed device has an API key installed, Panorama overwrites the old API key with the new one.

### Install the API Key

**Step 1** Retrieve the license deactivation API key from the [Customer Support Portal](#).

1. Log in to the Customer Support Portal.
2. From the Go To drop-down, select **License API**.
3. Copy the API key.



### Install the API Key

**Step 2** Use the CLI to install the API key copied in the previous step.

```
request license api-key set key <key>
```

**Step 3** After installing the license deactivation API key, [Deactivate VM](#) as normal.  
Deactivating a VM-Series license requires a software restart.

If you need to replace an license deactivation API key, use the following CLI command to delete an installed API key.

```
request license api-key delete
```

To deactivate a VM-Series firewall after deleting the API key, you must install a new one.

## Deactivate a Feature License or Subscription Using the CLI

If you accidentally installed a license/subscription on a firewall and need to reassign the license to another firewall, you can deactivate an individual license and re-use the same authorization code on another firewall without help from Technical Support. This capability is supported on the CLI only; this process is supported both on the hardware-based firewalls and on the VM-Series firewall.

### Deactivate a Feature License or Subscription Using the CLI

**Step 1** Log into the CLI on the firewall.

If your firewall has direct internet access, use the following commands:

**Step 2** View the name of the license key file for the feature you want to deactivate.

```
request license deactivate key features ?
```

**Step 3** Deactivate the license or subscription.

```
request license deactivate key features <name> mode auto
```

where, name is the full name for the license key file.

For example:

```
admin@vmPAN2> request license deactivate key features
WildFire_License_2015_01_28_I5820573.key mode auto
007200002599 WildFire License Success
Successfully removed license keys
```

If your firewall does not have direct internet access, use the following commands:

**Step 4** View the name of the license key file for the feature you want to deactivate.

```
request license deactivate key features
```

**Step 5** Deactivate the license manually.

```
request license deactivate key features <name> mode manual
```

For example:

```
admin@PA-VM> request license deactivate key features
PAN_DB_URL_Filtering_2015_01_28_I6134084.key mode manual
```

Successfully removed license keys

```
dact_lic.01282015.100502.tok
```



The token file uses the format `dact_lic.timestamp.tok`, where the timestamp is in the `dmmyyy.hrminsec` format.

### Deactivate a Feature License or Subscription Using the CLI (Continued)

**Step 6** Verify that the token file was generated.

```
show license-token-files
```

**Step 7** Export the token file to an SCP or TFTP server and save it to your computer.

```
scp export license-token-file to <username@serverIP> from <token_filename>
```

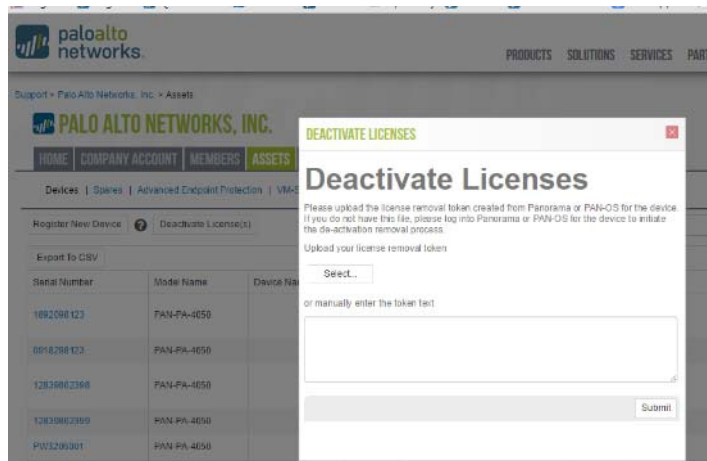
For example:

```
scp export license-token-file to admin@10.1.10.55:/tmp/ from
dact_lic.01282015.100502.tok
```

**Step 8** Log into the [Palo Alto Networks Customer Support web site](#).

**Step 9** Click the **Deactivate License(s)** link on the **Assets** tab.

**Step 10** While logged in to the [Palo Alto Networks Customer Support web site](#), upload the token file to complete the deactivation.



## Deactivate VM

When you no longer need an instance of the VM-Series firewall, you can free up all active licenses—subscription licenses, VM-Capacity licenses, and support entitlements—using the web interface, CLI, or the XML API on the firewall or Panorama. The licenses are credited back to your account and you can use the same authorization codes on a different instance of the VM-Series firewall.

Deactivating a VM removes all the licenses/entitlements and places the VM-Series firewall in an unlicensed state; the firewall will not have a serial number and can support only a minimal number of sessions. Because the configuration on the firewall is left intact, you can re-apply a set of licenses and restore complete functionality on the firewall, if needed.



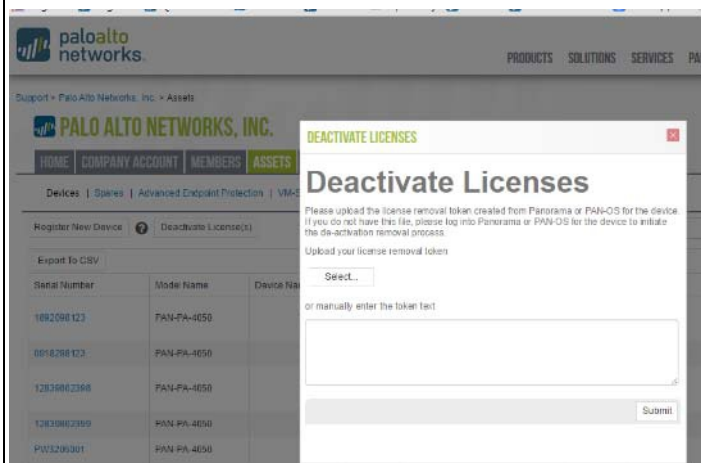
Make sure to deactivate licenses before you delete the VM-Series firewall. If you delete the firewall before deactivating the licenses you have two options:

- If the device was managed by Panorama, you can deactivate the license from Panorama.
- If the device was not managed by Panorama, you must contact [Palo Alto Networks Customer Support](#).

## Deactivate VM

- From the firewall

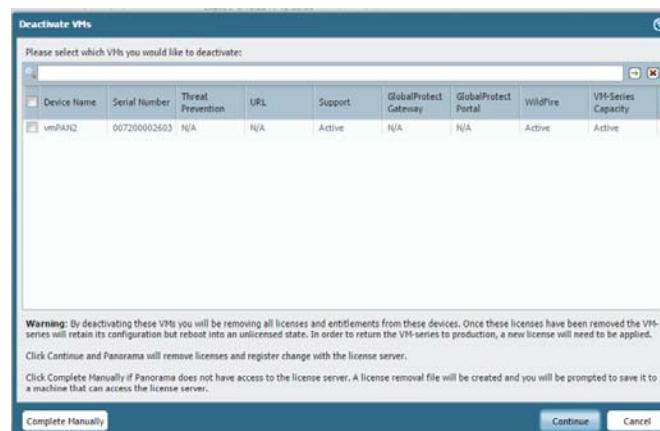
1. Log into the web interface and select **Device > Licenses**.
2. Select **Deactivate VM** in the License Management section.
3. Verify the list of licenses/entitlements that will be deactivated on the firewall.
4. Pick one of the following options to start deactivating the VM:
  - Click **Continue**, if the firewall can communicate directly with the Palo Alto Networks Licensing server. You will be prompted to reboot the firewall; on reboot the licenses are deactivated.
  - Click **Complete Manually**, if the firewall does not have internet access. Click the **Export license token** link to save the token file to your local computer. For example, the token filename is 20150128\_1307\_dact\_lic.01282015.130737.tok. You will be prompted to reboot the firewall; on reboot the licenses are deactivated.
5. (For the manual process only) Complete the following tasks to register the changes with the Licensing server:
  - a. Log into the [Palo Alto Networks Customer Support web site](#).
  - b. Click the Deactivate License(s) link on the **Assets** tab.
  - c. While logged in to the [Palo Alto Networks Customer Support web site](#), upload the token file to complete the deactivation.



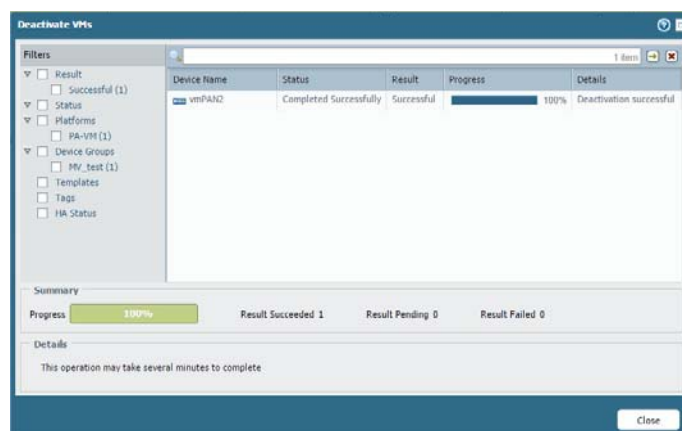
## Deactivate VM (Continued)

- From Panorama

1. Log in to the Panorama web interface and select **Panorama > Device Deployment > Licenses**.
2. Click **Deactivate VMs**, and select the VM-Series firewall that you want to deactivate.



3. Pick one of the following options to deactivate the VM:
  - Click **Continue**, if Panorama can communicate directly with the Palo Alto Networks Licensing servers and can register the changes. To verify that the licenses have been deactivated on the firewall, click **Refresh** on **Panorama > Device Deployment > Licenses**. The firewall is automatically rebooted.
  - Click **Complete Manually**, if Panorama does not have internet access. Panorama generates a token file. Click the **Export license token** link to save the token file to your local computer. The successful completion message is displayed on-screen, and the firewall will be automatically rebooted.



4. (For the manual process only) To use the token file register the changes with the licensing server, see step 5 above.

## Deactivate VM (Continued)

5. Remove the deactivated VM-Series firewall as a managed device on Panorama.

a. Select **Panorama > Managed Devices**.

b. Select the firewall that you deactivated from the list of managed devices, and click **Delete**.

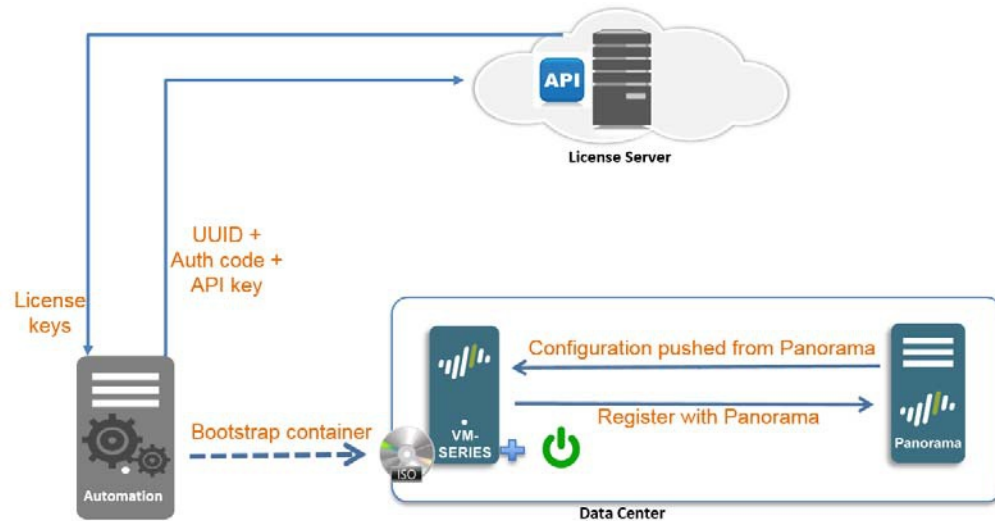


Instead of deleting the firewalls, if you prefer, you can create a separate device group and assign the deactivated VM-Series firewalls to this device group.



## Licensing API

To successfully license firewalls that do not have direct internet access, Palo Alto Networks provides a licensing API. You can use this API with a custom script or an orchestration service to register auth codes, retrieve licenses attached to an auth code, renew licenses, and to deactivate all licenses on a VM-Series firewall ([Deactivate VM](#)).



The API also allows you to view the details of an auth code so that you can track the number of unused licenses attached to an auth-code or auth-code bundle that enables you to license more than one instance of the firewall. An auth-code bundle includes the VM-Series model, subscriptions and support in a single, easy to order format; you can use this bundle multiple times to license VM-Series firewalls as you deploy them.

To use the API, each support account is assigned a unique key. Each API call is a POST request, and the request must include the API key to authenticate the request to the licensing server. When authenticated, the licensing server sends the response in json (content-type application/json).

- ▲ [Manage the Licensing API Key](#)
- ▲ [Use the Licensing API](#)
- ▲ [Licensing API Error Codes](#)

## Manage the Licensing API Key

To get the API key required to use the licensing API, your account must have super user privileges on the support portal.

Manage the Licensing API Key	
<b>Step 1</b> Get your Licensing API key.	<ol style="list-style-type: none"> <li>1. Log in to the Palo Alto Networks <a href="#">Support portal</a> with an account that has super user privileges.</li> <li>2. Select <b>Licensing API</b> from the <b>—Go To—</b> drop-down.</li> <li>3. Click <b>Enable</b> to view your key and copy it for use. Once you generate a key, the key is enabled until you regenerate or disable it.</li> </ol>
<b>Step 2</b> Regenerate or revoke the API key.	<ol style="list-style-type: none"> <li>1. You can generate a new API key or revoke the use of the key.             <ul style="list-style-type: none"> <li>• Click <b>Regenerate</b> to generate a new key. If you suspect that an API key may be compromised, you can generate a new key, which process automatically invalidates the old key.</li> <li>• Select <b>Disable</b> if you no longer plan to use the key. Disabling the API key revokes it.</li> </ul> </li> </ol>

## Use the Licensing API

The base URI for accessing the licensing API is <https://api.paloaltonetworks.com/api/license>; based on the task you want to perform, for example activate licenses, deactivate licenses, or track license use—the URL will change.

An API request must use the HTTP POST method, and you must include the API key in the apikey HTTP request header and pass the request parameters as URL-encoded form data with content-type application/x-www-form-urlencoded.

The API Version is optional and can include the following values—0 or 1. If specified, it must be included in the version HTTP request header. The current API version is 1; if you do not specify a version, or specify version 0, the request uses the current API version.

All API responses are represented in json.

Use the Licensing API
<b>Step 1</b> <a href="#">Get your Licensing API key.</a>
<b>Step 2</b> Select the task you want to perform. <ul style="list-style-type: none"> <li>- <a href="#">Activate Licenses</a></li> <li>- <a href="#">Deactivate Licenses</a></li> <li>- <a href="#">Track License Usage</a></li> </ul>

## Use the Licensing API (Continued)

### Activate Licenses

**URL:** <https://api.paloaltonetworks.com/api/license/activate>

**Parameters:** uuid, cpuid, authCode, and serialNumber.

Use these parameters to accomplish the following:

- For first time or initial license activation, provide the cpuid, uuid, auth-code in the API request.
- If you did not save the license keys or had a network connection trouble during initial license activation, to retrieve the license(s) again for a firewall that you have previously activated, you can either provide the cpuid and uuid in the API request, or provide the serial number of the firewall in the API request.

**Header:** apikey

### Sample request for initial license activation using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode cpuid=51060400FFFBAB1F
--data-urlencode uuid=564D0E5F-3F22-5FAD-DA58-47352C6229FF --data-urlencode
authCode=I7115398 https://api.paloaltonetworks.com/api/license/activate
```

### Sample API response:

```
[{"lfidField":"13365773","partidField":"PAN-SVC-PREM-VM-300","featureField":"Premi
um","feature_descField":"24 x 7 phone support; advanced replacement hardware
service","keyField":"m4iZEL1t3n60a+6111L7itDZTphYw48N1AM0ZXutDgExC5f5p0A52+QgljmAx
anB\nKOyat4FJI4k2hWiBYz9cONuKoiaN0tAGhJvAuZmYggAZejKueWrTzCuLrwxI/iEw\nnkRGR3cYG+j6
o84RitR937m2iOk2v9o8RSfLVilgX28nqmc08LcAnTqbrRWdFtwVk\nluz47AUMXauuqwpMipouQYjk0ZL
7fTHHslhyL7yFjCyXBoYXOt3JiqQ00CDdBdDI\n91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQX
KvaThuR8YyHr1Pdw/lAjs\nppyIVFa6FufPacfb2RHApQ==\n","auth_codeField":"","errmsgFiel
d":null,"typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5
/29/2016","vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseFiel
d":null,"mac_countField":null,"drrField":null,"expirationField":"8/29/2016
12:00:00
AM","PropertyChanged":null},{ "lfidField":"13365774","partidField":"PAN-VM-300-TP",
"featureField":"Threat Prevention","feature_descField":"Threat
Prevention","keyField":"NqaXoaFG+9qj0t9Vu7FBMizDarj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K
2yXtrl\n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jblMfAwEM8mlnCyLhDRM3EE+umS4b\ndZBRH5AQ
jPoaON7xZ46VMFovOR+asOUJXTptS/EulbLA17PBp3+nm04dYTF90500\ndey1jmGoiBZ9wBkesvukg3dV
Z7gxppDvz14+wekYEJqPfm0NZyxsC5dn0xg9pciF\ncFelhnTYlma1lXrCqjJcFdniHRw00RE9CIKWe0g2
HGolu02eq1XMXL9mE5t025im\nblMnhL06smrCdtXmb4jjtg==\n","auth_codeField":"","errmsgF
ield":null,"typeField":"SUB","regDateField":"2016-06-03T08:18:41","startDateField
":"5/29/2016","vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseF
ield":null,"mac_countField":null,"drrField":null,"expirationField":"8/29/2016
12:00:00 AM","PropertyChanged":null}
...<truncated>
```



The feature\_Field in the response indicates the type of key that follows in the keyField. Copy each key to a text file and save it with the .key extension. Because the key is in json format, it does not have newlines; make sure to convert it to newlines if needed for your parser. Make sure to name each key appropriately and save it to the /license folder of the [bootstrap package](#). For example, include the authcode with the type of key to name it as I3306691\_1pa-vm.key (for the capacity license key), I3306691\_1threat.key (for the Threat Prevention license key), I3306691\_1wildfire.key (for the WildFire subscription license key).

### Sample API request for retrieving previously activated licenses using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode serialNumber=007200006142
https://api.paloaltonetworks.com/api/license/activate
```

## Use the Licensing API (Continued)

**Sample API response:**

```

{"lfidField":"13365773","partidField":"PAN-SVC-PREM-VM-300","featureField":"Premium","feature_descField":"24 x 7 phone support; advanced replacement hardware service","keyField":"m4iZELit3n6Oa+6lllL7itDZTphYw48N1AMozXutDgExC5f5pOA52+QgljmAxanB\nkOyat4FJI4k2hWiBYz9cONuKoiaNoTAGhJvAuZmYgqAZejKueWrTzCuLrwxI/iEW\nkNRGR3cYG+j6o84RitR937m2iOk2v9o8RSfLVilgX28nqmcO8LcAnTqbrRwDftwVk\nluz47AUMXauuqwpMipouQYjk0ZL7fTHShlhyL7yFjCyxBoYXOt3JiqQ0OCdDbDDI\nn91RkVPylEwTKgSXm3xpzbmC2ciUR5b235gyqdyW8eQXKvaThuR8YyHr1Pdw/lAjs\nnpvyIVFa6FufPacFB2RHApQ==\n","auth_codeField":"","errmsgField":null,"typeField":"SUP","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2016","vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":null,"mac_countField":null,"drrField":null,"expirationField":"8/29/2016 12:00:00 AM","PropertyChanged":null},{ "lfidField":"13365774","partidField":"PAN-VM-300-TP","featureField":"Threat Prevention","feature_descField":"Threat Prevention","keyField":"NqaXoaFG+9qj0t9Vu7FBMizDARj+pmFaQEd6I2OqfBfAibXrvuoFKeXX/K2yXtrl\n2n2qJhNq3kwXBDxn181z3nrUOsQd/eW68dyp4jb1MfAwEM8mlnCyLhDRM3EE+umS4b\nndZBRH5AQjPoaON7xZ46VMFovOR+asOUJXTptS/EulbLAI7PBp3+nm04dYTF90500\ndeYljmGoiBZ9wBkesvukg3dVZ7gxppDvz14+wekYIEJqPfM0NZyxsC5dnoxg9pciF\ncFelhnTYLma1lXrCqjJcFdniHRw00RE9CIKWe0g2HGolu2eq1XMXL9mE5t025im\nnblMnhL06smrCdtXmb4jJtg==\n","auth_codeField":"","errmsgField":null,"typeField":"SUB","regDateField":"2016-06-03T08:18:41","startDateField":"5/29/2016","vm_capacityField":null,"uuidField":null,"cpuidField":null,"mac_baseField":null,"mac_countField":null,"drrField":null,"expirationField":"8/29/2016 12:00:00 AM","PropertyChanged":null}
...<truncated>

```

## Deactivate Licenses

**URL:** <https://api.paloaltonetworks.com/api/license/deactivate>

**Parameters:** encryptedToken

To deactivate the license(s) on a firewall that does not have direct internet access, you must generate the license token file locally on the firewall and then use this token file in the API request. For details on generating the license token file, see [Deactivate VM](#) or [Deactivate a Feature License or Subscription Using the CLI](#).

**Header:** apikey

**Request:** `https://api.paloaltonetworks.com/api/license/deactivate?encryptedtoken@<token>`

### Sample API request for license deactivation using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode
encryptedtoken@dact_lic.05022016.100036.tok
https://api.paloaltonetworks.com/api/license/deactivate
```

**Sample API response:**

[illegible]

### Use the Licensing API (Continued)

#### Track License Usage

**URL:** `https://api.paloaltonetworks.com/api/license/get`

**Parameters:** `authCode`

**Header:** `apikey`

**Request:** `https://api.paloaltonetworks.com/api/license/get?authCode=<authcode>`

#### Sample API request for tracking license usage using Curl:

```
curl -i -H "apikey:$APIKEY" --data-urlencode authcode=I9875031
https://api.paloaltonetworks.com/api/license/get
```

#### Sample API response:

```
HTTP/1.1 200 OK
Date: Thu, 05 May 2016 20:07:16 GMT
Content-Length: 182
```

```
{"AuthCode":"I9875031","UsedCount":4,"TotalVMCount":10,"UsedDeviceDetails":[{"UUID
":"420006BD-113D-081B-F500-2E7811BE80C
9","CPUID":"D7060200FFFBAB1F","SerialNumber":"007200006142"}]}.....
```

---

## Licensing API Error Codes

The HTTP Error Codes that the licensing server returns are as follows:

- 200 Success
- 400 Error
- 401 Invalid API Key
- 500 Server Error

## Licenses for Cloud Security Service Providers (CSSPs)

The Palo Alto Networks CSSP partners program allows service providers to provide security as a service or as a hosted application to their end customers. The license offerings that Palo Alto Networks provides for authorized Cloud Security Service Provider (CSSP) partners is different from the offerings for enterprise users.

For CSSP partners, Palo Alto Networks supports a usage-based model for the VM-Series firewalls bundled with subscriptions and support. For CSSP partners, you can combine a term-based capacity license for the [VM-Series Models](#) along with a choice of subscription licenses for Threat Prevention, URL Filtering, AutoFocus, GlobalProtect, and WildFire, and support entitlements that provide access to technical support and software updates. For cost-effectiveness, you can also opt for a high availability (HA) option, if you plan on deploying the firewalls in an HA configuration.

- ▲ [Get the Auth Codes for CSSP License Packages](#)
- ▲ [Register the VM-Series Firewall with a CSSP Auth Code](#)
- ▲ [Add End-Customer Information for a Registered VM-Series Firewall](#)

### Get the Auth Codes for CSSP License Packages

To be a CSSP Partner, you have to enroll in the Palo Alto Networks CSSP partners program. For information on enrolling in the CSSP program, contact your Palo Alto Networks Channel Business Manager. If you are enrolled, the Palo Alto Network Support portal provides tools that allow you to select a license package, track license usage, and apply license entitlements.

A license package is a combination of the following options:

- Usage term—The pay-per-use options are hourly, monthly, 1-year, and 3-years.
- VM-Series firewall model—The VM-100, VM-200, VM-300, and VM-1000-HV that give you the model number and the capacities associated with each model.
- Subscription bundle—The three options are basic, bundle 1, and bundle 2. The basic option does not include any subscriptions; bundle 1 has the Threat Prevention license that includes IPS, AV, malware prevention; bundle 2 has the Threat Prevention (includes IPS, AV, malware prevention), GlobalProtect, WildFire, and PAN-DB URL Filtering licenses.
- Level of support—Premium support or backline support.
- Redundant firewalls—The option are either high availability (HA) or without HA. This option is a cost-effective option if you plan to deploy a pair of redundant firewalls.

The offering PAN-VM-300-SP-PREM-BND1-YU, for example, is a one-year term package that includes the VM-300 with premium support and the subscription bundle 1. Each package supports up to a maximum of 10,000 instances of the VM-Series firewall.

After you select your license package, you receive an email with your auth code; the fulfillment process can take up to 48 hours.

#### Get the Auth Codes for the CSSP License Packages

**Step 1** Log in to the [Palo Alto Networks Customer Support web site](#) with your account credentials. If you need a new account, see [Create a Support Account](#).