Contact Information

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

About this Guide

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

- For information on the additional capabilities and for instructions on configuring the features on the firewall, refer to https://docs.paloaltonetworks.com or search the documentation.
- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/services/solution-assurance.
- For the most current PAN-OS and Panorama 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
Upgrade to PAN-OS 7.1

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

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

## Table: PAN-OS 7.1 Upgrade/Downgrade Considerations

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

If your firewall is running a PAN-OS 6.1 or earlier release and is in FIPS mode, you must [Enable FIPS and Common Criteria Support](#) using **Set CCEAL4 Mode** before you upgrade to PAN-OS 7.0.1 or a later release. If you do not change to CCEAL4 mode before you upgrade, the firewall will enter maintenance mode because FIPS mode is not supported as of PAN-OS 7.0.1.

After you change from FIPS mode to CCEAL4 mode, you will need to import the saved configuration backup that you created prior to the mode change. If the configuration contains IKE and IPSec crypto profiles that use 3DES, you will need to delete the profiles and create new profiles using AES because 3DES is not supported in CCEAL4 mode.

### DES Support for Crypto Profiles

When downgrading to an earlier PAN-OS version, the following actions occur:
- DES is removed from the crypto profile. If DES was the only encryption type in the crypto profile, then DES is converted to 3DES.
- If DES was used in an IPSec tunnel configuration that used a manual key, the IPSec tunnel entry is removed from the configuration. After a reboot, any such IPSec tunnels no longer exist in the running configuration.

### Custom Application Signatures

Before downgrading to a release earlier than PAN-OS 7.0, you must remove any custom application signatures that have the following settings:
- **Operator** set to **Greater Than** or **Less Than**
- **Operator** set to **Equal To** and a **Context** set to any value besides `unknown-req-tcp`, `unknown-rsp-tcp`, `unknown-req-udp`, or `unknown-rsp-udp`.

### Sinkholing of DNS Signatures

After you upgrade, all Palo Alto Networks DNS signatures are enabled by default. The default action for the DNS Signatures is sinkhole, and the sinkhole IP address is a Palo Alto Networks server (71.15.192.112). This IP address is not static and can change because it is pushed using Palo Alto Networks content updates.
Support for Multi-Tenancy and Multiple Policy Sets on the VM-Series NSX Edition Firewall

If you configured the VMware Service Manager on Panorama, note the following changes that occur after you upgrade to Panorama 7.1:

- The VMware Service Manager configuration that is required for enabling communication between Panorama and the NSX Manager is separated from the Service Definition.
- A new Service Definition named Palo Alto Networks NGFW is created. This service definition includes the configuration for deploying VM-Series firewalls. It also includes a template, device group, link to the OVA for the PAN-OS version, and the auth codes you configured on the VMware service manager in the earlier version. If you did not create a template in the earlier version, then a default template called NSX_TPL is created for you.
- A zone called Palo Alto Networks profile 1 is auto-generated within the template. On a Template and Device Group Commit, the VM-Series firewalls will generate a pair of virtual wire subinterfaces (ethernet1/1.2 and ethernet1/2.2) and bind the pair to this new zone.
- All existing policy rules are retained with source and destination zone set to 'any'. These rules are functional and you do not need to modify the rules.

External Dynamic List for IP Addresses

After you upgrade, Dynamic Block List for IP addresses are renamed to External Dynamic List of Type IP Address. The earlier maximum limit 10 Dynamic Block Lists for IP addresses has changed in PAN-OS 7.1. On each firewall platform, you can now configure a maximum of 30 unique sources for External Dynamic Lists of type IP address, URL or Domain. The firewall does not impose a limit on the number of lists of a specific type.

The PA-5000 Series and the PA-7000 Series firewalls support a maximum of 150,000 total IP addresses; all other platforms support a maximum of 50,000 total IP addresses. No limits are enforced for the number of IP addresses per list. When the maximum supported IP address limit is reached on the firewall, the firewall generates a syslog message.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Upgrade Considerations</th>
<th>Downgrade Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>PA-3000 Series and PA-500 Firewall Capacity Increases</td>
<td>When you upgrade to PAN-OS 7.1, the ARP table capacity automatically increases. To avoid a mismatch when upgrading a pair of HA firewalls, you should upgrade both HA peers within a short period of time. You should also clear the ARP cache (<code>clear arp</code>) on both HA peers before you upgrade.</td>
<td></td>
</tr>
<tr>
<td>Save User Credentials</td>
<td>The Allow user to save password option, which was available in PAN-OS 7.0, is superseded by the Save User Credentials setting in PAN-OS 7.1. After you upgrade the firewall or Panorama to PAN-OS 7.1, the setting is discarded. Because the default behavior—which allows GlobalProtect to save user credentials—is the same for both options, no additional configuration is required to retain this behavior. However, to enforce behavior other than the default—for example, to prevent GlobalProtect from saving credentials altogether or from saving the password only—you must manually configure the Save User Credentials option after upgrading to PAN-OS 7.1.</td>
<td></td>
</tr>
<tr>
<td>Authentication with Secure Encrypted Cookies</td>
<td>The Authentication Modifier option, which was available in PAN-OS 7.0, is superseded by the Authentication Override options in PAN-OS 7.1. After you upgrade the firewall or Panorama to PAN-OS 7.1, any authentication modifier settings are discarded. Because the new Authentication Override options are disabled by default, to configure GlobalProtect portals and gateways to accept secure encrypted cookies, you must manually configure the new Authentication Override options in PAN-OS 7.1.</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>After you downgrade from PAN-OS 7.1.16 or a later release to PAN-OS 7.1.15 or an earlier release, you must reset the QoS Egress Max to 16,000 Mbps or less to avoid commit failures (Network &gt; QoS &gt; &lt;interface&gt; &gt; Physical Interface).</td>
<td></td>
</tr>
<tr>
<td>Gateway Configuration with Tunnel Mode</td>
<td>When tunnel mode is enabled in a GlobalProtect gateway configuration, the gateway configuration is discarded after a downgrade to an earlier major release unless you use the automatically generated saved configuration prior to upgrading.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Upgrade Considerations</td>
<td>Downgrade Considerations</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GlobalProtect portals and gateways</td>
<td></td>
<td>Loading a configuration other than running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release removes authentication profiles from GlobalProtect portals and gateways, which causes an auto-commit failure. To prevent this issue, select running-config.xml when downgrading from PAN-OS 7.1.8 to a PAN-OS 7.0 release.</td>
</tr>
</tbody>
</table>
Upgrade the Firewall to PAN-OS 7.1

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

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

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

Upgrade Firewalls Using Panorama

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

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

### Upgrade Firewalls Using Panorama

**Step 1** Save a backup of the current configuration file on each managed firewall you plan to upgrade.

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

1. Log in to Panorama, select Panorama > Setup > Operations, and Export Panorama and devices config bundle to generate and export the latest configuration backup of Panorama and of each managed device.
2. Save the exported file to a location external to the firewall. You can use this backup to restore the configuration if you have problems with the upgrade.

**Step 2** Install the content updates.

Make sure the firewalls you plan to upgrade are running content release version 564 or later.

1. Select Panorama > Device Deployment > Dynamic Updates.
2. Check Now (located in the lower left-hand corner of the window) to check for the latest updates. If an update is available, the Action column displays a Download link.
3. Download the desired version. After a successful download, the link in the Action column changes from Download to Install.
4. Click Install, select the devices on which you want to install the update, and click OK.
Upgrade the Firewall to PAN-OS 7.1

Upgrade Firewalls Using Panorama (Continued)

**Step 3** Determine the software upgrade path. You cannot skip installation of any major release versions in the path to your target PAN-OS release. For example, if you intend to upgrade from PAN-OS 6.0.13 to PAN-OS 7.1.20, you must:

- Download and install PAN-OS 6.1.0 and reboot.
- Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release; not 7.0.0).
- Download and install PAN-OS 7.0.9 or a later PAN-OS 7.0 release and reboot.
- Download PAN-OS 7.1.0 (you do not need to install it).
- Download and install PAN-OS 7.1.20 and reboot.

**Step 4** Download the software updates.

1. To access the web interface of the firewall you intend to upgrade, use the Context drop-down in Panorama or log in to the firewall directly.
2. Select **Device > Software**.
3. Check which version has a check mark in the Currently Installed column and proceed as follows:
   - If PAN-OS 7.0.9 or later is currently installed, continue to **Step 4**.
   - If a version earlier than PAN-OS 7.0.9 is currently installed, follow the upgrade path to PAN-OS 7.0.9 or a later PAN-OS 7.0 release before you upgrade to PAN-OS 7.1. Refer to the Release Notes for your currently installed PAN-OS version for upgrade instructions.

1. On Panorama, select **Panorama > Device Deployment > Software** and **Check Now** for the latest updates. If an update is available, the Action column displays a **Download** link.
2. **Download** the file or files that correspond to the Platform of the firewalls to which you are upgrading and the version to which you need to upgrade (including any intermediate major release versions). You must download a separate installation file for each platform you intend to upgrade. For example, to upgrade your PA-3050 firewalls and PA-5060 firewalls to 7.1.0, download the images that have filename PanOS_3000-7.1.0 and PanOS_5000-7.1.0. After a successful download, the Action column changes to **Install** for that image.
**Upgrade Firewalls Using Panorama (Continued)**

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

<table>
<thead>
<tr>
<th>Step 6</th>
<th>Verify the software and content release version running on each managed firewall.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. On Panorama, select <strong>Panorama &gt; Managed Devices</strong>. 2. Locate the firewalls and review the content and software versions in the table.</td>
<td>1. Perform the steps that apply to your firewall deployment: 2. Verify the software and content release version running on each managed firewall.</td>
</tr>
</tbody>
</table>
Upgrade a Firewall to PAN-OS 7.1

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

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

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

<table>
<thead>
<tr>
<th>Upgrade PAN-OS</th>
<th>Step 1</th>
<th>Step 2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Save a backup of the current configuration file.</strong></td>
<td>1. Select Device &gt; Setup &gt; Operations and Export named configuration snapshot.</td>
<td><strong>Make sure the firewall is running content release version 564 or later.</strong></td>
</tr>
<tr>
<td>Although the firewall automatically creates a configuration backup, it is a best practice to create and externally store a backup before you upgrade.</td>
<td>2. Select the XML file that contains your running configuration (for example, running-config.xml) and click OK to export the configuration file.</td>
<td>1. Select Device &gt; Dynamic Updates.</td>
</tr>
<tr>
<td>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.</td>
<td>2. Check the Applications and Threats or Applications section to determine what update is currently running.</td>
<td>2. Check the Applications and Threats or Applications section to determine what update is currently running.</td>
</tr>
<tr>
<td></td>
<td>3. If the firewall is not running the minimum required update, Check Now to retrieve a list of available updates.</td>
<td>3. If the firewall is not running the minimum required update, Check Now to retrieve a list of available updates.</td>
</tr>
<tr>
<td></td>
<td>4. Locate and Download the appropriate update.</td>
<td>4. Locate and Download the appropriate update.</td>
</tr>
<tr>
<td></td>
<td>5. After the download completes, Install the update.</td>
<td>5. After the download completes, Install the update.</td>
</tr>
</tbody>
</table>
Upgrade to PAN-OS 7.1

Upgrade the Firewall to PAN-OS 7.1

Upgrade PAN-OS (Continued)

Step 3 Determine the upgrade path.
You cannot skip installation of any major releases in the path to your target PAN-OS version. Therefore, if you intend to upgrade to a version that is more than one major release away, you must still download, install, and reboot the firewall for each intermediate major release along the upgrade path.
For example, if you want to upgrade from PAN-OS 6.0.13 to PAN-OS 7.1.1, you must:
- Download and install PAN-OS 6.1.0 and reboot.
- Download and install PAN-OS 7.0.1 and reboot (7.0.1 is the base image for the 7.0 release, not 7.0.0).
- Download and install PAN-OS 7.0.9 or a later PAN-OS 7.0 release and reboot.
- Download PAN-OS 7.1.0 (you do not need to install it).
- Download and install PAN-OS 7.1.1 and reboot.

1. Select Device > Software.
2. Check which version has a check mark in the Currently Installed column and proceed as follows:
   - If PAN-OS 7.0.9 or a later release is currently installed, continue to Step 4.
   - If a version earlier than PAN-OS 7.0.9 is currently installed, follow the upgrade path to PAN-OS 7.0.9 or a later PAN-OS 7.0 release before you upgrade to PAN-OS 7.1.
   Refer to the Release Notes for your currently installed PAN-OS version for upgrade instructions.

Step 4 Install PAN-OS 7.1.
If your firewall does not have Internet access from the management port, you can download the software update from the Palo Alto Networks Support Portal. You can then manually Upload it to your firewall.

1. Check Now for latest updates.
2. Locate and Download the version to which you intend to upgrade.
3. After the download completes, Install the update.
4. After the installation successfully completes, reboot using one of the following methods:
   - If you are prompted to reboot, click Yes.
   - If you are not prompted to reboot, select Device > Setup > Operations and Reboot Device (Device Operations section).

Step 5 Verify that the firewall is passing traffic.
Select Monitor > Session Browser.

Upgrade an HA Firewall Pair to PAN-OS 7.1

Review the PAN-OS 7.1 Release Notes and then use the following procedure to upgrade a pair of firewalls in a high availability (HA) configuration. This procedure applies to both active/passive and active/active configurations.

When upgrading peers in an HA configuration, you must upgrade each firewall separately. Consequently, there is a period of time when PAN-OS versions differ on the individual firewalls in the HA pair. If you have session synchronization enabled, this will continue to function during the upgrade process as long as you are upgrading from one feature release to the next consecutive feature release, for example, from PAN-OS 7.0.9 to a PAN-OS 7.1 release. If you are upgrading the pair from an older feature release of PAN-OS, session...
syncing between the firewalls will not work and, if a failover occurs before both firewalls are running the same version of PAN-OS, session forwarding could be impacted. In this case, if session continuity is required, you must temporarily permit non-syn-tcp while the session table is rebuilt as describe in the following procedure.

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

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

### Upgrade PAN-OS

<table>
<thead>
<tr>
<th>Step 1: Save a backup of the current configuration file.</th>
<th>Perform these steps on each firewall in the pair:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Although the firewall automatically creates a backup of the configuration, it is a best practice to create and externally store a backup before you upgrade.</td>
<td>1. Select <strong>Device &gt; Setup &gt; Operations</strong> and <strong>Export named configuration snapshot</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select the XML file that contains your running configuration (for example, <code>running-config.xml</code>) and click <strong>OK</strong> to export the configuration file.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2: Make sure each device is running content release version 564 or later.</th>
<th>1. Select <strong>Device &gt; Dynamic Updates</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2. Check the <strong>Applications and Threats</strong> or <strong>Applications</strong> section to determine what update is currently running.</td>
</tr>
<tr>
<td></td>
<td>3. If the firewall is not running the minimum required update, <strong>Check Now</strong> to retrieve a list of available updates.</td>
</tr>
<tr>
<td></td>
<td>4. Locate and <strong>Download</strong> the content release version you intend to install.</td>
</tr>
<tr>
<td></td>
<td>5. After the download completes, <strong>Install</strong> the update.</td>
</tr>
</tbody>
</table>
### Upgrade PAN-OS (Continued)

**Step 3** Determine the upgrade path.

You cannot skip installation of any major releases in the path to your desired PAN-OS version. Therefore, if you intend to upgrade to a version that is more than one major release away, you must download, install, and reboot the firewall for each intermediate major PAN-OS releases along the upgrade path. For example, if you want to upgrade from PAN-OS 6.0.13 to PAN-OS 7.1.1, you must:

- Download and install PAN-OS 6.1.0 and reboot.
- Download PAN-OS 7.0.1 (7.0.1 is the base image for the 7.0 release; not 7.0.0).

*Although we recommend that you install PAN-OS 7.0.1 before you upgrade to PAN-OS 7.0.9 or a later PAN-OS 7.0 release, do not reboot the firewall after installing this image in an HA configuration.*

- Download and install PAN-OS 7.0.9 or a later PAN-OS 7.0 release and reboot.
- Download PAN-OS 7.1.0 (you do not need to install it).
- Download and install PAN-OS 7.1.1 and reboot.

**Step 4** Install PAN-OS 7.1 on the passive device (active/passive) or on the active-secondary device (active/active).

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

1. Select **Device > Software**.
2. Check which version has a check mark in the Currently Installed column and proceed as follows:
   - If PAN-OS 7.0.9 or a later release is currently installed, continue to **Step 4**.
   - If a version earlier than PAN-OS 7.0.9 is currently installed, follow the upgrade path to PAN-OS 7.0.9 or a later PAN-OS 7.0 release before you upgrade to PAN-OS 7.1. Refer to the Release Notes for your currently installed PAN-OS version for upgrade instructions.

### Upgrade PAN-OS (Continued)

1. **Check Now** for the latest updates.
2. Locate and **Download** the version to which you intend to upgrade.
3. After the download completes, **Install** the update.
4. After the installation completes successfully, reboot using one of the following methods:
   - If you are prompted to reboot, click **Yes**.
   - If you are not prompted to reboot, select **Device > Setup > Operations** and **Reboot Device** (Device Operations section). After the reboot, the device will not be functional until the active/active-primary device is suspended.
### Upgrade PAN-OS (Continued)

#### Step 5  
Suspend the active/active-primary firewall.

1. On the active (active-passive) or active-primary (active-active) peer, select **Device > High Availability > Operational Commands**.
2. **Suspend local device**.
3. Select **Dashboard** and verify that the state of the passive device changes to active in the High Availability widget.
4. Verify that the firewall that took over as active (or active-primary) and is passing traffic (**Monitor > Session Browser**).
5. **(Optional)** If you have session synchronization enabled and you are currently running a PAN-OS version prior to 6.1.0, run the `set session tcp-reject-non-syn no` operational command. This will rebuild the session table so that sessions that started prior to the upgrade will continue.

#### Step 6  
Install PAN-OS 7.1 on the other peer in the pair.

If your firewall does not have Internet access from the management port, you can download the software update from the Palo Alto Networks Support Portal. You can then manually **Upload** it to your firewall.

1. **Check Now** for the latest updates.
2. Locate and **Download** the version to which you intend to upgrade.
3. After the download completes, **Install** the update.
4. After the installation completes successfully, reboot using one of the following methods:
   - If you are prompted to reboot, click **Yes**.
   - If you are not prompted to reboot, select **Device > Setup > Operations** and **Reboot Device** in the Device Operations section. After the reboot, the device will not be functional until the active/active-primary device is suspended.
5. **(Optional)** If you configured the firewall to temporarily allow non-syn-tcp traffic in order to enable the firewall to rebuild the session table in **Step 4**, revert back by running the `set session tcp-reject-non-syn yes` command.

   If the preemptive option is configured, the current passive peer will revert to active when state synchronization is complete.
**Step 7** Verify that the firewalls are passing traffic as expected.
In an active/passive deployment, the active peer (only) should be passing traffic while both peers should be passing traffic in an active/active deployment.

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

- **(Active peer(s) only)** To verify that active peers are passing traffic, run the `show session all` command.
- To verify session synchronization, run the `show high-availability interface ha2` command and make sure that the Hardware Interface counters on the CPU table are increasing as follows:
  - In an active/passive configuration, only the active peer show packets transmitted and the passive device will only show packets received.
  - If you have enabled HA2 keep-alive, the hardware interface counters on the passive peer will show both transmit and receive packets. This occurs because HA2 keep-alive is bidirectional which means that both peers transmit HA2 keep-alive packets.
  - In an active/active configuration, you will see packets received and packets transmitted on both peers.
Downgrade from PAN-OS 7.1

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

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

Always downgrade into a configuration that matches the software version. Unmatched software versions and configurations can result in failed downgrades or force the system into maintenance mode. This only applies to a downgrade from one feature release to another (for example 7.1.1 to 7.0.9), not to downgrades to maintenance releases within the same feature release version (for example, 7.1.1 to 7.1.0).

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

Because maintenance releases do not introduce new features, you can downgrade to a previous maintenance release in the same feature release without having to restore the previous configuration. A maintenance release is a release in which the third digit in the release version changes, for example a downgrade from 7.1.1 to 7.1.0 is considered a maintenance release downgrade because only the third digit in the release version is different.

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

<table>
<thead>
<tr>
<th>Downgrade to a Previous Maintenance Release</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Downgrade from PAN-OS 7.1 to any version earlier than PAN-OS 5.0.5 is not supported because the log management subsystem has been significantly enhanced between PAN-OS 5.0 and PAN-OS 6.0. Because of the changes implemented in the log partitions, a firewall that is downgraded to PAN-OS 5.0.4 and earlier releases cannot accurately estimate the disk capacity available for storing logs and the log partition can reach maximum capacity without a user notification. Such a situation allows the log partition to reach 100% capacity, which results in a loss of logs.

**Downgrade to a Previous Feature Release**

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

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

### Downgrade to a Previous Feature Release

**Step 1** Save a backup of the current configuration file.

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

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

**Step 2** Install the previous feature release image.

- Autosave versions are created when you upgrade to a new release beginning with PAN-OS 4.1. If you are downgrading to a release prior to PAN-OS 4.1, you may need to do a factory reset and restore the device.

2. Locate the image to which you want to downgrade. If the image is not already downloaded, then `Download` it. (If the image is already downloaded, you can skip this step.)
3. After the download completes, `Install` the image.
4. Select a configuration to load after the device reboots from the `Select a Config File for Downgrading` drop-down. In most cases, you should select the autosaved configuration that was created when you upgraded from the release to which you are now downgrading. For example, if you are running PAN-OS 7.1.1 and want to downgrade to PAN-OS 7.0.3, select autosave-7.0.3.
5. After the installation completes successfully, reboot using one of the following methods:
   - If you are prompted to reboot, click `Yes`.
   - If you are not prompted to reboot, select `Device > Setup > Operations` and `Reboot Device` (Device Operations section).
**Downgrade While Maintaining Enhanced Capacities on PA-3050 Firewalls and PA-3020 Firewalls**

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

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

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

### Downgrade PA-3000 Series and PA-500 Firewalls and Preserve PA-3000 Series Firewall Capacity Increases on Downgrade

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