



Release Notes

FortiWeb 7.6.4



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



May 30, 2025

FortiWeb 7.6.4 Release Notes

TABLE OF CONTENTS

Introduction	4
What's New	5
Product Integration and Support	6
Upgrade instructions	8
Upgrade notes and important information	9
Image checksums	11
Supported upgrade paths	12
Repartitioning the hard disk	17
To use the special firmware image to repartition the operating system's disk	18
To repartition the operating system's disk without the special firmware image	18
Upgrading an HA cluster	20
Downgrading to a previous release	20
FortiWeb-VM license validation after upgrade from pre-5.4 version	21
Resolved issues	22
Known issues	24

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 7.6.4, build 1062.

FortiWeb is a web application firewall (WAF) that protects hosted web applications from attacks that target known and unknown exploits. Using multi-layered and correlated detection methods, FortiWeb defends applications from known vulnerabilities and zero-day threats. The Web Application Security Service from FortiGuard Labs uses information based on the latest application vulnerabilities, bots, suspicious URL and data patterns, and specialized heuristic detection engines to keep your applications safe.

FortiWeb also offers a machine-learning function that enables it to automatically detect malicious web traffic. In addition to detecting known attacks, the feature can detect potential unknown zero-day attacks to provide real-time protection for web servers.

FortiWeb allows you to configure these features:

- Vulnerability scanning and patching
- IP reputation, web application attack signatures, credential stuffing defense, anti-virus, and Fortinet Sandbox powered by FortiGuard.
- Real-time attack insights and reporting with advanced visual analytics tools
- Integration with FortiGate and FortiSandbox for ATP detection
- Behavioral attack detection
- Advanced false positive and negative detection avoidance

FortiWeb hardware and virtual machine platforms are available for medium and large enterprises, as well as for service providers.

For additional documentation, please visit the FortiWeb documentation:

<http://docs.fortinet.com/fortiweb/>

What's New

FortiWeb 7.6.4 introduces enhancements and new features across various modules including Web Application Firewall (WAF) capabilities, server configurations, system settings, etc. Refer to [this link](#) for the new features.

Product Integration and Support

Supported Hardware:

D-Series:

- FortiWeb 100D
- FortiWeb 400D
- FortiWeb 600D
- FortiWeb 1000D

E-Series:

- FortiWeb 100E
- FortiWeb 400E
- FortiWeb 600E
- FortiWeb 1000E
- FortiWeb 2000E
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000E

F-Series:

- FortiWeb 100F
- FortiWeb 400F
- FortiWeb 600F
- FortiWeb 1000F
- FortiWeb 2000F
- FortiWeb 3000F
- FortiWeb 4000F

Supported hypervisor versions:

- VMware vSphere Hypervisor ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0/6.5/6.7/7.0/8.0.2/8.0.3
- Citrix XenServer 6.2/6.5/7.1
- Open source Xen Project (Hypervisor) 4.9 and higher versions
- Microsoft Hyper-V (version 6.2 or higher, running on Windows 8 or higher, or Windows Server 2012/2016/2019/2022)
- KVM (Linux kernel 2.6, 3.0, or 3.1)
- OpenStack Wallaby
- Docker Engine CE 18.09.1 or higher versions, and the equivalent Docker Engine EE versions; Ubuntu 18.04.1 LTS or higher versions
- Nutanix AHV

FortiWeb is tested and proved to function well on the hypervisor versions listed above. Later hypervisor releases may work but have not been tested yet.

To ensure high performance, it's recommended to deploy FortiWeb-VM on the machine types with minimum 2 vCPUs, and memory size larger than 8 GB.

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- Google Cloud
- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud

Supported web browsers:

- Microsoft Edge 41
- Mozilla Firefox version 59
- Google Chrome version 65

Other web browsers may function correctly, but are not supported by Fortinet.

Build-in AV engine version: 7.00041

Upgrade instructions

Upgrade notes and important information

Upgrading to the latest FortiWeb release may involve specific considerations when transitioning from previous versions. This section outlines essential warnings, potential issues, and key information users need to be aware of to ensure a smooth and successful upgrade. Please review all details carefully to avoid compatibility issues and to take full advantage of the latest features and improvements.

Key sections:

- [Common Upgrade Issues and Solutions on page 9](#)
- [Known Issues and Workarounds on page 10](#)
- [FortiWeb-VM Specific Notes on page 11](#)

Common Upgrade Issues and Solutions

Backup Restoration Issue After Enabling Private Encryption Key

When `private-encryption-key` is enabled with the following commands in versions prior to 7.6.3, backup files may no longer be restorable after the upgrade. To avoid this issue, please ensure you create a new backup after upgrading to version 7.6.3.

```
config system encryption-method
  set private-encryption-key enable
end
```

Log Delay Post-Upgrade (6.4.x & 7.0)

In several hours or days (depending on the number of existing logs) after upgrading from earlier versions, there might be a delay (30-60 mins) in displaying new logs on the GUI. This is caused by the log version upgrade in 6.4.x & 7.0. It takes time to scan and process all existing logs.

Browser Cache Issues After Upgrade

After upgrading FortiWeb to a new version, you may occasionally encounter issues where the browser continues to use a cached version of the GUI instead of fetching the updated resources from the server.

Recommendation: To ensure all resources are refreshed and the GUI functions correctly, we recommend clearing the browser cache after completing the upgrade.

Error Message to Ignore

During the upgrade, the following error message may appear in the console. This is expected and does not require any action.

```
System is started!!!

System is running with new partition table
Couldn't find valid filesystem superblock.
Skip resize of the 3rd partition

mke2fs 1.44.5 (15-Dec-2018)
ext2fs_check_if_mount: Can't check if filesystem is mounted due to missing mtab
file while determining whether /dev/sda3 is mounted.
Creating filesystem with 50000 4k blocks and 50048 inodes
Filesystem UUID: c6f27062-46ca-4501-8936-f6bfb1e93e1
Superblock backups stored on blocks:
    32768

Allocating group tables: done
Writing inode tables: done
```

Known Issues and Workarounds

Compatibility Issue with FortiWeb 100D and 7.6.0/7.6.1

DO NOT update to 7.6.0/7.6.1 for FortiWeb 100D.

Global Settings and Configuration Loss (Pre-7.6.1)

On versions earlier than 7.6.1, a non-`prof_admin` user changing any global settings — such as executing the commands `config system global` and `config system admin` or modifying equivalent settings in the GUI — can result in the loss of the `prof_admin` user's configurations after a system reboot.

To prevent this configuration loss, we recommend the following workaround before upgrading:

1. Log in with a "prof_admin" account.
2. Make a change to a global setting (e.g., config the hostname).
3. Reboot the system.

In summary, ensure that the last change to any global setting is made by a "prof_admin user" before rebooting the system.

Note: This issue has been resolved in versions 7.2.10, 7.4.5, 7.6.1, and later. If you are upgrading from these versions, the recommended workaround is unnecessary.

Admin Password Hash Change (Post-7.2.0)

The admin user password hash is changed from SHA1 to SHA256 starting from version 7.2.0. If you upgrade from versions earlier than 7.2.0, the hash will remain the same as before, but if the admin user changes their password or if new admin users are added, the password hash will be updated to SHA256.

Port 995 Disabled (Pre-7.2.0)

If upgrading from versions earlier than 7.2.0, port 995 will be switched to a disabled state. Remember to manually enable it in **System > Admin > Settings** if required for configuration synchronization.

VLAN and IP Address Conflicts Post-7.2.3 Upgrade

VLAN interfaces/interfaces with overlapping IP addresses and the VIP/Server Policy bound to them cannot be imported (while loading the config file) after upgrading to 7.2.3 and later due to the implementation of an IP overlap check in this release.

Workaround: Downgrade to an earlier version through booting from the alternate partition (see "Bootting from the alternate partition"). The old configuration can be restored through this method, edit IP addresses to eliminate overlapping, and then upgrade to 7.6.2.

Maintenance for 6.4.x

We do not provide maintenance for 6.4.x releases unless major errors occur. We recommend upgrading 6.4.x to later versions.

Configuration Reset on Upgrades Before 6.0

When upgrading from releases prior to version 6.0, the "Retain Packet Payload" settings in Log & Report > Log Config > Other Log Settings will be reset to new defaults. This means that the following features — JSON Protection, Syntax-Based Detection, Malicious Bots, Known Good Bots, Mobile API Protection, and API Management — will be disabled. If you had these options enabled prior to the upgrade, please remember to re-enable them if they are still required.

FortiWeb-VM Specific Notes

VM License Upgrade Requirement

- For FortiWeb-VM with a license purchased earlier than February 2019, you must upgrade to 6.3.4 or higher. Do not use a lower patch.
- The VLAN, 802.3ad Aggregate, and Redundant interfaces are not supported on -VMs deployed on public cloud platforms since 6.3.6. If you upgrade from versions earlier than that, these configurations will be removed.

FortiWeb-VM Troubleshooting for Persistent Issues

If issues persist after the upgrade, consider deploying a new FortiWeb-VM instance with the 7.6.4 image and a trial license. You can download necessary database files from the support site to maintain valid services temporarily.

Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

<https://support.fortinet.com>

VM Image integrity is also verified when the FortiWeb is booting up. the running OS will generate signatures and compare them with the signatures attached to the image. If the signatures do not match, the running OS will be shutdown.

To download the Customer Service & Support image checksum tool

After logging in to the website, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. This button appears only if one or more of your devices has a current support contract. In the **File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Supported upgrade paths

This section discusses the general paths to upgrade FortiWeb from previous releases.

If you are upgrading from a version that is 7.6.1 or lower, then you will need to upgrade to version 7.6.2 before proceeding with subsequent updates.

For example, to upgrade from 7.2.1 to 7.6.4, you will follow the upgrade path below:

7.2.1 → 7.6.2 → 7.6.4



Version 7.6.2 introduces an expanded partition size. Ensure the log disk has at least 1.5 GB of free space before upgrading.

For details, refer to the [FortiWeb 7.6.2 Release Notes](#).

To upgrade to FortiWeb 7.6.4

Upgrade to version 7.6.2 before proceeding to upgrade to version 7.6.4.

To upgrade from FortiWeb 7.6.0/7.6.1 to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 7.4.x to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 7.2.x to 7.6.2

Upgrade directly.



If you had enabled Threat Analytics in previous releases but did not have a valid license, the 14-day eval license will be automatically applied after upgrading to version 7.2.2 and later.

In this case, if you don't want to start the 14-day eval immediately after upgrade, it's recommended to disable the Threat Analytics first, then execute upgrade.

To upgrade from FortiWeb 7.0.x to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 6.4.x to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 6.3.x to 7.6.2

Upgrade directly.



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

To upgrade from FortiWeb 6.1.x and 6.2.x to 7.6.2

Upgrade directly.

The machine learning data will be lost after the upgrade as the database format is enhanced in 6.3.0. Machine Learning will automatically start collecting data again after the upgrade.



For FortiWeb-VM on docker platform, it's not supported to upgrade to 7.6.4 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.6.4 instead of upgrading to 7.6.4. For how to install, see [FortiWeb-VM on docker](#).



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

To upgrade from FortiWeb 6.0 or 6.0.x to 7.6.2

Upgrade directly.

After the upgrade:

- If you upgrade from 6.0, there might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
 - Run `get system status` to check the Database Status.
 - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.
- If you upgrade from 6.0.1, it's not necessary to run `execute db rebuild` because the database format has already been enhanced in 6.0.1, so that it's compatible with the new database.



The machine learning data will be lost after the upgrade as the database format is enhanced in 6.3.0. Machine Learning will automatically start collecting data again after the upgrade.



For FortiWeb-VM on docker platform, it's not supported to upgrade to 7.6.4 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.6.4 instead of upgrading to 7.6.4. For how to install, see [FortiWeb-VM on docker](#).



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

To upgrade from FortiWeb 5.5.x, 5.6.x, 5.7.x, 5.8.x, or 5.9.x to 7.6.2

Before the upgrade:

- If you upgrade from a version of FortiWeb previous to 5.9.0 on Azure platform, first change the addressing mode to DHCP in **Network > Interface**, then upgrade to FortiWeb 6.1.1, because FortiWeb on Azure platform has enforced the DHCP addressing mode since release 5.9.0.

After the upgrade:

- There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
 - Run `get system status` to check the Database Status.
 - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.
-



If you upgrade from a version of FortiWeb previous to 5.5.4, the upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

To upgrade from FortiWeb 5.4.x to 7.6.2

Before the upgrade:

- Resize your FortiWeb hard disk partitions. See [Repartitioning the hard disk](#).

After the upgrade:

- There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
 - Run `get system status` to check the Database Status.
 - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.



The upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

To upgrade from FortiWeb 5.3.x to 7.6.2

Before the upgrade:

- Resize your FortiWeb hard disk partitions. See [Repartitioning the hard disk](#).

After the upgrade:

- There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
 - Run `get system status` to check the Database Status.
 - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.



- If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see [FortiWeb-VM license validation after upgrade from pre-5.4 version](#).
- The upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If you upgrade from a version of FortiWeb previous to 5.3.4 and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.
- If you upgrade from a version of FortiWeb previous to 5.3.6, the upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

To upgrade from a version previous to FortiWeb 5.3 to 7.6.2

FortiWeb5.3.exe is a Microsoft Windows executable script that automatically migrates your FortiWeb 5.2.x configuration settings to a 5.3.x configuration.

1. If your version is 5.0.x or 5.1.x, upgrade to FortiWeb 5.2.x.
2. Use **System > Maintenance > Backup & Restore** to back up your FortiWeb configuration. Fortinet recommends that you use the **Backup entire** configuration option.
3. To obtain the upgrade script, log in to the Fortinet Customer Service & Support website:
<https://support.fortinet.com>

In the menus at the top of the page, click **Download**, and then click **Firmware Images**.

4. For product, select **FortiWeb**. Then, on the Download tab, navigate to the following folder:
/FortiWeb/v5.00/5.3/Upgrade_script/
5. Download the .zip compressed archive (for example, `FortiWeb5.3Upgrade_v1.9.zip`) to a location you can access from your Windows PC.
6. In Windows, extract the .zip archive's contents, and then use a command line interface to execute the upgrade script.

For example, in the directory where the file `FortiWeb5.3Upgrade.exe` and your backup configuration file are located, execute the following command:

```
FortiWeb5.3Upgrade.exe -i YOUR_CONFIG_NAME.conf -o 5.3_new.conf
```

The script removes the Domain Server, Physical Server, Server Farm, Content Routing policy configurations and generates a new configuration file named `5.3_new.conf`.

7. Resize your FortiWeb hard disk partitions. See [Repartitioning the hard disk](#).
8. Upgrade to 6.3.9 first, then upgrade to 7.6.4.
9. Use **System > Maintenance > Backup & Restore** to restore the configuration file you created using the script (for example, `5.3_new.conf`).

10. There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2:

- Run `get system status` to check the Database Status.
- If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.



- If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see [FortiWeb-VM license validation after upgrade from pre-5.4 version](#).
- The upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.
- The upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

Note: To upgrade from 4.0 MR4, Patch x or earlier, please contact Fortinet Technical Support.

Repartitioning the hard disk

To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb operating system's disk.

In most cases, you'll have to install a special firmware image to repartition the disk. For details, see [To use the special firmware image to repartition the operating system's disk on page 18](#).

For the following FortiWeb-VM tools, you cannot install the special firmware image to repartition the hard disk:

- Citrix XenServer
- Open-source Xen Project
- Microsoft Hyper-V
- KVM

For these platforms, to repartition the disk you must deploy a new virtual machine and restore the configuration and log data you backed up earlier. See [To repartition the operating system's disk without the special firmware image on page 18](#).



Repartitioning affects the operating system's disk (USB/flash disk), not the hard disk. Existing data such as reports and event, traffic, and attack logs, which are on the hard disk, are not affected.

You can use this image to upgrade an HA cluster by following the same procedure you use for a regular firmware upgrade. For details, see "Updating firmware on an HA pair" in the *FortiWeb Administration Guide*:
<http://docs.fortinet.com/fortiweb/admin-guides>

To use the special firmware image to repartition the operating system's disk

1. Perform a complete backup of your FortiWeb configuration.
Although the repartitioning firmware image automatically saves your FortiWeb configuration, Fortinet recommends that you also manually back it up. For details, see the *FortiWeb Administration Guide*:
<http://docs.fortinet.com/fortiweb/admin-guides>
2. Contact Fortinet Technical Support to obtain the special repartitioning firmware image: special build 5.4.1, build 6066.
3. Follow one of the same procedures that you use to install or upgrade firmware using a standard image:
 - In the Web UI, go to **System > Status > Status**. Locate the **System Information** widget. Beside **Firmware Version**, click **[Update]**.
 - In the Web UI, go to **System > Maintenance > Backup & Restore**. Select the **Restore** option in **System Configuration**.
 - In the CLI, enter the `execute restore config` command.

FortiWeb backs up the current configuration, resizes the hard drive partitions, and boots the system.

Continue with the instructions in [Supported upgrade paths on page 12](#).

To repartition the operating system's disk without the special firmware image

1. Perform a complete backup of your FortiWeb configuration. For details, see the *FortiWeb Administration Guide*:
<http://docs.fortinet.com/fortiweb/admin-guides>
2. Use the instructions for your hypervisor platform to detach the log disk from the VM:
 - [To detach the log disk from a Citrix XenServer VM on page 19](#)
 - [To detach the log disk from a Microsoft Hyper-V VM on page 19](#)
 - [To detach the log disk from a KVM VM on page 19](#)
3. Deploy a new FortiWeb 5.5 or later virtual machine on the same platform.
4. Use the instructions for your hypervisor platform to attach the log disk you detached earlier to the new VM:
 - [To attach the log disk to a Citrix XenServer VM on page 19](#)
 - [To attach the log disk to a Microsoft Hyper-V VM on page 19](#)
 - [To attach the log disk to a KVM VM on page 19](#)
5. Restore the configuration you backed up earlier to the new VM.
6. When you are sure that the new VM is working properly with the required configuration and log data, delete the old VM.

To detach the log disk from a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the VM, on the Storage tab, select **Hard disk 2**, and then click **Properties**.
3. For **Description**, enter a new description, and then click **OK**.
4. Select **Hard disk 2** again, and then click **Detach**.
5. Click **Yes** to confirm the detach task.

To detach the log disk from a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the FortiWeb-VM in the list of machines, and then, under **Actions**, click **Settings**.
2. Select **Hard Drive (data.vhd)**, and then click **Remove**.
3. Click **Apply**.

To detach the log disk from a KVM VM

1. In Virtual Machine Manager, double-click the FortiWeb-VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.

To attach the log disk to a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the new, FortiWeb 5.5 or later VM, on the Storage tab, select **Hard disk 2**, and then click **Delete**.
3. Click **Yes** to confirm the deletion.
4. On the Storage tab, click **Attach Disk**.
5. Navigate to the hard disk you detached from the old VM to attach it.
6. Start your new virtual machine.

To attach the log disk to a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the new, FortiWeb 5.5 or later virtual machine in the list of machines, and then, under **Actions**, click **Settings**.
2. Select **Hard Drive (log.vhd)**, and then click **Browse**.
3. Browse to the hard drive you detached from the old virtual machine to select it.
4. Click **Apply**.
5. Start the new virtual machine.

To attach the log disk to a KVM VM

For KVM deployments, you remove an existing virtual disk from the new VM before you attach the disk detached from the original VM.

1. In Virtual Machine Manager, double-click the new, FortiWeb 5.5 or later VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.
4. Click **Add Hardware**.
5. Click **Storage**, select **Select managed or other existing storage**, and then click **Browse**.
6. Click **Browse Local**.

7. Navigate to the log disk file for the original machine to select it, and then click **Open**.
8. For **Device type**, select **Virtio disk**, for **Storage format**, select **qcow2**, and then click **Finish**.
9. Start the new virtual machine.

Upgrading an HA cluster

If the HA cluster is running FortiWeb 4.0 MR4 or later, the HA cluster upgrade is streamlined. When you upgrade the active appliance, it automatically upgrades any standby appliance(s), too; no manual intervention is required to upgrade the other appliance(s). This includes upgrading using the special hard disk repartitioning firmware image for upgrading to 5.5 or later from earlier releases.

If the HA cluster is running FortiWeb 4.0 MR3 Patch x or earlier, contact Fortinet Technical Support for assistance.

Downgrading to a previous release



We don't recommend performing a downgrade because unexpected results may occur. If you insist on a downgrade, please first contact FortiWeb Technical Support team.

Please be aware that both uploading and switching to a lower version image are considered a downgrade operation.

ML based modules data loss

The machine learning data will be lost if you downgrade to versions lower than 6.2.0. It cannot be recovered because the database architecture is changed since 6.2.0.

Log compatibility issue

There might be log compatibility issue between different FortiWeb versions. If logs are not available on GUI after downgrading to an earlier version, please run `execute database rebuild`.

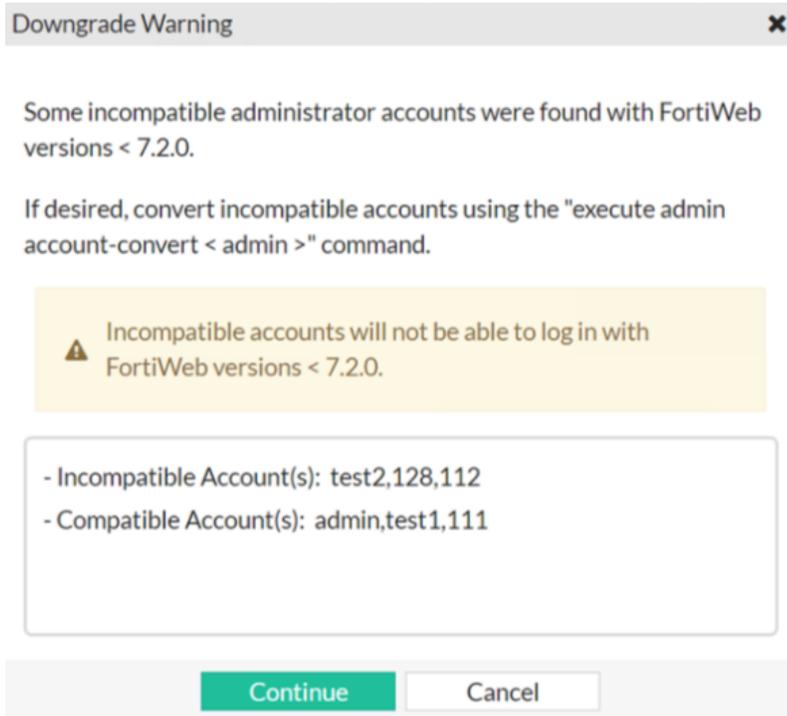
Basic configuration preserved if downgrading to 5.1 or 5.0

When you downgrade to version 5.1 or 5.0, the basic configuration for your appliance's connections to the network (e.g., IP address and route configuration) is preserved.

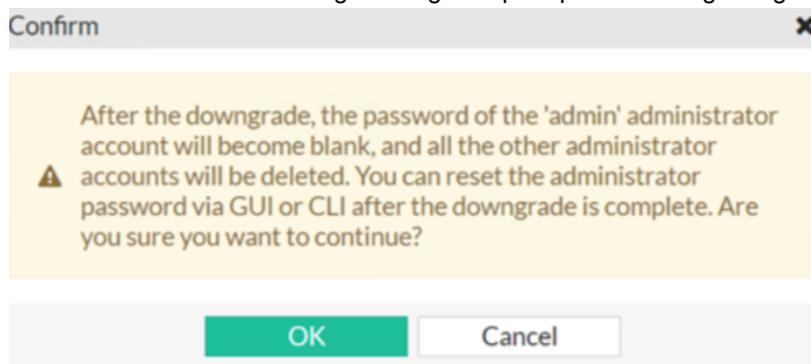
Admin user password hash change

The admin user password hash is changed from sha1 to sha256 since 7.2.0. **System > Admin > Administrators**

If you downgrade to 7.0.x and 7.1.x, you may need to convert password hash otherwise the admin users can't log in with their credentials. The following message will prompt after downgrading:



If you downgrade to versions earlier than 7.0, you need to recreate the lost accounts **System > Admin > Administrators**. The following message will prompt after downgrading:



FortiWeb-VM license validation after upgrade from pre-5.4 version

On some virtual machine deployments, upgrading FortiWeb-VM from a version previous to 5.4 changes the virtual machine's universal unique identifier (UUID). Because of this change, the first time you upload your existing FortiWeb-VM license, the FortiGuard Distribution Network (FDN) server reports that it is invalid.

To solve this problem, after you have uploaded the license, wait 90 minutes, and then upload the license again.

This issue does not affect FortiWeb-VM deployed on a VMware vSphere hypervisor.

Resolved issues

This section lists issues that have been fixed in version 7.6.4. For inquiries about a particular bug, please contact Fortinet Customer Service & Support: <https://support.fortinet.com>

Bug ID	Description
1158537	<code>proxyd</code> crash occurred due to the use of an uninitialized pointer, which led to invalid memory access during request handling.
1156928/ 1143509/ 1128127	Dashboard widgets failed to display because the <code>config system dashboard-widget</code> table exceeded the maximum entry limit of 256, preventing widget loading and creation after upgrade. The limit has been increased to 1024 in the fix.
1140903	When using the Least Connection algorithm, servers exiting Maintenance Mode could receive all new connections due to inaccurate session statistics, including negative values. This issue has been fixed by recalculating session data during policy reload.
1140417	HA fails to synchronize in AAH mode when an External IP connector is configured due to last-update timestamp mismatches, as primary and secondary nodes update IP lists independently.
1138459	JavaScript errors appeared in browser console logs after upgrade due to use of unsupported syntax (<code>hookXHR</code> , nullish coalescing assignment, and <code>const</code>) in the <code>ajaxhook.js</code> script. The script has been rewritten to remove modern JavaScript features and ensure compatibility with older browsers.
1133888	When creating a custom rule through the GUI and clicking OK to save the configuration, the corresponding <code>set signature</code> command disappears from the CLI.
1133642	Traffic could hang on FortiWeb due to a dead loop in the AV engine when scanning truncated gzip or bzip content with optimization enabled. The decompression buffer handling logic has been fixed.
1133199	The "Blocked IPs" monitor failed to display data when accessed by SSO admin users due to incorrect <code>mkey</code> handling in the dashboard widget API. The issue was resolved by adding logic to assign the correct <code>mkey</code> prefix (<code>sso</code> or <code>sys</code>) based on the user type.
1130296	FortiWeb did not perform URL canonicalization when matching OpenAPI-defined paths, causing requests with or without trailing slashes to be treated as different endpoints. As a result, OpenAPI validation rules were inconsistently applied, allowing some invalid requests to bypass enforcement.
1129479	Pressing Enter in the Automation CLI Script editor incorrectly triggered the Save action instead of inserting a new line, making it difficult to edit multi-line scripts. This has been fixed so that Enter now correctly adds a new line in the script editor.

Bug ID	Description
1123449	OpenAPI validation failed to prioritize specific literal paths over templated paths, resulting in incorrect policy matching. Additionally, improper handling of the <code>oneOf</code> schema construct caused validation errors.
1121774	The event log message "Source Address running low for 127.0.0.1 → 127.0.0.1" was triggered under normal conditions and did not indicate an actual port exhaustion issue. The logging behavior has been corrected to prevent false alarms.
1115495	IPv6 packets with VLAN tagging intermittently contain an IPv4 header, causing downstream devices to drop them. This issue is caused by an incorrect <code>eth->h_proto</code> value of <code>ETH_P_IP</code> in the IPv6 packets.
1113220	Scheduled SFTP backups are not running after upgrading to version 7.4.6 due to a race condition where <code>cron</code> and <code>ftp_backup</code> start almost simultaneously. This prevents <code>cron</code> from reading the updated <code>/tmp/crontab</code> file, causing the backup to fail.
1106859	FortiWeb failed to detect and block the EICAR test file when it was Base64-encoded before upload. The issue occurred due to limitations in Base64 content inspection. Detection logic has been improved to support Base64-encoded payloads.
1104146	Intermittent 500 errors occur on a specific site due to DNS resolution failures, caused by low TTL values (0-2 seconds) in DNS answer records, which prevent proper caching. This results in HTTP code 0 being logged in traffic logs, but no attack logs are generated. The issue is resolved by setting a minimum TTL of 10 seconds for DNS caching, ensuring successful lookups, with a potential side effect of stale records for up to 10 seconds.

Common Vulnerabilities and Exposures

For more information, visit <https://www.fortiguard.com/psirt>.

Bug ID	Description
1129747	FortiWeb 7.6.4 is no longer vulnerable to the following CVE-Reference: CVE-2025-26466.
1105473	FortiWeb 7.6.4 is no longer vulnerable to the following CVE-Reference: CVE-2025-25254.

Known issues

The following issues have been identified in version 7.6.4. To inquire about a particular bug or report a bug, please contact Fortinet Customer Service & Support: <https://support.fortinet.com>.

Bug ID	Description
1177524	When attempting to view a generated report from the GUI, the process fails with the error message: "Requested URL not found." Workaround: configure the system to send reports in alternative formats (PDF, MS Word, Text, and MHT) via Email or FTP
1158769	HA synchronization may fail if a Let's Encrypt certificate with a wildcard domain name is present on the primary device. The certificate does not sync to the secondary unit, causing the HA status to remain in INIT. Deleting the certificate allows synchronization to complete successfully.



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.