



# Release Notes

FortiWeb 8.0.3



**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](mailto:techdoc@fortinet.com)



December 12, 2025

FortiWeb 8.0.3 Release Notes

# TABLE OF CONTENTS

|                                                                               |           |
|-------------------------------------------------------------------------------|-----------|
| <b>Introduction</b>                                                           | <b>4</b>  |
| <b>What's New</b>                                                             | <b>5</b>  |
| <b>Product Integration and Support</b>                                        | <b>6</b>  |
| <b>Upgrade instructions</b>                                                   | <b>8</b>  |
| 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        |
| <b>Resolved issues</b>                                                        | <b>23</b> |
| <b>Known issues</b>                                                           | <b>26</b> |

# Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 8.0.3, build 0083.

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 8.0.3 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 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:** 7.00047

# 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 8.0.3 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 8.0.3, you will follow the upgrade path below:

7.2.1 → 7.6.2 → 8.0.3



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 8.0.3

Upgrade to version 7.6.2 before proceeding to upgrade to version 8.0.3.

### 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 8.0.3 from versions earlier than 6.3.0. You need to install FortiWeb-VM 8.0.3 instead of upgrading to 8.0.3. 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 8.0.3 from versions earlier than 6.3.0. You need to install FortiWeb-VM 8.0.3 instead of upgrading to 8.0.3. 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 8.0.3.
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`.

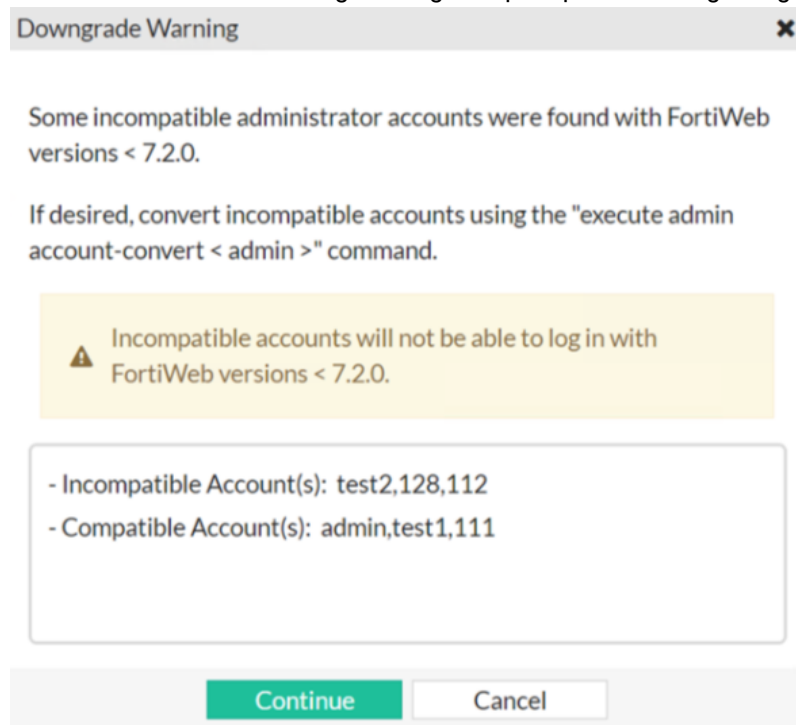
### Basic configuration preserved if downgrading to 5.1 or 5.0

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.

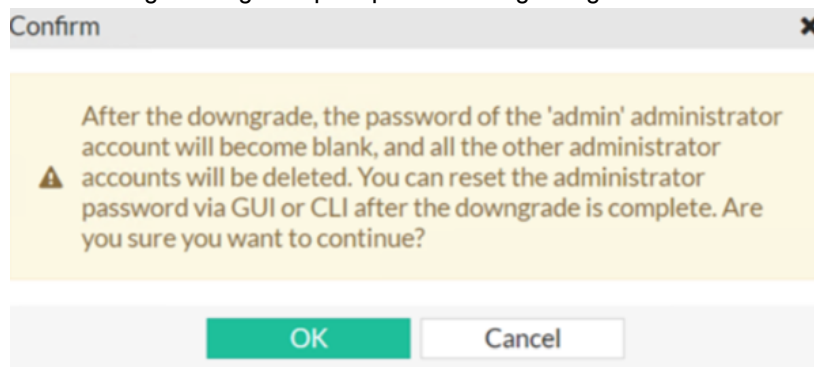
### Admin user password hash change

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 8.0.3. For inquiries about a particular bug, please contact Fortinet Customer Service & Support: <https://support.fortinet.com>

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                             |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1161319 | certd may stop checking for expiring certificates due to file descriptor leaks caused by unfreed BIO objects, leading to a silent failure until the process is restarted.                                                                                                                                                                               |
| 1165918 | Pasting multiple IP addresses into the Source filter field on the Attack Log page produced empty results. The filter logic did not correctly interpret pasted entries as separate values. A note has been added to the GUI log pages explaining how to manually use the <b>OR</b> operator when entering multiple filter conditions.                    |
| 1177864 | Traffic did not fail over when using scripting-based load balancing. When a server returned an HTTP 503 response, subsequent requests continued to be sent to the same server because Lua persistence entries could not be removed.                                                                                                                     |
| 1178228 | Changes to signature exceptions may not apply immediately under high traffic. The update takes effect only after a delay or after HA failover. The issue is caused by configuration writer starvation under the current locking mechanism.                                                                                                              |
| 1194449 | Customized column settings in the Attack Log page were not retained when viewing archived log files. Opening logs through Log Management caused the column configuration to revert to default.                                                                                                                                                          |
| 1197768 | FortiWeb generated incorrect event log entries for administrator login failures from untrusted hosts. When multiple administrator accounts were configured with trust host restrictions, the system logged failed login attempts under other valid usernames due to a loop error in the trust host verification logic.                                  |
| 1200770 | FortiWeb reset HTTP/2 requests when content routing was enabled. Under high HTTP/2 request rates, the Session Management module incorrectly counted individual requests as separate TCP connections, causing the request counter to accumulate and triggering period-block actions. This resulted in unexpected connection resets for all routed hosts. |
| 1207216 | When the HTTP Header Security (HHS) module was enabled with no rules configured, FortiWeb continued to buffer response data, which caused Server-Sent Events (SSE) responses to be dropped.                                                                                                                                                             |
| 1208900 | FortiWeb allowed the use of weak SSH MAC algorithms umac-128-etm@openssh.com and umac-128@openssh.com. These algorithms have been removed from the supported MAC list to ensure compliance with cryptographic security standards such as PCI DSS.                                                                                                       |

| Bug ID           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1209339          | FortiWeb failed to authenticate administrators using FortiCloud SSO on some appliances with identical firmware. The SAML login process stopped due to missing certificate handling, preventing completion of the FortiCloud SSO flow.                                                                                                                                                                                                                                                                    |
| 1212297          | FortiWeb blocked gRPC responses due to incorrect handling of HTTP/2 frame sequences. When a response included headers followed by trailers without an intervening data frame, FortiWeb generated an invalid 0-byte DATA frame with the EndStream flag set, causing the trailing header frame to be dropped and preventing the response from reaching the client.                                                                                                                                         |
| 1212635/ 1220457 | The proxyd process became unresponsive due to a client-management operation that performed slow Redis writes while holding a lock. This caused the proxy to hang, preventing traffic from being processed until the unit rebooted or failed over.                                                                                                                                                                                                                                                        |
| 1212693          | FortiWeb did not include the Host header when forwarding requests to an ICAP server, causing downstream ICAP systems to receive incomplete contextual information.                                                                                                                                                                                                                                                                                                                                       |
| 1214406          | FortiWeb returned intermittent HTTP 503 errors when processing multiple HTTP/1.1 requests over the same client connection. If consecutive requests matched different content-routing rules or backend pools, FortiWeb incorrectly reused the previous upstream connection instead of opening a new one, causing routing failures.                                                                                                                                                                        |
| 1215779          | OFTP log forwarding did not resume after the connection to FortiAnalyzer was disrupted. The OFTP client failed to re-establish the transport session following events such as a FortiAnalyzer reboot or HA role change, leaving the session in a persistent “not ready” state and causing logs to remain queued rather than forwarded.                                                                                                                                                                   |
| 1219535          | FortiWeb did not detect SQL injection payloads embedded inside nested JSON strings. When the SQL expression appeared within an escaped JSON value, the signature engine matched the payload but the False Positive Mitigation (FPM) stage incorrectly classified it as benign, resulting in the attack not being blocked.                                                                                                                                                                                |
| 1222647          | <p>When the <b>Login Disclaimer banner</b> is enabled, the GUI becomes inaccessible and returns an ERR_EMPTY_RESPONSE error. The issue occurs due to a null pointer condition during cookie handling in the login disclaimer process.</p> <p><b>Important:</b> FIPS users are advised <b>not to upgrade</b> to this release, as the login disclaimer cannot be disabled in FIPS mode. Upgrading under these conditions results in loss of GUI access, leaving only SSH and console access available.</p> |
| 1224444          | In some deployments using 10-Gbps i40e interfaces, a link-down event on one v-zone member did not propagate to the other port. Although FortiWeb reported the interface as down, the physical link remained active, preventing expected failover behavior. The issue was caused by the i40e driver not bringing down the PHY on interface close. The driver has been updated to ensure v-zone members drop link correctly when any member fails.                                                         |

| Bug ID          | Description                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1225626         | Remote administrator logins using RADIUS experienced GUI failures. In HA mode, the secondary unit rejected API calls because the access profile name was not passed correctly, causing the GUI to log out when loading HA Topology. An input-validation error also caused widget actions to fail.                                                                                                                |
| 1226243         | FortiWeb experienced high memory consumption due to a memory leak in proxyd. The module did not release svrnm_sess_hash and associated SNI domain data during SSL context cleanup, causing heap growth over time.                                                                                                                                                                                                |
| 1228155         | In certain cases, the Web Vulnerability Scan (WVS) runtime directory was initialized in an incorrect filesystem path (/var/log/lib/ rather than /var/log/wvs/). When this occurred, the WVS engine could not locate required working files, resulting in scan-startup failures, template-creation errors, and “Internal Server Error” responses when accessing Web <b>Vulnerability Scan &gt; Scan History</b> . |
| 1228318         | Report generation could stall at <b>1%</b> due to a crash in the reportd process when processing Attack Details data.                                                                                                                                                                                                                                                                                            |
| 1231821/1231926 | Intermittent server-to-server communication failures were caused by crashes in the proxyd process. The issue occurred when the Real Browser Enforcement (RBE) module accessed uninitialized or corrupted state from a previous transaction.                                                                                                                                                                      |
| 1233160         | After a reboot triggered by operations such as applying a new VM license, the admin account password could be reset to the default value, and in some cases remote administrator entries were removed. The issue was caused by the configuration save process incorrectly restoring the admin user during cmf_write_all_config.                                                                                  |

# Known issues

The following issues have been identified in version 8.0.3. To inquire about a particular bug or report a bug, please contact Fortinet Customer Service & Support: <https://support.fortinet.com>.

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1258393 | <p>The GeolP configuration is lost after upgrading to version 8.0.4. This occurs because version 8.0.3 fails to perform a mandatory automatic backup of the GeolP database during the upgrade process. Consequently, the missing database prevents the GeolP module from restoring its country-list settings in version 8.0.4, leading to parsing errors and empty policies.</p> <p><b>Workaround:</b> After the GeolP database is automatically recovered following the upgrade, you must restore the configuration from a backup file or manually reconfigure the GeolP policies.</p>                                                                                                                                                            |
| 1236503 | <p><b>FortiAI chat history export in PNG format may become unresponsive when handling large histories.</b></p> <p>With sufficiently large transcripts, exporting to PNG may cause the browser to freeze or display a long-running script warning.</p> <p>This issue affects <b>only</b> the PNG export function; all other FortiAI features operate normally.</p> <p><b>Recommendation:</b> For long chat histories, export the transcript in <b>HTML format</b>, which does not experience this performance issue.</p>                                                                                                                                                                                                                            |
| 1237118 | <p>When multiple administrators use FortiAI concurrently on the same FortiWeb appliance, FortiAI authentication tokens may intermittently become invalid.</p> <p>To improve service availability and distribute load, FortiAI login requests are load-balanced across multiple FortiAI service domains. However, in some concurrent multi-user scenarios, login requests may be routed to different FortiAI domains, which can overwrite the stored domain information on FortiWeb.</p> <p>As a result, previously issued tokens may no longer match the active FortiAI domain, causing subsequent FortiAI requests to fail.</p> <p>This issue occurs <b>sporadically</b> and <b>only in concurrent multi-user scenarios</b>.</p>                  |
| 1225818 | <p>CRL files cannot be restored using the <code>execute backup cert-config</code> and <code>execute restore cert-config</code> commands, and must be manually re-imported after restoring certificate configuration.</p> <p>Because large CRLs generate substantial encoded data during backup, including them can exceed CMDB capacity and lead to system instability. As a result, these commands intentionally back up and restore only certificate and key objects; the CRL store under <code>/var/log/crl/</code> remains empty after a restore. Deployments that rely on CRL-based revocation checking will not retain their CRL configuration and may experience incomplete certificate-validation behavior until CRLs are reinstalled.</p> |

| Bug ID  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1222520 | <p>When upgrading to FortiWeb 8.0.3 or 7.6.6, the system may display console messages such as:</p> <pre>Parsing error at 'ssl-custom-cipher'. err=1 Parsing error at 'tls13-custom-cipher'. err=1</pre> <p>These messages occur because 8.0.3 and 7.6.6 include changes that eliminate the need for <code>ssl-custom-cipher</code> and <code>tls13-custom-cipher</code> entries when standard cipher categories are used. Older configurations may still contain these settings, and the parser logs errors when rejecting them during the upgrade process.</p> <p>This behavior is cosmetic and does not affect SSL operation or any existing configuration. The issue appears only during this upgrade, and subsequent upgrades will not display these messages.</p> |
| 1224275 | <p>SAML signature-certificate updates require a second request to take effect. When a custom Service Provider (SP) certificate is updated in the SAML configuration, the new certificate does not take effect immediately. The first SAML request after the update may still be validated using the previous certificate, and the updated certificate is applied only on the subsequent request.</p> <p>This behavior occurs because the underlying SAML library does not reload signature-validation state instantly after configuration changes.</p> <p><b>SAML authentication functionality is not affected</b>; all authentication attempts succeed once the second request is sent.</p>                                                                           |



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

Copyright© 2026 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.