FortiWeb Release Notes

VERSION 7.0.4

FORTINET DOCUMENT LIBRARY
HTTPs://docs.fortinet.com

FORTINET VIDEO GUIDE
HTTPs://video.fortinet.com

FORTINET BLOG
HTTPs://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
HTTPs://support.fortinet.com

FORTINET COOKBOOK
HTTPs://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
HTTPs://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
HTTPs://training.fortinet.com

FORTIGUARD CENTER
HTTPs://fortiguard.com/

END USER LICENSE AGREEMENT
HTTPs://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

November 18, 2022
FortiWeb 7.0.4 Release Notes
1st Edition

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 7.0.4, build 0124.

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 FortiWeb Cloud 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

New features

FortiWeb 7.0.4 offers the following new features and enhancements.

100-continue headers

New CLI commands are added to control how FortiWeb interacts with clients and servers when forwarding the 100-continue headers.

```
config server-policy policy
   edit <policy-name>
      set reply-100-continue {enable | disable}
      set forward-expect-100-continue {enable | disable}
   next
end
```

Variables	Description
reply-100-continue {enable | disable}	• When disabled, the clients should wait for FortiWeb to forward the `100-continue` response sent by server. • When enabled, FortiWeb will not wait for the server's `100-continue` response. Instead it directly reply `100-continue` header to clients to reduce delay. **Note:** FortiWeb only supports HTTP/1.1, so the `100-continue` response sent by FortiWeb will be `HTTP/1.1 100-continue`.
forward-expect-100-continue {enable | disable}	• When disabled, FortiWeb will remove the `Expect: 100-continue` header from the request packets then forward them to servers. • When enabled, the `Expect: 100-continue` will be forwarded to server.

It's recommended to set `reply-100-continue` as `enabled` and `forward-expect-100-continue` as `disabled`, so that FortiWeb can directly reply `100-continue` header to reduce delay, then remove the `Expect: 100-continue` header from request packets to avoid unnecessary header being forwarded.

Enhancement on HA fail-over upon core dump

A new CLI command is introduced to trigger HA fail-over upon proxyd coredump, so that the secondary node can immediately take over the traffic when coredump file is being generated on the primary node.

```
config server-policy setting
   set enable-core-file enable
   set corefile-ha-failover enable
end
```

Please note you should enable `enable-core-file` as well for the `corefile-ha-failover` to work. From 7.0.4, `enable-core-file` is by default disabled.

Signature Algorithm setting for TLS1.2

When `tls12-compatible-sigalg` is enabled, signature algorithm negotiation in TLS handshake for FortiWeb behaves exactly the same as OpenSSL 1.1.0.

```
config server-policy setting
   set tls12-compatible-sigalg enable
end
```

Please note executing this command causes the proxyd to restart so all current sessions will be dropped.

This command is specific to very rare case. Do not use it unless suggested by Fortinet support team.

Product Integration and Support

Supported Hardware:

- FortiWeb 100D
- FortiWeb 400C
- FortiWeb 400D
- FortiWeb 400E
- FortiWeb 600D
- FortiWeb 600E
- FortiWeb 1000D
- FortiWeb 1000E
- FortiWeb 2000E
- FortiWeb 3000D/3000DFsx
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000D
- FortiWeb 4000E
- FortiWeb 100E
- 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
- 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)
- 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; Ubuntu18.04.1 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: 6.00137

Upgrade instructions

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

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**.

Upgrading from previous releases

- 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 anymore on FortiWeb-VMs deployed on public cloud platforms since 6.3.6. If you upgrade from versions earlier than that, these configurations will be removed.

We don't provide maintenance for 6.4.x releases unless major errors, so we don't recommend you to upgrade to 6.4.x. Please upgrade 6.4.x to 7.0.

In several hours or days (depends on number of existing logs) after upgrading from version earlier than 6.4.0 (5.x and 6.0.x-6.3.x) to 7.0, there might be delay (30-60 mins) to display new logs on GUI. This is caused by log version upgrade in 6.4.x & 7.0. It takes time to scan and process all existing logs.

To upgrade from FortiWeb 7.0.x

Upgrade directly.

To upgrade from FortiWeb 6.4.x

Upgrade directly.

To upgrade from FortiWeb 6.3.x

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

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 7.0.4 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.0.4 instead of upgrading to 7.0.4. 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

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 7.0.4 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.0.4 instead of upgrading to 7.0.4. 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

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 **System > 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

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

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

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.
   Note: If you forget to back up the configuration before you upgrade to FortiWeb 5.3, you can use the **Boot into alternate firmware** option to downgrade to the previous version, and then backup its configuration. For details, see the *FortiWeb Administration Guide*:
   HTTP://docs.fortinet.com/fortiweb/admin-guides
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 7.0.4.
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 15.

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 15.

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 Upgrading from previous releases on page 9.

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 16
   - To detach the log disk from a Microsoft Hyper-V VM on page 16
   - To detach the log disk from a KVM VM on page 16
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 16
   - To attach the log disk to a Microsoft Hyper-V VM on page 16

- To attach the log disk to a KVM VM on page 16

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

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.

Please note that 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.

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`.

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 7.0.4. For inquires about a particular bug, please contact Fortinet Customer Service & Support: HTTPs://support.fortinet.com

Bug ID	CVE reference
0860696	HTTP Parsing error occurs after rebooting proxyd or FortiWeb.
0858699	Let's Certificate status shows OK for non existing domain.
0856276	When core-file-count is 3, the newly generated coredump file will always be removed and cannot be displayed.
0856101	Proxyd dead loop with specific length (255 bytes) of content-type in HTTP response.
0851929	HA module needs to synchronize MAC address of all physical interfaces. Currently the maximum restrict is 20.
0850228	Frequent and fast certificate operations cause policy reload issue.
0848148	Slow traffic processing due to the web shell detection modules.
0847495	Memory leakage issue due to web socket traffic.
0847211	Admin certificate cannot work after upgrade to 7.0.2/7.0.3.
0846656	SNMP-inaccurate interface speed reported for 10G interface.
0846369	Traffic is blocked due to Occurrence filter setting 'within 1' in custom rule.
0846332	WAD site shows as disconnected and no files being backed up even though connection test shows successful.
0843673	Proxyd crashes under HTTP/2 stress with 1024 KB page size in TTP mode.
0845822	Specification issues about server pool.
0841704	Secondary unit is stuck in INIT state. The CRLF converting rules break the HA sync status.
0841686	The health status is Unavailable because we do not use the standard Azure Linux Agent.
0841635	Remove the filter pserver-ip in `diagnose debug flow` under non-RP platforms.
0840279	Parser using uninitialized data causes hdb_dump to crash.
0840259/0835458/0757998	There is a dead lock in client management process, which will trigger connection failure.
0839557	Expecting `100-Continue` header causes application delay for about 3 seconds with SOAP UI application when enabling XML Protection.

Bug ID	CVE reference
0837591	Enhancement on the signature filter in custom rule. When the main/sub class is enabled, members of the class should be enabled by default.
0837033	Spaces in passwords is not allowed via Console.
0832471	Memory optimization for Web Cache module.
0832165	Data filter does not work as expected. Excluded data still shows in the results.
0830863	White space in report data filter subtype is not allowed.
0818944	Caching inserts unwanted strings when response contains "Connection: close" and "Transfer-Encoding: chunked" header.
0818140	Memory usage issue in machine learning modules.
0816169	The 'Not' operator doesn't work as expected in the event log filters (add sql statement buffer and fix comma symbol issue).
0808401	Some logs are lost when they are forwarded to FortiAnalyzer.
0786883	There are duplicated logs if the traffic is GRPC or HTTP/2 in certain condition.
0690328	Add http-parse-max-size CLI setting to fix the "parameter too large" attack log issue.

Common Vulnerabilities and Exposures

For more information, visit HTTPs://www.fortiguard.com/psirt.

Bug ID	CVE reference
0858695	FortiWeb 7.0.4 is no longer vulnerable to the following CWE-Reference: CWE-79..

Known issues

This section lists known issues in version 7.0.4, but may not be a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support: HTTPs://support.fortinet.com

Bug ID	Description

0870313	Due to the file descriptor leak, new logs cannot be stored on FortiWeb and the SIEM server after the system running for about 15 days.
	FortiAnalyzer and **Syslog servers with TLS enabled** are not affected but make sure that they haven't been disconnected from FortiWeb, otherwise the same issue will occur.
	
	Workaround:
	Kill logd process every 15 days so that the file descriptor can be restarted then.
	1. Check the logd id. Run:
	`diagnose system top | grep logd`
	Here is an example of the output. The logd id is 23366.
	`23366 1 root S 243m 0.7 1 0.0 /bin/logd`
	2. Kill logd. Run:
	`diagnose system kill 9 <logd_id>`

0839559	Persistence works only for 30 seconds when traffic is routed through the Cloudflare DDOS solution.