# FortiWeb Release Notes

VERSION 7.0.2

**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

August 8, 2022
FortiWeb 7.0.2 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 7.0.2, build 0097.

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

FortiWeb 7.0.2 offers the following new features and enhancements.

**Zero Trust Network Access (ZTNA)**

Zero Trust Network Access (ZTNA) is an access control method that uses client device identification and Zero Trust tags to provide role-based application access for On-net local users and Off-net remote users. Access to applications is granted only after verifying the device and user identity, and then performing context-based posture checks using Zero Trust tags.

When a client connects to a virtual server, FortiWeb proxies the connection and takes steps to authenticate the user. It promotes the user for their certificate on the browser, and verifies this against the ZTNA endpoint record that is synchronized from the EMS. If this passes, traffic is allowed based on the ZTNA profile. If an site publish, such as SAML authentication, is configured in the web protection profile, the client is redirected to a captive portal for sign-on. It this also passes, FortiWeb returns the web page to the client.

**FortiClient EMS integration**

As part of the ZTNA process, FortiWeb supports integrating FortiClient EMS through Fabric Connectors. ZTNA endpoint records are synchronized from the FortiClient EMS to verify the user's certificate.

**Scripting language support**

FortiWeb now supports using Lua scripts to write simple, network aware pieces of code that will influence network traffic in a variety of ways. By using the scripts, you can customize FortiWeb's features by granularly controlling the traffic flow or even the contents of given sessions or packets.

**Machine learning changes**

- **Machine Learning > Anomaly Detection** is moved to **Web Protection > ML Based Anomaly Detection**.
- **Machine Learning > Bot Detection** is moved to **Bot Mitigation > ML Based Bot Detection**.
- **Machine Learning > API Protection** is moved to **API Protection > ML Based API Protection**.

**Machine learning based API Protection statistics**

FortiWeb now provides more statistics graphs on the domain level and endpoints level API Protection data.

**Domain usage statistics**

On **Status** page, a new widget is added to show the domain usage statistics for Machine Learning Based API Protection and Anomaly Detection.

**X-Forwarded-For header full scan**

It's now supported to scan all the IP addresses listed in the X-Forwarded-For header against IP reputation. Turn on **Block Using Full Scan** in **Serve Objects > X-Forwarded-For**.

**Credential Stuffing local check**

In addition to checking the availability of the Credential Stuffing online database, it's now also supported to test the Credential Stuffing local database.

**Sensitivity level for signatures**

Signatures now include Sensitivity Levels. You can choose from four categories of attack signatures (L1 to L4) based on their sensitivity to false positives and their requirement for a higher security level. Every level adds additional signatures thus increasing security but also the possibility of blocking legitimate traffic.

**Set-Cookie attributes decoding**

It's now supported to retrieve the set-cookie's attributes such as httponly, secure, and samesite.

**HTTP method and protocol check**

In URL Access Rule, you can now specify the HTTP methods and protocols to check, so that only the matched requests will be passed for further scan.

**Port and sub-domain match in hostnames**

FortiWeb now supports protecting hostnames with ports or sub-domains. Enable **Ignore Port** or **Include Sub-domain** in **Server Objects > Protected Hostnames**

**File security enhancements**

- You can now clear the cache of the scan results from ICAP Server.
- In addition to the pre-defined file types, you can now specify custom file types.

**Policy based allow list**

Instead of global allow list, you can now apply allow list at the policy level.

**Chunk encoding**

You can enable `chunk-encoding` in `config server-policy policy` to encode the response packets.

**More flexible x509-certificate-subject match in content routing**

Content Routing now supports matching against x509-certificate-Subject by the following options: Match prefix, Match suffix, Match contains, Is equal to and Regular Expression.

**Allowing editing HTTP content routing in Server policy**

It's now allowed to edit the settings of an existing HTTP content routing policy while creating a server policy.

**Cryptographic key**

To ensure higher level of security, a random application key is generated when the system first starts up. Each appliance has a different key. Security modules such as Cookie Security, MITB, and Site Publish use this key for encryption and decryption. If multiple FortiWeb appliances are deployed behind a load balancer, do make sure to manually synchronize the key so that the appliances in a load balance cluster use the same key.

To manually synchronize the key, you need to first enable **Cryptographic key Backup/Restore** in **System > Config > Visibility**, then import or export the key in **System > Maintenance > Backup & Restore**.

**SSL ciphers enhancements**

- You can now group SSL ciphers and reference the group in server policy and server pool settings.
- Most ciphers in Advanced SSL Settings are supported when HTTP/2 is enabled.

**SAML authentication enhancement**

The CPU consumption is improved when the system runs SAML authentication.

**Intermediate CA authentication**

FortiWeb now supports partial certificate chain validation. External clients can be validated by the Intermediate CA only.

**LetsEncrypt Certificate enhancements**

- It's now supported to set the renew interval of the LetsEncrypt Certificate.
- Multiple FQDNs are now supported in a single LetsEncrypt Certificate.

**Support password change for RADIUS server user authentication**

FortiWeb now supports the users authenticated by RADIUS server to change their passwords.

**FortiAuthenticator authorization**

FortiWeb now supports FortiAuthenticator authorization, which allows users to access your application through logging in with FortiAuthenticator.

**More than one ADOMs for an administrator**

One administrator can now manage multiple ADOMs.

**Database version in event log**

When signature database is upgraded, the database version can now be recorded in the event log.

**XML validation attack logs enhancement**

The XML validation attack logs are now enhanced to provide detailed information on why the validation fails.

**OWASP API Top10 attack log field**

FortiWeb now records the OWASP API Top10 attack categories in attack logs, and you can now filter the attack logs by OWASP API Top10. It's also supported to turn on or off the OWASP API Top10 attack fields by running `set owasp_api_top10_log_field {enable/disable}` in `config waf web-protection-profile inline-protection`.

**Historical update information added in `diagnose system update`**

The date and time of the historical updates can be printed out in `diagnose system update`.

**The comlog command support**

FortiWeb now supports `comlog` command: `diagnose debug comlog {info|read|clear|disable|enable}`

**Health probe port in Azure Load balancer deployment**

When FortiWeb-VMs are deployed behind an Azure Load Balancer, you can configure a dedicated port to reply the Health Probe reponse.

**Certificate maximum increased on VM16, 4000E, and 4000F**

For VM16 platform, the limits of the local, multi-certificate, inline SNI, CA, intermediate CA, CRL, and certificate will be raised to 5000.

For 4000E, 4000F, and VM16 platforms, the limit of the sub-table in Inline SNI will be raised to 2048.

**Full configuration sync via HA on Google Cloud**

FortiWeb-VMs deployed on Google Cloud now supports full configuration synchronization via HA clusters.

**Cloud-int support on Google Cloud**

Cloud-init can now be used on FortiWeb-VM on Google Cloud. It supports specifying CLI commands to be automatically run when the VM is deployed.

**Unicast HA heartbeat on VMWare**

FortiWeb-VM on VMware now supports Unicast HA heartbeat in Active-Passive HA mode.

# 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 6.4.0**

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 7.0.2 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.0.2 instead of upgrading to 7.0.2. 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 7.0.2 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.0.2 instead of upgrading to 7.0.2. 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 7.0.2.
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 16.

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 16.

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 10.

## 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 17
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 17
   - To attach the log disk to a Microsoft Hyper-V VM on page 17
   - To attach the log disk to a KVM VM on page 17
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 7.0.2. For inquires about a particular bug, please contact Fortinet Customer Service & Support: https://support.fortinet.com

| Bug ID | Description |
|---|---|
| 0830836 | Slave unit is stuck in INIT state due to some configuration not synchronized correctly. |
| 0830054 | HTTP/2 traffic can't be forwarded correctly when there is only Header Frame and no content-length in response. |
| 0829276 | WSDL import error when the target Namespace in WSDL is empty. |
| 0828444 | SNMP doesn't work for virtual interface. |
| 0827615 | CPU usage is high due to the frequent malloc/release of large memory on sql/ast feature. |
| 0825989 | Sometimes proxy can't get the actual domain pserver in server pool randomly. |
| 0825385 | HTTP/2 file download freezes. |
| 0825062 | FortiWeb should support getting local certificate by certificate name RestfulAPI. |
| 0823179 | Performance issue on 4000E - "`nf_conntrack: nf_conntrack: table full, dropping packet`". |
| 0822216 | Report time period does not match with the content. |
| 0820554 | Due to chunk-decode mechanism, it can't deal with traffic when the response is text/event-stream. |
| 0817883 | Attack log view in GUI for certain signature descriptions doesn't properly wrap. |
| 0815601 | FortiWeb recognizes the XML keyword in boundary as XML type of access. |
| 0815561 | There are memory leakage about API protection. |
| 0815515 | REST API handler for JSON local cert and intermediate CA lacks the validation process. |
| 0814486 | The kernel crashes when receiving ICMP message. Destination Unreachable and the message is delivered to SNMPD specifically. |
| 0812111 | The system allows users to successfully authenticate via SSH -CLI without FortiToken code appended to password. |
| 0812016 | SNMP fails when users modify SNMPv3 configuration due to wrong password sent. |
| 0811484 | Saved Filter on Log can't be applied when the filter is large. |
| 0811361 | The system does not check whether the matching parameter is in Global White |

| Bug ID | Description |
|---|---|
| | List or not while performing PCRE searching. |
| 0808469 | Power supply flaps on 3000F/4000F. |
| 0808104 | Should enhance the signature attack log about JSON parameter. |
| 0807074 | The `mkey` value with blank space passes to the slider dialog gets truncated on GUI. |
| 0806891 | The WCCP communications are not working in certain topology. |
| 0806587 | There are some loopback addresses as the source IPs in attack logs. |
| 0805497 | In offline mode, the packet log is confused due to HTTP parse error about pipeline scenario. |
| 0805339 | For Basic delegation, the system converts default domain prefix to uppercase which leads to a server error. |
| 0805169 | Web Cache is stuck in clearing state in certain cases. |
| 0803819 | Certain traffic triggers API Protection machine learning model to turn into building status. |
| 0803058/0788784 | The TLS1.1 SSL protocol is dropped on config Synchronization. |
| 0802044 | The proxy crashes related with API Protection. |
| 0801828 | Cookie exception does not work as expected. The customer wishes to add exemption for wildcard cookies. |
| 0801023 | Threshold Based Detection doesn't detect a plain text slow HTTP attack when the traffic triggers the redirection action. |
| 0801014 | Scan report has multiple weakness and potential VULN on GUI. |
| 0800993 | Configuration changes about custom policy triggers secondary node's daemon to restart and business is interrupted in HA A-A mode. |
| 0800758 | Cross-month log download is abnormal. |
| 0797298 | The system can’t deal with HTTP2_PING Frame correctly. |
| 0796213 | Receiving SNMP queries on VIP where SNMP is not configured. |
| 0768217 | The `/var/run/shibd.pid` takes up too many CPU resources. |
| 0765492 | FortiWeb needs to support cookiesession1 based on session. |
| 0759826 | SAML SSO for GUI Administrators is only possible when using FortiGate as IDP via Fabric Connector. |
| 0757485 | Let's Encrypt should support longer domain name. |
| 0684352 | Report generating is stuck when the report has a large amount of data. |

**Common Vulnerabilities and Exposures**

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

| Bug ID | CVE reference |
|---|---|
| 0816382/0815262/0810117 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-121. |
| 0815273/0814407/0804896 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-78. |
| 0810982 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-476. |
| 0807681/0806117 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-23. |
| 0806541 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-23. |
| 0806493 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-89. |
| 0758336 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-804. |
| 0755600 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-321. |
| 0754252 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-329. |
| 0603276 | FortiWeb 7.0.2 is no longer vulnerable to the following CWE-Reference: CWE-79. |

# Known issues

This section lists known issues in version 7.0.2, 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 |
|---|---|
| 0830863 | White space in report data filter subtype is not allowed |
| 0822918 | The Chrome HTTP2 traffic Oauth authentication fails sometimes. |
| 0808401 | FortiWeb forwards logs to FortiAnalyzer mismatched. |
| 0802523 | The X509 Certificate Subject verifies only a partial string (from the beginning) in HTTP Content Routing policy. |
| 0785916 | Link Chocking: the website load will have some delay due to design mechanism. |
| 0785909 | Link Clocking: the js cannot execute when the website have Content-Security-Policy restriction. |
| 0765262 | The system doesn't update when the Health Check DNS server is updated. |