FORTINET

Release Notes

FortiWeb 7.2.1

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

March 03, 2023
FortiWeb 7.2.1 Release Notes
1st Edition

TABLE OF CONTENTS

Introduction **4**
What's new **5**
Product Integration and Support **8**
Upgrade instructions **10**
Image checksums 10
Upgrading from previous releases 10
Repartitioning the hard disk 16
To use the special firmware image to repartition the operating system's disk 16
To repartition the operating system's disk without the special firmware image 17
Upgrading an HA cluster 18
Downgrading to a previous release 18
FortiWeb-VM license validation after upgrade from pre-5.4 version 20
Resolved issues **21**
Known issues **23**

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 7.2.1, build 0330.

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 7.2.1 offers the following new features and enhancements.

Custom rule enhancements

- HTTP Methods scan is moved out of the HTTP headers filter to stand out as a separate filter. More HTTP method types are supported including WEBDAV,RPC, and OTHERS.
- To target the inspection point more accurately in parameter filter, it's now supported to scan the parameters located only in URL or the HTTP body.

Reverse DNS lookup timeout setting in URL Access rules

To avoid the process hanging for a long time, you can now set a timeout value to limit the reverse DNS lookup time in URL Access rule.

IP groups

You can now create IP groups in **Server Objects > IP Groups** then reference them in modules where it requires to specify IP addresses or IP ranges. IP Groups is supported in **IP Protection > IP List** and will be introduced in other modules in future releases.

LUA script update

A new predefined Lua script "SSL_COMMANDS" is added. The newly supported SSL commands can be used to retrieve information about the SSL handshake such as SNI status, the SSL ciphers, certificate verification status, etc.

For more information, see "SSL commands" in Script Reference.

JSON Protection enhancements

- You can now choose the JSON schema version for the system to check if the uploaded JSON schema file is valid against the specified version.
- Multiple JSON schemas can now be added in one group and be referenced in JSON Protection rules.

Support defining "format" for "string" type in OpenAPI file

In OpenAPI file, for the optional modifier property "format" of the "string" type, you can define it as "email" (rfc5322) or "uuid" (rfc4122).

For example:

```
id:
   type: string
   format: uuid
work-email:
   type: string
   format: email
```

We accept "email", "Email", and "EMAIL"; "uuid" and "UUID". They are case sensitive, so do not use strings other than them. For example, UuID is not accepted.

HTTP header insertion in URL rewrite rule

It's now supported to insert more than one HTTP headers when rewriting an URL. Configure it in **Application Delivery > URL Rewriting**.

Host and peer verification in Fetch URL & Quarantine IP

Fetch URL & Quarantine IP can now establish HTTPS connection with FortiGuard or back-end servers and verify the SSL certificates. Configure in **System > Config > FortiGate Integration** and **Web Protection > Input Validation > Hidden Fields**.

Validating server certificate when connecting with FortiClient EMS

You can now configure FortiWeb to validate the server certificate when connecting with FortiClient EMS. Enable **Server Certificate** for the FortiClient EMS fabric connector (**System > Fabric Connector**).

OAuth Authorization enhancement

It's now supported to use an SSL certificate to check the TLS traffic between FortiWeb and the third party OAuth authentication servers.

Least response time load balancing algorithm

The back-end server load balancing algorithm now supports **Least Response Time** and **Probabilistic Weighted Least Response Time**. It can distribute the incoming traffic to the server with the shortest average response time and the lowest number of connections, thus making the client connect to the most efficient back-end server.

Request redirection

- Requests with a naked domain can now be redirected to “www” domain.
- The status code for redirecting HTTP to HTTPS is changed from 301 to 302.

Health check result synchronization

In certain case when different server pools sharing the same IP address it's unnecessary to perform health check to all the server pools. Use the following command to share the health check result across multiple server pools.

```
config server-policy health
   edit "<health-check_name>"
      set group-id <int>
      set role {master | slave}
   next
end
```

With this command, you can create several health checks with the same group-id, assigning master role to one of them while the slave role to the rest. Health check result is automatically pushed from the master to the slave.

Shell access enhancements

- It's now supported to view the history of commands executed in Shell. Run `diagnose debug shell-access history show`.
- To ensure the security of Shell access, you can now restrict the access only from trusted hosts.

  Run the following commands to set the history size and specify trusted hosts.

  ```
  config system global
     set shell-access enable
     set shell-history-size <int>
     set shell-trusthostv4 <IPv4_address_range>
     set shell-trusthostv6 <IPv6_address_range>
  end
  ```

Replacement Message enhancement

`%%USERNAME%%` and `%%RAWNAME%%` are introduced in the **Replacement Message** so that you can configure FortiWeb to display different format of usernames such as "username@abc.com" or "username".

RFC-9719 Comply

RFC-9719 TLS security can now be applied to both inbound or outbound HTTPS connections with FortiWeb. Configure in **Server Pool** and **Server Policy.**

Up to 4096 bits key size supported for Let's Encrypt certificates

RSA algorithm with different key length can be implemented and accepted by the Let’s Encrypt Server. Those key sizes are 2048, 3072, and 4096 bits. Please note that larger keys consume more computing resources, however, achieve better security.

Support forwarding logs to ELK

Attack and traffic packet logs can now be sent to syslog servers in JSON format through TCP or TLS protocol. Configure it in **Log&Report > Log Policy > Syslog Policy**.

RBE attack log enhancement

The HTTP host and URL are now revealed in the RBE (including RBE, CAPTCHA, and reCAPTCHA) attack logs to better help with troubleshooting.

Support updating the URL of Google reCAPTCHA service

It's now supported to edit the URL of Google reCAPTCHA service so that you can update it in time when Google changes it.

Restrict ADOM admin permissions to VIPs

Global administrators can create, edit, and delete VIPs, while ADOM administrators can now only view the VIPs assigned to their ADOM.

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 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
- 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

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**.

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 recommend you to upgrade 6.4.x to later versions.

In several hours or days (depends on number of existing logs) after upgrading from versions earlier than 6.4.0 (5.x and 6.0.x-6.3.x), 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.

The admin user password hash is changed from sha1 to sha256 since 7.2.0.

If you upgrade FortiWeb from versions earlier than 7.2.0, the hash will keep the same as before, but if admin user changes its password or there is new admin users added, the password hash will be sha256.

Port 995 will be switched to disabled state if you upgrade from versions earlier than 7.2.0. Remember to enable it (in **System > Admin > Settings**) if you need to use it for config sync.

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 7.2.1 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.2.1 instead of upgrading to 7.2.1. 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 7.2.1 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.2.1 instead of upgrading to 7.2.1. 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 **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 7.2.1.
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 17.

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 17
   - To detach the log disk from a Microsoft Hyper-V VM on page 17
   - 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 18
   - To attach the log disk to a KVM VM on page 18
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

ML based modules data loss

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

Log compatibility issue

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

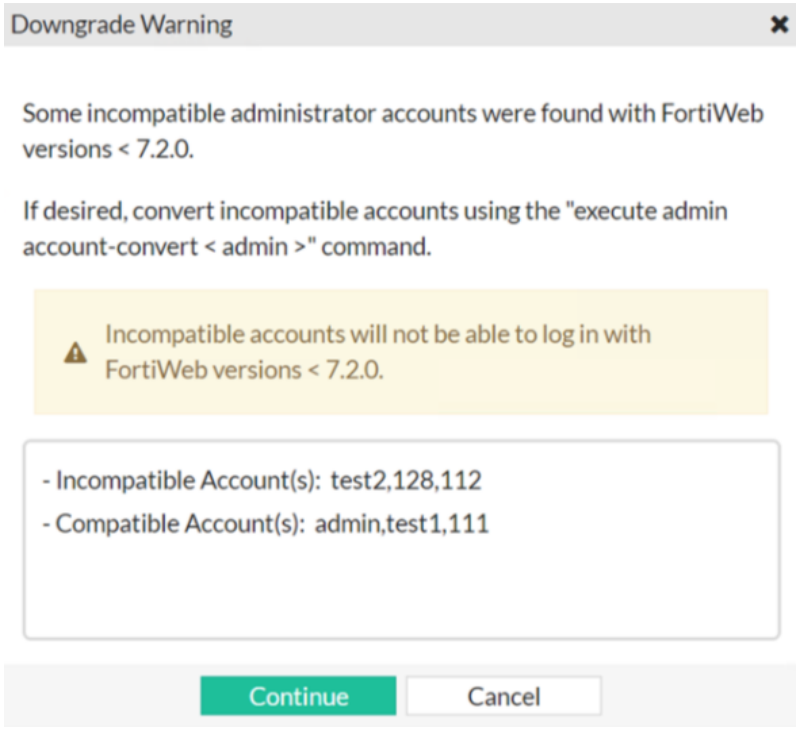
Basic configuration preserved if downgrading to 5.1 or 5.0

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

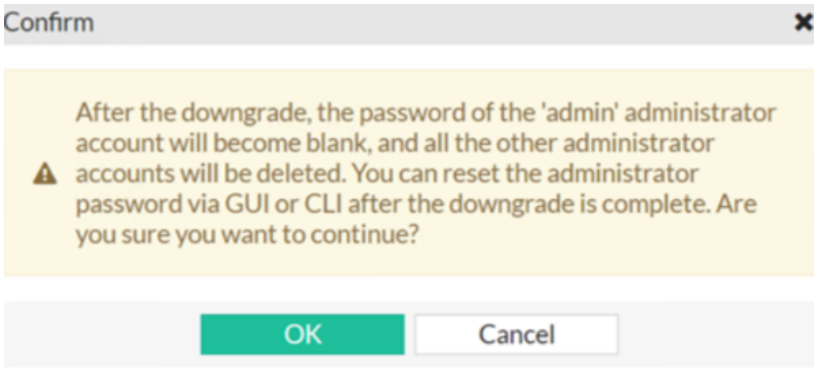
Admin user password hash change

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

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



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



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

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

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

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

Resolved issues

This section lists issues that have been fixed in version 7.2.1. For inquires about a particular bug, please contact Fortinet Customer Service & Support: HTTPs://support.fortinet.com

Bug ID	Description
0889174	Non-standard location in XML WSDL file causes High CPU issue.
0885080	FortiWeb cannot connect with FortiWeb Cloud on Hardware platforms for Threat Analytics.
0880314	The interface name contains illegal characters, which causes the interface name modification to fail, and the previously created VLAN interface is not deleted successfully.
0872030	Should implement debug enhancement to avoid traffic outage.
0868363	The SCEP type in CRL cannot work properly.
0867454	If there are multiple wildcard admins and the first one can’t match ldap, accessing the RESTful API will get 401 unauthorized error.
0834665	When there is a delay between sending the request header and body, the raw body cannot be displayed in the package log.
0886420/0883069/ 0883889/0880771/ 0883446	Proxyd crashes when there are multiple GEO IP Exception Rules.
0886039	proxyd crashes when processing early data traffic.
0883939	Wrong memory calculation method results in a problem with the number of VDOMs.
0883734/0871074	License are not valid when upgrading to 7.2.0 due to anycast FDN server connection is not stable.
0881709	In Transparent Inspection mode, attacks are detected but not blocked (no RST sent).
0876993	When the length of the request and response is greater than 1024 and the response is chunked and gzipped, the page cannot be loaded correctly.
0875424	The process confd_sync leads to high memory usage.
0871054	There is a semaphore leak in httpsd. FortiWeb's GUI can't be accessed when httpsd daemon has restarted several times.
0870313	FortiWeb does not show new logs on GUI until the process logd is killed.
0865939	FortiView Server Policies page does not show destination sessions.
0853027	If there are spaces before the Content-Disposition field, the attack detection about

Bug ID	Description
	Apache Struts2 S2-046 can be bypassed.
0846605	ADOM-Admin can see/edit other ADOMS VIPs.
0830926	OpenAPI schema cannot detect format UUID and email type.
0880088	When a wildcard user log in to FortiWeb then access the page “HA Topology”, it causes the user's session to be logged out.
0871156	Microsoft Software Installer(.msi) can’t be recognized in File Security.
0869393	In Signature Management page, the signature description is cut off in Firefox.
0868779	Under certain conditions, FortiWeb treats the internal JS request as an ordinary traffic, resulting in CSRF not working properly.
0843810	Client "End to End Timing" displays incorrect RTT value under **Dashboard > Policy Status**.

Common Vulnerabilities and Exposures

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

Bug ID	CVE reference
0858695	FortiWeb 7.2.1 is no longer vulnerable to the following CWE-Reference: CWE-79.
0745694	FortiWeb 7.2.1 is no longer vulnerable to the following CWE-Reference: CWE-329.

Known issues

The following issues have been identified in version 7.2.1. To inquire about a particular bug or report a bug, please contact Fortinet Customer Service & Support: HTTPs://support.fortinet.com

Bug ID	Description
0839559	Persistence works only for 30 seconds when traffic is routed through the CloudFlare DDOS solution.
0858695	FortiWeb is vulnerable to Cross-site Scripting (XSS) attack due to an improper neutralization of input during the HTML report generation.

www.fortinet.com