

Release Notes

FortiWeb 7.2.2



FORTINET DOCUMENT LIBRARY

[HTTPs://docs.fortinet.com](https://docs.fortinet.com)

FORTINET VIDEO GUIDE

[HTTPs://video.fortinet.com](https://video.fortinet.com)

FORTINET BLOG

[HTTPs://blog.fortinet.com](https://blog.fortinet.com)

CUSTOMER SERVICE & SUPPORT

[HTTPs://support.fortinet.com](https://support.fortinet.com)

FORTINET COOKBOOK

[HTTPs://cookbook.fortinet.com](https://cookbook.fortinet.com)

FORTINET TRAINING & CERTIFICATION PROGRAM

[HTTPs://www.fortinet.com/support-and-training/training.html](https://www.fortinet.com/support-and-training/training.html)

NSE INSTITUTE

[HTTPs://training.fortinet.com](https://training.fortinet.com)

FORTIGUARD CENTER

[HTTPs://fortiguard.com/](https://fortiguard.com/)

END USER LICENSE AGREEMENT

[HTTPs://www.fortinet.com/doc/legal/EULA.pdf](https://www.fortinet.com/doc/legal/EULA.pdf)

FEEDBACK

Email: techdocs@fortinet.com

April 21, 2023

FortiWeb 7.2.2 Release Notes

1st Edition

TABLE OF CONTENTS

Introduction	4
What's new	5
Product Integration and Support	6
Upgrade instructions	8
Image checksums	8
Upgrading from previous releases	8
Repartitioning the hard disk	14
To use the special firmware image to repartition the operating system's disk	14
To repartition the operating system's disk without the special firmware image	15
Upgrading an HA cluster	16
Downgrading to a previous release	16
FortiWeb-VM license validation after upgrade from pre-5.4 version	18
Resolved issues	19
Known issues	21

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 7.2.2, build 0344.

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/](http://docs.fortinet.com/fortiweb/)

What's new

FortiWeb 7.2.2 offers the following new features and enhancements.

Threat Analytics 14-day eval license

A new 14-day eval license is now available for customers that want to try out the powerful AI-based Threat Analytics service that helps identify significant threats and helps you zoom in on the threats that matter. Eval license can be enabled directly from the UI.

For more information, see [Analyzing attack logs in FortiWeb Cloud Threat Analytics](#).

Firewall Admin policy

Firewall Admin policy is introduced in **System > Firewall**. It has the ability to granularly restrict the admin access to FortiWeb by combining multiple matching conditions, e.g. the source and destination addresses of the traffic, the ingress interface, and services.

For more information, see [Configuring the integrated firewall](#).

IP Group – uploading an IP List in batch

In **IP Group**, instead of configuring IPs one by one, you can now upload a CSV file with a list of IPs instead.

For more information, see [Creating IP groups](#).

IP group in IP reputation

It is now possible to reference an IP group when configuring the exception list in **IP reputation**.

Site publish rule configuration maximum increased

The maximum number of site publish rules has been increased from 216 to 512.

TLS settings for ADFS proxy server pool

When FortiWeb is deployed as an ADFS proxy, it is now possible to configure the SSL protocols and SSL/TLS encryption level of the server pool.

FortiWeb HA on AliCloud

FortiWeb-VM instances can now be deployed in active-passive HA and high volume active-active HA modes on AliCloud.

FortiWeb-VM on AWS support IMDSv2

From 7.2.2, FortiWeb-VM on AWS supports Instance Metadata Service Version 2. If you use the cloud-init feature to upload license or run CLI commands while deploying the image, it's recommended to enable IMDSv2 on AWS to ensure better security. See [this article](#) for how to enable IMDSv2.

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; Ubuntu 18.04.1 LTS or higher versions
- Nutanix AHV

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

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

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- Google Cloud

- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud

Supported web browsers:

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

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

Build-in AV engine version: 6.00283

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](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 7.2.x

Upgrade directly.



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

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

To upgrade from FortiWeb 7.0.x

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 7.2.2 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.2.2 instead of upgrading to 7.2.2. 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 7.2.2 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.2.2 instead of upgrading to 7.2.2. 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 **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](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](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 7.2.2.
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 14](#).

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](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](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 8](#).

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](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 15](#)
 - [To detach the log disk from a Microsoft Hyper-V VM on page 15](#)
 - [To detach the log disk from a KVM VM on page 15](#)
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

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`.

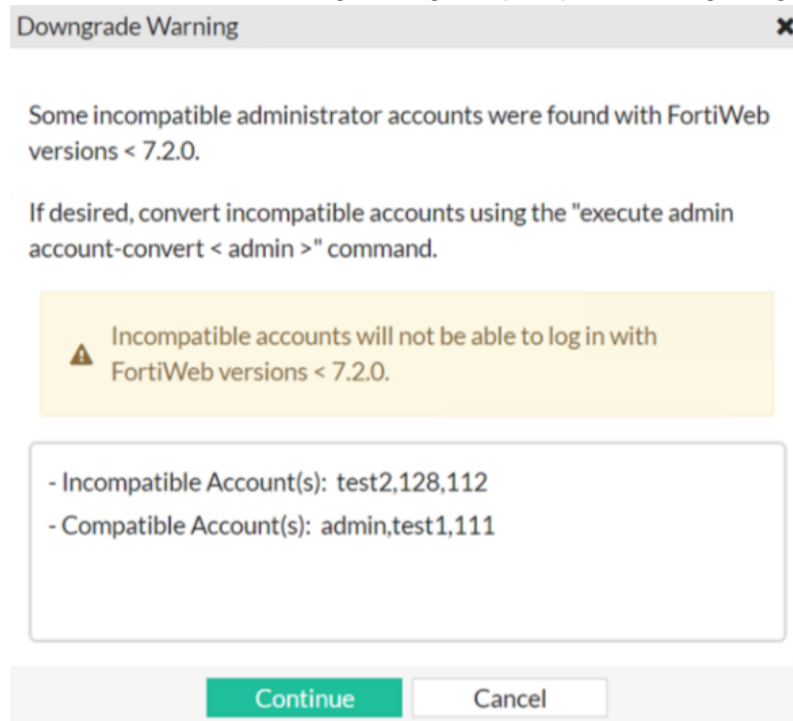
Basic configuration preserved if downgrading to 5.1 or 5.0

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.

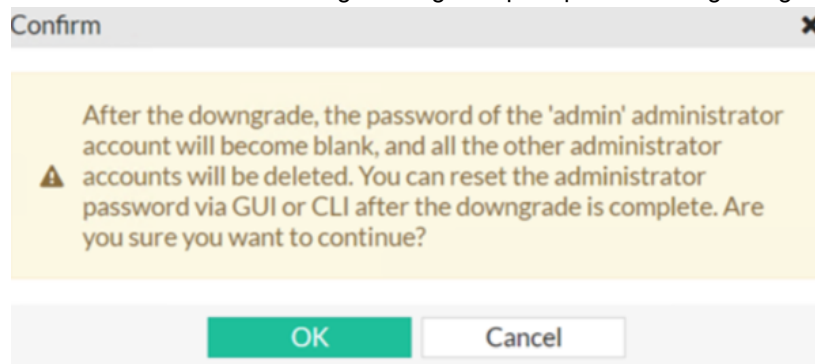
Admin user password hash change

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 7.2.2. For inquiries about a particular bug, please contact Fortinet Customer Service & Support: [HTTPS://support.fortinet.com](https://support.fortinet.com)

Bug ID	Description
0892273/0900578	Traffic with an empty Host will trigger proxyd crash when Redirect HTTP to HTTPS option is enabled in the policy.
0890481/0893552	Error message should be added for API error code.
0902652	Fix console error message: 'fopen(): No such file or directory.
0901243	When ADOM is enabled, sometimes VIPs cannot be created successfully.
0898442	Sometimes HTTP parses critical errors that will trigger traffic-stuck issues.
0897933	The sensitive info is masked in the Packet Header and not in the Detailed Information .
0894536	Config sync is using the weak Ciphers for the TLS key exchange. Should upgrade the TLS protocol to TLS1.3.
0894535	If a response contains multiple Content-Length headers, it may cause errors in the application. The system should handle all Content-Length headers appropriately to avoid issues.
0893896	Need extra permission to view Server Policy configurations on FWB GUI.
0892717	XML protection blocks the SOAP request with a PDF attachment file (MTOM enabled) sized smaller than 500 KB.
0892663	SSH management access host key algorithm does not support 'ssh-rsa'.
0892348	FortiGate Integration can't work properly.
0891711	Add support for '.tsv' file type in FileUpload.
0887066	MITB breaks authentication when the parameter is in the URL location.
0885834	Traffic logs generated by FortiWeb and forwarded to FortiAnalyzer receive a time stamp that is at least 10 seconds apart from the real one.
0885619	There is one zombie mysqld_monitor process.
0883806	There is a deadlock issue on url_record_db_drop.
0881517	Attack log filters don't work correctly.
0880828	Firewall Policy's default action affects the management connection.
0874348	ADFS Policy should also support TLS protocol version chosen.
0874077	FIPS encode/decode fails, which will lead to the HA pair not syncing, and it will be in an INIT state.

Bug ID	Description
0873792	Zscaler IP address has been wrongly classified as a bad reputation IP and has been blocked.
0832949	FortiWeb can't register with ADFS farm.

Common Vulnerabilities and Exposures

For more information, visit [HTTPS://www.fortiguard.com/psirt](https://www.fortiguard.com/psirt).

Bug ID	CVE reference
0880224	FortiWeb 7.2.2 is no longer vulnerable to the following CVE: CVE-2023-25610

Known issues

The following issues have been identified in version 7.2.2. To inquire about a particular bug or report a bug, please contact Fortinet Customer Service & Support: [HTTPS://support.fortinet.com](https://support.fortinet.com)

Bug ID	Description
0906184	The SNMP service condition configured in Firewall Admin policies doesn't take effect. Workaround: The rule for SNMP service can be added in Firewall Policy to control the SNMP traffic.
0903772	SNMP does not work on FortiWeb-VM deployed on docker.
0901939	Missing country "Heard Island And McDonald Islands" in GEO list.
0900520	When importing IP Group list with a large amount of IP addresses or ranges, CPU usage unexpectedly keeps high for a while.
0897057	When an IP group with maximum configurations is loaded in IP List or IP Reputation, 4G memory VM is not recommended.
0896613	Importing a large IP group list will trigger an unexpected event log.
0839559	Persistence works only for 30 seconds when traffic is routed through the Cloudflare DDOS solution.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.