FORTINET

High Performance Network Security

WEB APPLICATION FIREWALL

FortiWeb Release Notes

VERSION 5.7.3

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 3, 2020

FortiWeb 5.7.3 Release Notes

1st Edition

Change log

June 3, 2020	Initial release.

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 5.7.3, build 1126.

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 from:

- Sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, and cookie poisoning
- Malicious sources
- DoS attacks

For additional documentation, please visit the FortiWeb documentation:

http://docs.fortinet.com/fortiweb/

What’s new

FortiWeb 5.7.3 is a patch release, and no new features and enhancements are covered in this release.

Upgrade instructions

Hardware & VM support

FortiWeb 5.7.3 supports:

- FortiWeb 100D
- FortiWeb 400C
- FortiWeb 400D
- FortiWeb 600D
- FortiWeb 1000C
- FortiWeb 1000D
- FortiWeb 2000E
- FortiWeb 3000C/3000CFsx
- FortiWeb 3000D/3000DFsx
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000C
- FortiWeb 4000D
- FortiWeb 4000E
- FortiWeb-VM

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 install a special firmware image to repartition the disk. See "To use the special firmware image to repartition the operating system's disk " on page 8.

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 8.

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. Go to the Fortinet Customer Service & Support website to download the special repartitioning firmware image from the FTP site:

   https://support.fortinet.com/

   Ensure that you download the correct image for your FortiWeb platform.

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.

4. 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 9
   - "To detach the log disk from a Microsoft Hyper-V VM" on page 9
   - "To detach the log disk from a KVM VM" on page 9

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 9
- "To attach the log disk to a Microsoft Hyper-V VM" on page 9
- "To attach the log disk to a KVM VM" on page 10

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.

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. (The 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

- To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb hard disk partitions. See "Repartitioning the hard disk" on page 7.

- 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.
- 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.
- 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.

Note: To upgrade from 4.0 MR4, Patch x or earlier, please contact Fortinet Technical Support.

To upgrade from FortiWeb 5.5.x

Upgrade to FortiWeb 5.7.3 directly.

To upgrade from FortiWeb 5.4.x or FortiWeb 5.3.x

Upgrade to FortiWeb 5.7.3 directly after completing the hard disk repartitioning process.

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" on page 12.

To upgrade from a version previous to FortiWeb 5.3

FWB5.3.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, `FWB5.3Upgrade_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 `FWB5.3Upgrade.exe` and your backup configuration file are located, execute the following command:

```
FWB5.3Upgrade.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" on page 7.
8. Upgrade to FortiWeb 5.7.3.
9. Use **System > Maintenance > Backup & Restore** to restore the configuration file you created using the script (for example, `5.3_new.conf`).

   If you upgrade from a previous version of FortiWeb 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.

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 your FortiWeb 5.7.3 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.

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

The following issues have been fixed in version 5.7.3. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
636994	The certificate in the image file is expired, preventing FortiWeb from connecting with FDS servers to validate its license.

Known issues

This section lists the known issues of this release, 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
412449	Admin login attempts may prompt for admin authentication credentials from untrusted hosts even when all admin accounts have trusted hosts configured.
445306	Statistics of HTTP transactions in FortiView record the values of only the first 100 records, and the 5-minute filter records up to only the first 250 transactions.

High Performance Network Security