



FortiWeb Release Notes

VERSION 6.3.3

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



May 20, 2020

FortiWeb 6.3.3 Release Notes

1st Edition

TABLE OF CONTENTS

| | |
|---|-----------|
| Change log | 4 |
| Introduction | 5 |
| What's new | 6 |
| New features | 6 |
| Enhancements | 7 |
| Upgrade instructions | 9 |
| Hardware , VM, cloud platforms, and browsers support | 9 |
| Image checksums | 10 |
| Upgrading from previous releases | 10 |
| Repartitioning the hard disk | 15 |
| To use the special firmware image to repartition the operating system's disk | 15 |
| To repartition the operating system's disk without the special firmware image | 16 |
| Upgrading an HA cluster | 17 |
| Downgrading to a previous release | 18 |
| FortiWeb-VM license validation after upgrade from pre-5.4 version | 18 |
| Resolved issues | 19 |
| Known issues | 20 |

Change log

May 20, 2020 Initial release.

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 6.3.3, build 1074.

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 FortiSandbox Cloud powered by FortiGuard
- Real-time attack insights and reporting with advanced visual analytics tools
- Integration with FortiGate and FortiSandbox for ATP detection
- Behavioral attack detection
- Advanced false positive and negative detection avoidance

FortiWeb hardware and virtual machine platforms are available for medium and large enterprises, as well as for service providers.

For additional documentation, please visit the FortiWeb documentation:

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

What's new

New features

Introducing Deep Learning

As part of Machine Learning for Anomaly Detection, FortiWeb now builds mathematical models with fewer samples but continues to collect samples and optimize the mathematical models as more samples are collected overtime. This allows FortiWeb to provide protection much faster and to enhance accuracy over time.

For more information, see [Configuring anomaly detection policy](#).

New XSS Syntax Based Detection module

- XSS Syntax Based Detection is introduced to detect XSS injection attacks by analyzing the HTML/JavaScript syntax.
- SQL Injection (Syntax Based Detection) is moved from **Web Protection > Signatures** to **Web Protection > Advanced Protection > SQL/XSS Syntax Based Detection**.

For more information, see [Syntax-based SQL/XSS injection detection](#).

Client management

Client management allows to track a client by either the recognized cookie or the source IP. When a client violates a WAF rule, FortiWeb accumulates the threat score based on the configured threat weight value, and takes actions accordingly. This feature replaces Device Tracking, Device Reputation, and Client Device Management.

For more information, see [Client management](#).

Bad Robot and Known Search Engines integrated to Known Bots for better bot management

- Bad Robot is removed from the main signature class in **Web Protection > Known Attacks > Signatures**.
- Known Search Engines is removed from **Server Objects > Global** and **Policy > Web Protection Profile**.
- Both the modules are integrated into **Bot Mitigation > Known Bots**.

For more information, see [Configuring known bots](#).

New AJAX block page for AJAX requests

You can now enable Replacement Message for AJAX requests in **Config > Replacement Message > Replacement Message**.

For more information, see [Configuring an error or authentication page](#).

Support for Cookieless clients in NTLM Delegation

The Site Publish module can now support NTLM delegation for cookieless clients.

For more information, see [Offloaded authentication and optional SSO configuration](#).

Additional information on Blocked IPs

A new "reason" column has been added in **Monitor > Blocked IPs**.

For more information, see [Monitoring currently blocked IPs](#).

Parameter type in Global White List optimized

URL/Domain filters are added for parameter type in Global White List, allowing better granularity when certain parameters need to bypass the security modules.

For more information, see [Configuring the global object white list](#).

User tracking data shared across content routing rules

Web protection profiles using the same user tracking rules can share user tracking data now.

SameSite flag added in cookiesession1 to help prevent CSRF attacks

You can now assign a `SameSite` flag to internal cookies and set strict, lax or none value to define whether any request from the third parties carries such cookies or not.

For more information, see [server-policy policy](#).

Support for chunk encoded HTTP requests

FortiWeb can now parse the chunk encoded body in HTTP requests.

client-ip/server-ip support in diagnose debug flow filter module-detail

You can now specify a source and/or destination IP address to include or exclude module debug logs involving the specified IP address.

For more information, see [debug flow filter](#).

Enhancements

Login failure message optimization

"Failed to search user DN" and "Failed to bind LDAP server" login failure messages are replaced with generic "Failed to login" message to avoid user enumeration attacks. You can view more login failure information in the event log.

Default block period value increase

The default value for "Period Block" is updated to 600 seconds to ensure higher security.

Bot Analysis moved to FortiView > Security

The Bot Analysis page is optimized to show detailed information on search engines and malicious bots.

For more information, see [Bot analysis](#).

Predefined policies in Custom Policy and Bot Mitigation Policy

- Predefined Bot Mitigation policies are added in Bot Mitigation Policy.
- Predefined Advanced Protection policy (alert only) is added in Custom Policy.

Device Tracking, Device Reputation, and Client Device Management removed

Device tracking related modules and configurations are removed from this release. Tracking is now done using the new Client Management feature.

For more information, see [Client management](#).

Least connection algorithm enhancement

When distributing new TCP connections to the server pool member, the Least Connection algorithm is enhanced to avoid new connections always being processed by the same member.

Enhancements for Machine Learning Anomaly Detection

- You can re-admit a noisy sample to the legitimate sample pool.
- Threat Models have been optimized to reduce false positives.
- You can define an expiration time for patterns. All the samples related with the expired patterns will be cleared from the database.

For more information, see [Configuring anomaly detection policy](#).

HA heartbeat enhancement

HA heartbeat is optimized to provide better stability and scalability.

Virtual IP limit lifted in high volume active-active HA mode

In addition to standalone, active-passive, standard active-active modes, now FortiWeb 1000E, 2000E, 3000E, 3010E, and 4000E appliances in high volume active-active HA mode also support a maximum number of 6000 virtual IPs.

New regions support by FortiWeb Fabric Connectors for OCI platform

Fabric Connectors now support all available OCI regions.

Autoscaling enhancement on AWS

For the FortiWeb autoscaling solution on AWS, an elastic IP is now supported to access the master node.

Using templates to auto-deploy FortiWeb HA on AWS and Azure

FortiWeb HA group with up to eight members can be automatically deployed using templates on AWS and Azure.

Limiting access to specific source IP addresses

You can now define an Allow Only IP range in **IP List** to limit access to the application to specified IP addresses.

For more information, see [Blacklisting & whitelisting clients](#).

FortiAnalyzer support for log export

Forwarding attack logs to FortiAnalyzer is now supported.

TCP buffer default value changed

The default value of `tcp-buffer` is changed to `max`.

Upgrade instructions

Hardware , VM, cloud platforms, and browsers 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

Supported hypervisor versions:

- VMware vSphere Hypervisor ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0/6.5/6.7
- 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 Queens 17.0.5
- 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.

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.

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.

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 6.3.3 from versions earlier than 6.3.0. You need to install FortiWeb-VM 6.3.3 instead of upgrading to 6.3.3. 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

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 master appliance will take effect on all slaves 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.



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.



For FortiWeb-VM on docker platform, it's not supported to upgrade to 6.3.3 from versions earlier than 6.3.0. You need to install FortiWeb-VM 6.3.3 instead of upgrading to 6.3.3. For how to install, see [FortiWeb-VM on docker](#).

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 master appliance will take effect on all slaves 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 master appliance will take effect on all slaves 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 master appliance will take effect on all slaves 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

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](#).
8. Upgrade to FortiWeb 6.1.1.
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 master appliance will take effect on all slaves simultaneously.



- If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see [FortiWeb-VM license validation after upgrade from pre-5.4 version](#).
- The upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.
- The upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.



The "Bad Robot" and "SQL Injection (Syntax Based Detection)" signatures had been integrated into WAF modules "Bot Mitigation > Known Bots" and "SQL/XSS Syntax Based Detection" since 6.3.3. If you upgrade from a version earlier than 6.3.3, all settings of these two signatures will be merged to corresponding modules except the exception list.

Make sure to **add the exception list manually** after the upgrade, otherwise certain traffic will be blocked unexpectedly because of the missing of the exception list.

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

Repartitioning the hard disk

To upgrade from a version of FortiWeb previous to 5.5, you must first resize your FortiWeb operating system's disk.

In most cases, you'll have to install a special firmware image to repartition the disk. For details, see [To use the special firmware image to repartition the operating system's disk on page 15](#).

For the following FortiWeb-VM tools, you cannot install the special firmware image to repartition the hard disk:

- Citrix XenServer
- Open-source Xen Project
- Microsoft Hyper-V
- KVM

For these platforms, to repartition the disk you must deploy a new virtual machine and restore the configuration and log data you backed up earlier. See [To repartition the operating system's disk without the special firmware image on page 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 16](#)
3. Deploy a new FortiWeb 5.5 or later virtual machine on the same platform.
4. Use the instructions for your hypervisor platform to attach the log disk you detached earlier to the new VM:
 - [To attach the log disk to a Citrix XenServer VM on page 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.

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 6.3.3. For inquiries about a particular bug, please contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

| Bug ID | Description |
|-----------------|---|
| 0631605 | Modified static route caused system outage. |
| 0629617 | When the element type is JSON Elements, the created signature exception fails to be applied. |
| 0628496 | FortiWeb crashes when libcmime parses the MIME header if the protocol is ActiveSync for file security. |
| 0624865 | Multiple HTTP constraint exceptions fail to be added using the same hostname while different IPs in GUI. |
| 0622698 | MSG_ID is missing in 503 replacement response message. |
| 0618549 | When the connection ends abnormally, some modules may leak memory. |
| 0620888/0612474 | If the redirect action policy is triggered by a certain part of the request, FortiWeb directly executes the action, without parsing the rest part of the request. |
| 0606221 | When setting port1 as hbdev port and executing <code>ha disconnect</code> , port10 and above ports are not shut down unexpectedly. |
| 0604298 | With <code>fortiguard-anycast</code> enabled, if FortiWeb-VM is disconnected from FDS for over 4 hours, it won't generate elog to warn this situation. |
| 0603448 | The IPv6 DAD checks VIP IPv6 conflict, but no event log is generated. |

Known issues

This section lists known issues in version 6.3.3, but may not be a complete list. For inquiries about a particular bug, please contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

| Bug ID | Description |
|-----------------|--|
| 0665507 | The exception list of WAF signatures under "Bad Robot" and "SQL Injection (Syntax Based Detection)" will be lost if you upgrade from a version earlier than 6.3.3. |
| 0630923/0630919 | For FortiWeb-VM with a license purchased earlier than February 2019, upgrading to 6.3.3 will cause FortiWeb-VM to break down or its performance drops down dramatically. |
| 0633427 | Uploading large file through FTP fails when the back end server's performance is low. |
| 0604053 | FortiWeb 100D devices reboot for unknown reasons in rare cases. |
| 0604051 | Cannot get the API key when the API key is set in request body in HTTP2 environment. |
| 0602759 | Selecting NO-NAT or Pool in SNAT policy and leaving the Egress Interface blank may cause display problems on GUI. |
| 0602712 | Not configuring external and mapped addresses in DNAT policy may cause the port forwarding configurations to be lost. |
| 0598144 | In Web Cache, when the gzip response is cached but the client does not support gzip, it may result in page display issues at the client side. |
| 0597351 | In machine learning, for certain domain types with multiple patterns, it costs very long time to finish the sample collection. |
| 0596000 | Users with privileges to a certain ADOM can access contents restricted to other ADOMs through CLI. |
| 0595053 | If the IP address is IPv6 and the HTTP version is 1.1 or 2, the device tracking module does not work well. |
| 0578585 | In active-active high volume HA mode, if the physical port IP address and the VIP address are in the same network segment, the physical port's mac address instead of the VIP's mac address will be learned by the switch. |
| 0556301 | FortiWeb responds with different TCP ports when running <code>sudo nmap</code> towards a physical interface. |



FORTINET[®]



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.