FORTINET

Release Notes

FortiWeb 7.2.0

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

December 16, 2022
FortiWeb 7.2.0 Release Notes
1st Edition

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 7.2.0, build 0311.

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 7.2.0 offers the following new features and enhancements.

API Gateway enhancements

- User rate limit setting is added in **API Protection > API Gateway** to rate limit API requests by users. When enabled, if a user sends too many API requests, subsequent requests from the same user will be blocked.
- **X-RateLimit-*** headers can be added in the response packet if the user exceeds the rate limit. The following information can be displayed to users: the request limit, the remaining requests, and the minimum time to wait before the user is allowed to send the next request.
- More ways to secure the API key. It's now possible to refresh the standard API key. Dynamic key and 3rd party key such as JWT are also supported.

Parameter Validation enhancements

It's now supported to configure the following options in Parameter Validation:

- Whether the parameters to be scanned are in URL or the request body;
- Limit the maximum number of parameters in a request;
- Whether to check the parameters in JSON or not.

Client Management enhancements

- You can now configure multiple Threat Score profiles in an ADOM.
- In addition to Block Period by IP or Client ID, you can also set the action to Alert or Alert&Deny for suspicious and malicious clients.
- You can limit Threat Score threshold calculation to signature violations only thus only using this feature for signature violations. When enabled, Action will only be taken based on the calculated threshold rather than the signature category action configuration.
- Multiple history threats are now recorded in Client Management attack logs.

Sensitivity level for signatures available in GUI

You can now set the sensitivity level for signatures in GUI as well as in CLI.

Added to CLI only in version 7.0.2 this feature lets you can choose from four categories of attack signatures (L1 to L4) based on their sensitivity to false positives and their requirement for a higher security level. Every level adds additional signatures thus increasing security but also the possibility of blocking legitimate traffic

FortiToken mobile notification

If you are using FAC Radius server to authenticate clients, it's now supported to send FortiToken mobile notification automatically to clients for extra token authentication.

Run the following command to enable it:

```
config user radius-user
   edit "fac-radius"
      set fac-push enable
   next
end
```

Server policy tags

Administrators can now use tags for server policy. This helps in labeling server policy for future usage such as sorting, filtering and acknowledging policies.

Certificate verification for LDAP server

LDAP authentication now supports certificate and hostname verification for TLS connections. Both commercial and private certificates are supported.

TLS-ALPN-01 and DNS challenges from Let's Encrypt

To avoid using port 80 on FortiWeb when Let's Encrypt validates your ownership of the domain names, the following two challenge methods are now supported:

- TLS-ALPN-01: This method allows Let's Encrypt to send HTTPS requests to FortiWeb for validation. It requires HTTPS service to be enabled on FortiWeb.
- DNS-01: This method allows Let's Encrypt to do validation through your DNS provider. FortiWeb will generate a TXT record, then you need to add this TXT record to the DNS record.

Run the following command to enable them:

```
config system certificate letsencrypt
   edit <lets_cert_name>
      set domain <domain-name>
      set validation-method {TLS-ALPN-01 | DNS-01}
   next
end
```

Tracking users with JSON format login

It's now supported to track users with JSON format login credentials such as the token based API login.

Lua script update

A new predefined Lua script "HTTP_REWRITE_BODY" is added. It can be used to find, remove, and replace data in the body of an HTTP request. For example, during Site Publishing authentication you can use it to parse and modify the Username field located in the HTTP Request Body before it's sent to the back-end server.

Global resource

Global Resource page is added under **System** to display the current usage and maximum configuration values of the FortiWeb appliance.

HA debug enhancement

HA debug commands are enhanced to be more user friendly.

Debug file download for the secondary appliances

The debug file for the secondary FortiWeb can now be downloaded in **System > High Availability > Topology** of the primary node in an HA group.

Real time packet capture

Packet captures and flow debug logs can now be recorded in real-time and viewed in **Network > Packet Capture**.

TCP buffer size increase

The TCP buffer size can now be set to at most 3992 KB.

ASAN executable integrated into debug symbol file

To enhance the deployment of ASAN (Address Sanitization), the ASAN bin files are now bundled as part of the debug symbol file "image.out.debug.zip", which can be loaded onto FortiWeb through **Maintenance > Debug > Upload Debug Symbol File**.

Event log on JSON Schema file upload failure

The error message of the JSON Schema file upload failure now reveals more details on the possible causes, and an event log will also be recorded.

Admin password hash change

The admin user password hash is changed from sha1 to sha256 in this release.

If you upgrade FortiWeb from previous version to 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.

If you downgrade from 7.2.0 to earlier releases, you may need to convert password hash or recreate the lost accounts depending on which version you are downgrading to. Notification message will be displayed in GUI or CLI when you first reboot after the downgrade. Please follow the instructions accordingly.

Support disabling config-sync port

To improve security, you can now disable port 995 if you don't need config sync. This option is added in **System > Admin > Settings**.

It is disabled by default, so remember to enable port 995 when you need to execute config sync.

Global menu not available to ADOM users

The Global menu in GUI and the global commands in CLI will no longer be available to ADOM Users.

New platform support

FortiWeb 1000F is introduced in this release.

Flex-VM license importing through Cloud-init

For FortiWeb deployed on AWS, you can now import the Flex-VM license through Cloud-init.

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

To download the Customer Service & Support image checksum tool

After logging in to the website, in the menus at the top of the page, click **Download**, and then click **Firmware Image Checksums**.

Alternatively, near the bottom of the page, click the **Firmware Image Checksums** button. This button appears only if one or more of your devices has a current support contract. In the **File Name** field, enter the firmware image file name including its extension, then click **Get Checksum Code**.

Upgrading from previous releases

- For FortiWeb-VM with a license purchased earlier than February 2019, you must upgrade to 6.3.4 or higher. Do not use a lower patch.
- The VLAN, 802.3ad Aggregate, and Redundant interfaces are not supported anymore on FortiWeb-VMs deployed on public cloud platforms since 6.3.6. If you upgrade from versions earlier than that, these configurations will be removed.

We don't provide maintenance for 6.4.x releases unless major errors, so we don't recommend you to upgrade to 6.4.x. Please upgrade 6.4.x to 7.0.

In several hours or days (depends on number of existing logs) after upgrading from version earlier than 6.4.0 (5.x and 6.0.x-6.3.x) to 7.0, there might be delay (30-60 mins) to display new logs on GUI. This is caused by log version upgrade in 6.4.x & 7.0. It takes time to scan and process all existing logs.

To upgrade from FortiWeb 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 7.2.0 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.2.0 instead of upgrading to 7.2.0. 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 7.2.0 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.2.0 instead of upgrading to 7.2.0. For how to install, see FortiWeb-VM on docker.

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

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

To upgrade from FortiWeb 5.5.x, 5.6.x, 5.7.x, 5.8.x, or 5.9.x

Before the upgrade:

- If you upgrade from a version of FortiWeb previous to 5.9.0 on Azure platform, first change the addressing mode to DHCP in **System > Network > Interface**, then upgrade to FortiWeb 6.1.1, because FortiWeb on Azure platform has enforced the DHCP addressing mode since release 5.9.0.

After the upgrade:

- There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
  - Run `get system status` to check the `Database Status`.
  - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.

If you upgrade from a version of FortiWeb previous to 5.5.4, the upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.

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

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

To upgrade from FortiWeb 5.4.x

Before the upgrade:

- Resize your FortiWeb hard disk partitions. See Repartitioning the hard disk.

After the upgrade:

- There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
  - Run `get system status` to check the `Database Status`.
  - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.

The upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.

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

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

To upgrade from FortiWeb 5.3.x

Before the upgrade:

- Resize your FortiWeb hard disk partitions. See Repartitioning the hard disk.

After the upgrade:

- There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2.
  - Run `get system status` to check the `Database Status`.
  - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.

- If you are upgrading FortiWeb-VM on a hypervisor other than VMware vSphere, see FortiWeb-VM license validation after upgrade from pre-5.4 version.
- The upgrade process deletes any HTTP content routing policies that match X509 certificate content. You can re-create these policies using the new, enhanced X509 certificate settings.
- If you upgrade from a version of FortiWeb previous to 5.3.4 and your server policy configuration includes settings that customize an attack blocking or server unavailable error page, the upgrade deletes these server-based settings. The functionality is replaced by the global, default FortiWeb pages.
- If you upgrade from a version of FortiWeb previous to 5.3.6, the upgrade process deletes any V-zone IP addresses, which are no longer required. This operation has no impact on routing or connectivity after the upgrade.

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

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

To upgrade from a version previous to FortiWeb 5.3

FortiWeb5.3.exe is a Microsoft Windows executable script that automatically migrates your FortiWeb 5.2.x configuration settings to a 5.3.x configuration.

1. If your version is 5.0.x or 5.1.x, upgrade to FortiWeb 5.2.x.
2. Use **System > Maintenance > Backup & Restore** to back up your FortiWeb configuration. Fortinet recommends that you use the **Backup entire** configuration option.
   Note: If you forget to back up the configuration before you upgrade to FortiWeb 5.3, you can use the **Boot into alternate firmware** option to downgrade to the previous version, and then backup its configuration. For details, see the *FortiWeb Administration Guide*:
   HTTP://docs.fortinet.com/fortiweb/admin-guides
3. To obtain the upgrade script, log in to the Fortinet Customer Service & Support website:
   HTTPs://support.fortinet.com
   In the menus at the top of the page, click **Download**, and then click **Firmware Images**.
4. For product, select **FortiWeb**. Then, on the Download tab, navigate to the following folder:
   `/FortiWeb/v5.00/5.3/Upgrade_script/`
5. Download the .zip compressed archive (for example, `FortiWeb5.3Upgrade_v1.9.zip`) to a location you can access from your Windows PC.
6. In Windows, extract the .zip archive's contents, and then use a command line interface to execute the upgrade script.
   For example, in the directory where the file `FortiWeb5.3Upgrade.exe` and your backup configuration file are located, execute the following command:
   ```
   FortiWeb5.3Upgrade.exe -i YOUR_CONFIG_NAME.conf -o 5.3_new.conf
   ```

The script removes the Domain Server, Physical Server, Server Farm, Content Routing policy configurations and generates a new configuration file named `5.3_new.conf`.

7. Resize your FortiWeb hard disk partitions. See Repartitioning the hard disk.
8. Upgrade to 6.3.9 first, then upgrade to 7.2.0.
9. Use **System > Maintenance > Backup & Restore** to restore the configuration file you created using the script (for example, `5.3_new.conf`).
10. There might be database compatibility issue after the upgrade, because the MarisDB database version is upgraded to 10.3.8 since FortiWeb 6.0.2:
    - Run `get system status` to check the `Database Status`.
    - If it shows `Available`, it means the database works well. If it shows `Not Available`, you need to run `execute db rebuild` to solve the database compatibility issue. Please note in HA mode, running `execute db rebuild` on primary appliance will take effect on all secondary appliances simultaneously.

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

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

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

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

Repartitioning the hard disk

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

In most cases, you'll have to install a special firmware image to repartition the disk. For details, see To use the special firmware image to repartition the operating system's disk on page 16.

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

- Citrix XenServer
- Open-source Xen Project

- Microsoft Hyper-V
- KVM

For these platforms, to repartition the disk you must deploy a new virtual machine and restore the configuration and log data you backed up earlier. See To repartition the operating system's disk without the special firmware image on page 16.

Repartitioning affects the operating system's disk (USB/flash disk), not the hard disk. Existing data such as reports and event, traffic, and attack logs, which are on the hard disk, are not affected.

You can use this image to upgrade an HA cluster by following the same procedure you use for a regular firmware upgrade. For details, see "Updating firmware on an HA pair" in the *FortiWeb Administration Guide*:
HTTP://docs.fortinet.com/fortiweb/admin-guides

To use the special firmware image to repartition the operating system's disk

1. Perform a complete backup of your FortiWeb configuration.
   Although the repartitioning firmware image automatically saves your FortiWeb configuration, Fortinet recommends that you also manually back it up. For details, see the *FortiWeb Administration Guide*:
   HTTP://docs.fortinet.com/fortiweb/admin-guides
2. Contact Fortinet Technical Support to obtain the special repartitioning firmware image: special build 5.4.1, build 6066.
3. Follow one of the same procedures that you use to install or upgrade firmware using a standard image:

- In the Web UI, go to **System > Status > Status**. Locate the **System Information** widget. Beside **Firmware Version**, click **[Update]**.
- In the Web UI, go to **System > Maintenance > Backup & Restore**. Select the **Restore** option in **System Configuration**.
- In the CLI, enter the `execute restore config` command.

FortiWeb backs up the current configuration, resizes the hard drive partitions, and boots the system.

Continue with the instructions in Upgrading from previous releases on page 10.

To repartition the operating system's disk without the special firmware image

1. Perform a complete backup of your FortiWeb configuration. For details, see the *FortiWeb Administration Guide*:
   HTTP://docs.fortinet.com/fortiweb/admin-guides
2. Use the instructions for your hypervisor platform to detach the log disk from the VM:
   - To detach the log disk from a Citrix XenServer VM on page 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 17

- To attach the log disk to a KVM VM on page 17

5. Restore the configuration you backed up earlier to the new VM.
6. When you are sure that the new VM is working properly with the required configuration and log data, delete the old VM.

To detach the log disk from a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the VM, on the Storage tab, select **Hard disk 2**, and then click **Properties**.
3. For **Description**, enter a new description, and then click **OK**.
4. Select **Hard disk 2** again, and then click **Detach**.
5. Click **Yes** to confirm the detach task.

To detach the log disk from a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the FortiWeb-VM in the list of machines, and then, under **Actions**, click **Settings**.
2. Select **Hard Drive (data.vhd)**, and then click **Remove**.
3. Click **Apply**.

To detach the log disk from a KVM VM

1. In Virtual Machine Manager, double-click the FortiWeb-VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.

To attach the log disk to a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.
2. In the settings for the new, FortiWeb 5.5 or later VM, on the Storage tab, select **Hard disk 2**, and then click **Delete**.
3. Click **Yes** to confirm the deletion.
4. On the Storage tab, click **Attach Disk**.
5. Navigate to the hard disk you detached from the old VM to attach it.
6. Start your new virtual machine.

To attach the log disk to a Microsoft Hyper-V VM

1. In the Hyper-V Manager, select the new, FortiWeb 5.5 or later virtual machine in the list of machines, and then, under Actions, click **Settings**.
2. Select **Hard Drive (log.vhd)**, and then click **Browse**.
3. Browse to the hard drive you detached from the old virtual machine to select it.
4. Click **Apply**.
5. Start the new virtual machine.

To attach the log disk to a KVM VM

For KVM deployments, you remove an existing virtual disk from the new VM before you attach the disk detached from the original VM.

1. In Virtual Machine Manager, double-click the new, FortiWeb 5.5 or later VM in the list of machines.
2. Click **Show virtual hardware details** (the "i" button).
3. Click **VirtIO Disk 2**, and then click **Remove**.
4. Click **Add Hardware**.
5. Click **Storage**, select **Select managed or other existing storage**, and then click **Browse**.
6. Click **Browse Local**.
7. Navigate to the log disk file for the original machine to select it, and then click **Open**.
8. For **Device type**, select **Virtio disk**, for **Storage format**, select **qcow2**, and then click **Finish**.
9. Start the new virtual machine.

Upgrading an HA cluster

If the HA cluster is running FortiWeb 4.0 MR4 or later, the HA cluster upgrade is streamlined. When you upgrade the active appliance, it automatically upgrades any standby appliance(s), too; no manual intervention is required to upgrade the other appliance(s). This includes upgrading using the special hard disk repartitioning firmware image for upgrading to 5.5 or later from earlier releases.

If the HA cluster is running FortiWeb 4.0 MR3 Patch x or earlier, contact Fortinet Technical Support for assistance.

Downgrading to a previous release

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

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

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

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

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

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

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

Resolved issues

This section lists issues that have been fixed in version 7.2.0. For inquires about a particular bug, please contact Fortinet Customer Service & Support: HTTPs://support.fortinet.com

Bug ID	Description
0865971	FSSI related errors occur after switching to Flex VM license.
0865489	Base64 decoding fails because of missing padding character '='.
0863863	Should a dd a search function on the site publish rule in GUI.
0862893	Support JSON Restful-API on certificate CRL and CA.
0859928	Memory leak occurs in mlapi_daemon on cloud.
0858312	Error message `Refused to get unsafe header "X-FWB-AJAX-REPONSE"` displays.
0850444	In transparent Inspection mode, the new master device does not work when HA switchover occurs
0849939	Should add field "eventtime" when sending logs to FortiAnalyzer.
0848896	The maximum length of the CSP HTTP header should be extended.
0842062	WAD site shows as disconnected and no files being backup even though connection test shows successful.
0840985	Legitimate users are mistakenly considered as bots due to the current RBE design mechanism
0830883	URL Rewrite for response packets cannot work when the request body is large and the response is compressed.
0825842	CAPTCHA challenge cannot work sometimes, which is due to the table size in code.
0821873	Add CLI option client-real-ip-random-port to fix port issue when connecting to pserver.
0818909	More details should be explained in the error message when uploading JSON file fails.
0806491	Should support single source IP in health check.
0791636	The reqeusts with 304 response and dropped by Cache should not be added to blocked requests.

Common Vulnerabilities and Exposures

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

Bug ID	CVE reference
0856580	FortiWeb 7.2.0 is no longer vulnerable to the following CWE-Reference: CWE-415.

Known issues

This section lists known issues in version 7.2.0, 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
0868802	JWT parameter value of API Gateway is incomplete on GUI.
0867761	Duplicated or blank IP list can be accepted and saved to configuration.
0867088	Fail to parse the payload by XML parser due to the entity with syntax errors.
0859380	The traffic is blocked when a user is not in the referenced API user group, but there is no attack log and the debug info is not right.
0846605	ADOM user can see Virtual IPs in other ADOM user's account.
0834665	Raw body cannot be recorded when there is a delay between the request headers and the request body.

www.fortinet.com

Copyright© 2022 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.