FortiWeb Release Notes

VERSION 7.0

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

January 19, 2022
FortiWeb 7.0 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 7.0, build 0057.

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

FortiWeb 7.0 offers the following new features and enhancements.

New features

API Discovery and Protection

Machine Learning Based API Discovery and Protection is introduced. Using machine learning algorithms FortiWeb parses the REST API schema and data structure and builds mathematical models to block any malicious API requests.

For more information, see Configuring API Protection Policy.

Enhancements

Dashboard and FortiView enhancements

New Widgets are introduced in Dashboard to display System information, security events, user tracking information, and FortiView statistics. The Monitor tab and FortiView tab are removed in this release.

For more information, see Dashboard.

New Action Type – Client ID Block Period

A new action type has been added - Client ID Block Period. It allows blocking a malicious user based on the FortiWeb generated client ID rather than source IP.

For more information, see the Block Method option in Client management.

Ability to block directly from FortiView

You can now conveniently block source IP addresses from FortiView.

OAuth 2.0 support

FortiWeb now supports OAuth 2.0 in Site Publish for front-end authentication.

Personally Identifiable Information

The Personally Identifiable Information signature dictionary can now be used in custom rules.

Credential stuffing online query

It is now possible to use the extended FortiGuard credential stuffing database using an online query instead of the local DB query. The online database is larger and covers additional leaked credentials from data breaches. Enable it using the online database from CLI.

Exceptions in SQL/XSS-Syntax-Based-Detection (SBD) and Bot-Mitigation

You can now add exceptions in SQL/XSS-Syntax-Based-Detection (SBD) and Bot-Mitigation modules to mitigate false positives.

For more information, see Exception Policy.

Default route enhancements

To avoid conflict, the system route, HA static route, and DHCP route can now be assigned with different routing metrics. Duplicate destination verification will be performed.

Support for multiple wildcard admin users

It's now supported to set more than one wildcard admin users.

Support for HSM HA group

FortiWeb now supports HSM HA group containing two HSM servers.

LDAP server health check

You can now enable LDAP server health check so that user authentication will not be affected if some of the IP addresses associated with the LDAP domain name are down.

Configuration change event logging enhancement

The event log has been enhanced to include additional information when the configuration changes (Log&Report > Event).

Traffic logging default behavior change

To avoid unnecessary resource consumption, the system by default doesn't generate traffic log for all server policies unless specified. In order for the traffic log to work, not only should it be enabled via “Other Log Settings” under Log&Report, but also in server policy settings via the CLI command `config server-policy policy`.

New VM16 license

VM-16 license is introduced to support up to 16 vCPUs.

FortiWeb-VM on OpenStack license file importing method update

FortiWeb-VM on Openstack has changed the license file importing method due to OpenStack changes.

Azure load balancer support enhancements

FortiWeb-VMs can now be deployed in multiple shared back-end pools behind an Azure load balancer.

Optimization of GEO IP, IP List, and IP Reputation

To optimize performance FortiWeb now executes GEO IP, IP List, and IP Reputation policies at the TCP layer to avoid HTTP data being processed unnecessarily. This is only enabled when Server Objects > X-Forwarded-For is not used. It's now also supported to set the trigger action to Deny (no log) or Period Block to avoid alert flooding.

For more information, see the description of "Ignore X-Forwarded-For" and "Trigger Action" in GEO IP, IP List, and IP Reputation.

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 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 Queens 17.0.5
- 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 wait for the next major version.

To upgrade from FortiWeb 6.4.0

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 7.0 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.0 instead of upgrading to 7.0. 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 7.0 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.0 instead of upgrading to 7.0. 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

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 6.3.9 first, then upgrade to 7.0.
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 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 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

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 9.

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 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 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 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

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 7.0. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0770509	IP List feature does not work with Content Routing.
0770008	Fail to add IP to block list due to threat score exceeds limit.
0767114	proxyd crashes when data is bigger than 2048 and contains HTTP Annotation.
0767042	FortiWeb's syslog payload is more than 64k per entry.
0766608	Local user can't access or download reports at Report Browse page.
0766087	Configured administrators can't view Reports at Report Browse page.
0760603	Authentication Failure in Active-Sync (Missing Domain Prefix).
0760376	Debugging logs are printed in UTC time only.
0760190	Attack log filter does not apply properly immediately after another filter.
0759685	Cloud Connector server-type not selectable or CLI parse error.
0759242	Blockage due to Unauthorized GEO IP.
0758649	Disable javascript injection.
0758200	There are some false positives of "SQL/XSS Syntax Based Detection" module.
0757846	The "client certificate verify" setting to be greyed out if SNI is applied under "Advanced SSL Settings".
0755118	Caching causes some image files to fail uploading.
0754881	Alert emails are not sent as per interval.
0754774	Javascript is not blocked as configured.
0754375	GUI missing bottom Left-to-right scroll bar on HTTP Content Routing page.
0754230	Missing "includeSubDomains; preload" in HSTS header.
0753521	Parameter validation module does not work properly because there is a parameter validation policy which doesn't refer any parameter validation rules.
0752790	Synchronization with the peer device fails randomly.
0752769	The message "is not a qualified HTTP hostname" is displayed when creating a new report.
0752742	Cannot delete pending undefined reports.

Bug ID	Description
0752531	The "diagnose hardware check" memory failure may occur unexpectedly.
0751401	The error message "Invalid XML WSDL file." displays when importing WSDL schema.
0750312	High memory usage - proxyd restarted due to OOM.
0750111	Logs for certificate issue are not shown in summary.
0747536/0741318	Letsencrypt is not issuing certificate and not synch via HA.
0744677	Saved attack log filter will not apply.
0742851	SNAT breaks the backend communication halfway in 6.3.13 version and above. This is caused by the HA-AAS session output having higher priority than `nf_confirm`.
0741625/0725696	Signatures are matching content of uploaded file. This is a false positive detection caused by the system wrongly takes body data as parameters.
0735446	Unable to download a pdf file while using HTTP/2.
0734471	Application slowness when the traffic starts to increase. This occurs when syslog is enabled and FortiWeb is deployed in HA-AAS mode.
0733114	Firefox can't access with Block Mode enabled
0728661	When HTTP2 and web cache enabled, FortiWeb would return the cache content to the client if the request hits the cache.
0724993	Slow attack prevention based on "Threshold based detection" configuration does not work.
0719617	FortiWeb is correctly validating OpenAPI schema of a POST but not highlighting in the logs what is causing the failure.
0714950	When FortiWeb is behind a Load balancer that has multiple backend pools (not only FortiWeb backend pools), FortiWeb updates the wrong backend pool (the first one in the list) and sometimes with wrong NIC.
0692109	The proxyd crashes unexpectedly.
0687564	Marking multiple attack log entries only takes effect on the first one.
0683776	Executing a lot of configurations in short time through CLI might cause certain command failure.
0671018	FortiWeb won't log attack and delete the oldest log file when the disk usage is over 81%.

Common Vulnerabilities and Exposures

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

Bug ID	CVE reference
0765466	FortiWeb 7.0 is no longer vulnerable to the following CVE-Reference: CVE-2021-3672 and CVE-2020-8277.
0764512/0748216/0702593/0746027/0745991/0744624/0754964/0754591/0754309/0753920/0745330/0748202	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-121.
0761947	FortiWeb 7.0 is no longer vulnerable to the following CVE-Reference: • CVE-2021-42374 • CVE-2021-42376 • CVE-2021-42378 • CVE-2021-42379 • CVE-2021-42380 • CVE-2021-42381 • CVE-2021-42382 • CVE-2021-42384 • CVE-2021-42385 • CVE-2021-42386 • CVE-2019-5747 • CVE-2021-28831 • CVE-2018-1000500 • CVE-2018-1000517
0761250	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-792.
0759713	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-384.
0759275	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-312.
0757476/0754964/0754591/0754309/0753920	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-121.
0755562	FortiWeb 7.0 is no longer vulnerable to the following CVE-Reference: • CVE-2021-33193 • CVE-2021-34798 • CVE-2021-36160 • CVE-2021-40438 • CVE-2020-13938 • CVE-2019-17567
0750135/0754269/0749521	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-122.
0753313	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-120.
0747552/0747551/0752799/0750827/0753292	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-78.

Bug ID	CVE reference
0751765/0744937	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-601.
0748808/0744638/0748852/ 0748820/0748555	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-22.
0748234/0748536/0748537/ 0748531/0748232	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-23.
0745673	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-321
0746602	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-284.
0742534/0742239/0745289/ 0744904/0742240	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-79.
0742829/0745014	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-77.
0744621	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-400.
0744329	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-362.
0744269	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-788.
0744041	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-347.
0743744	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-124.
0743076	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-441.
0750135/0754269/0749521	FortiWeb 7.0 is no longer vulnerable to the following CWE-Reference: CWE-122.

Known issues

This section lists known issues in version 7.0, 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
	Error message "Parsing error at 'oauth-spool'. err=1" appears after to 7.0 on Docker platform.
0773890	Cannot get the quarantine IP list from FortiGate
0773349	Client ID is not shown correctly in event log after the ID is released.
0765262	The system doesn't update when the Health Check DNS server is updated.
0760459	Raw and Hex body log does not show for HTTPv2.
0758584	The GET request's content-type can be other types than application/json.
0745659	The WAD behavior should be enhanced when backup file size exceeds log disk size.
0740886	Machine Learning > Anomaly Detection > Console printed "machine learning db rebuild failed" info after rebooted FortiWeb.