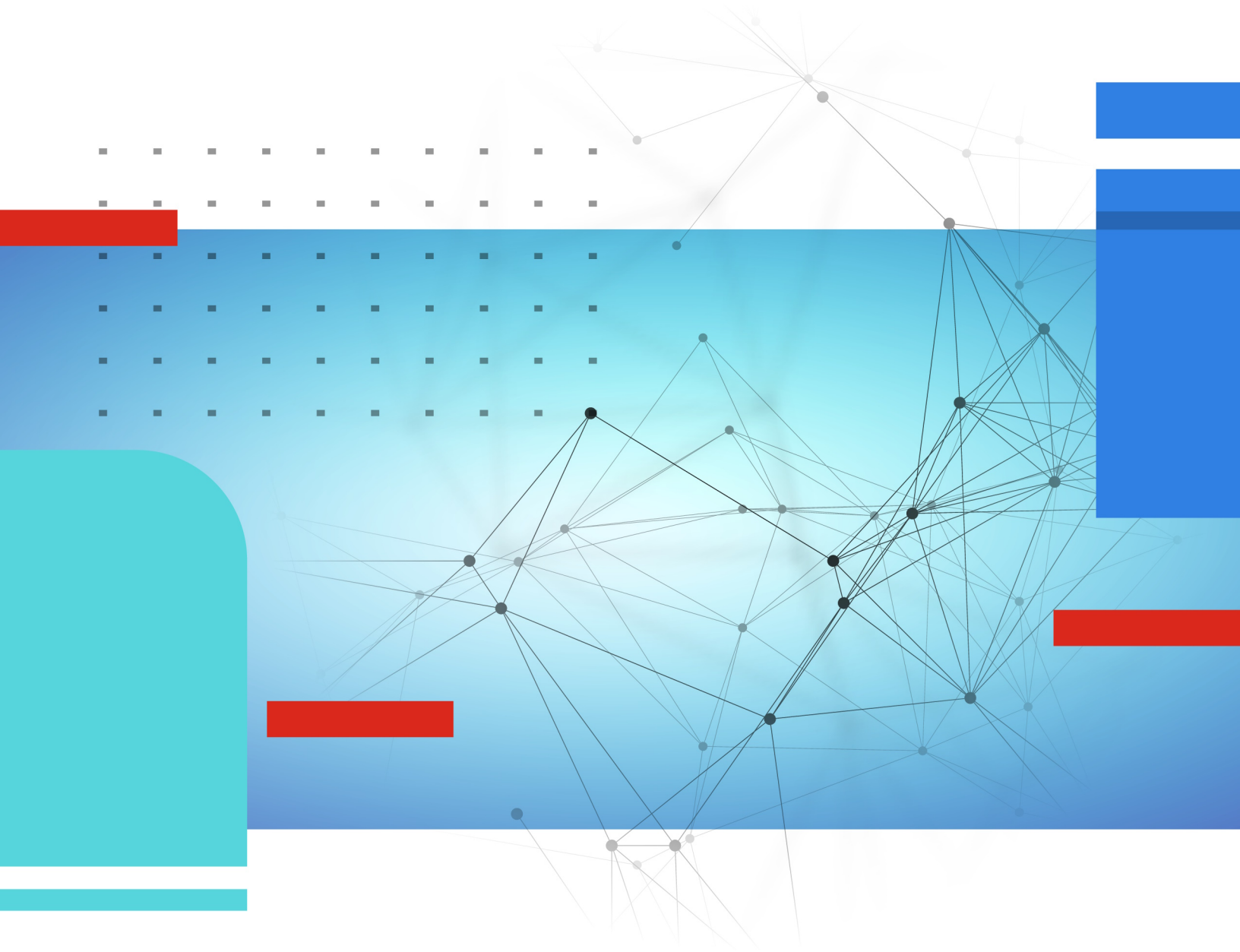
FORTINET

Release Notes

FortiWeb 7.6.8



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 22, 2026
FortiWeb 7.6.8 Release Notes

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 7.6.8, build 1128.

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 Fortinet 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 7.6.8 introduces enhancements and new features across various modules including Web Application Firewall (WAF) capabilities, server configurations, system settings, etc. Refer to this link for the new features.

Product Integration and Support

Supported Hardware:

D-Series:

- FortiWeb 400D-USG
- FortiWeb 600D-USG
- FortiWeb 1000D-USG

E-Series:

- FortiWeb 100E
- FortiWeb 400E
- FortiWeb 600E
- FortiWeb 1000E
- FortiWeb 2000E
- FortiWeb 3000E
- FortiWeb 3010E
- FortiWeb 4000E

F-Series:

- FortiWeb 100F
- FortiWeb 400F
- FortiWeb 600F
- FortiWeb 1000F
- FortiWeb 2000F
- FortiWeb 3000F
- FortiWeb 4000F

Supported hypervisor versions:

- VMware vSphere Hypervisor ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0/6.5/6.7/7.0/8.0.2/8.0.3
- 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 2012/2016/2019/2022)
- 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: 7.00051

Upgrade instructions

Upgrade notes and important information

Upgrading to the latest FortiWeb release may involve specific considerations when transitioning from previous versions. This section outlines essential warnings, potential issues, and key information users need to be aware of to ensure a smooth and successful upgrade. Please review all details carefully to avoid compatibility issues and to take full advantage of the latest features and improvements.

Key sections:

Common Upgrade Issues and Solutions

Backup Restoration Issue After Enabling Private Encryption Key

When `private-encryption-key` is enabled with the following commands in versions prior to 7.6.3, backup files may no longer be restorable after the upgrade. To avoid this issue, please ensure you create a new backup after upgrading to version 7.6.3.

```
config system encryption-method
  set private-encryption-key enable
end
```

Log Delay Post-Upgrade (6.4.x & 7.0)

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

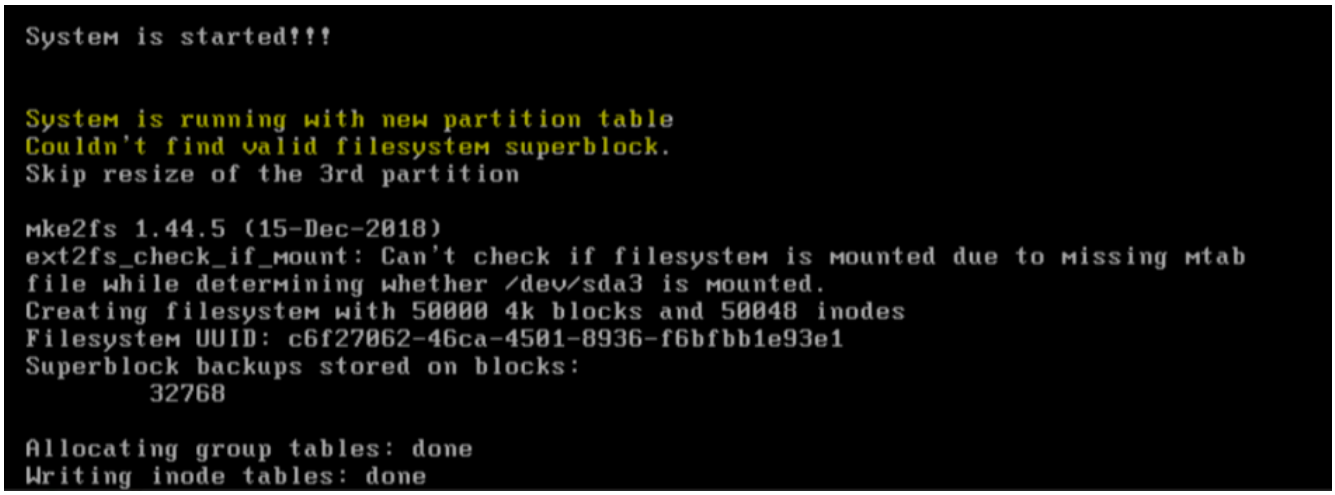
Browser Cache Issues After Upgrade

After upgrading FortiWeb to a new version, you may occasionally encounter issues where the browser continues to use a cached version of the GUI instead of fetching the updated resources from the server.

Recommendation: To ensure all resources are refreshed and the GUI functions correctly, we recommend clearing the browser cache after completing the upgrade.

Error Message to Ignore

During the upgrade, the following error message may appear in the console. This is expected and does not require any action.



Known Issues and Workarounds

Compatibility Issue with FortiWeb 100D and 7.6.0/7.6.1

DO NOT update to 7.6.0/7.6.1 for FortiWeb 100D.

Global Settings and Configuration Loss (Pre-7.6.1)

On versions earlier than 7.6.1, a non-prof_admin user changing any global settings — such as executing the commands `config system global` and `config system admin` or modifying equivalent settings in the GUI — can result in the loss of the prof_admin user's configurations after a system reboot.

To prevent this configuration loss, we recommend the following workaround before upgrading:

1. Log in with a "prof_admin" account.
2. Make a change to a global setting (e.g., config the hostname).
3. Reboot the system.

In summary, ensure that the last change to any global setting is made by a "prof_admin user" before rebooting the system.

Note: This issue has been resolved in versions 7.2.10, 7.4.5, 7.6.1, and later. If you are upgrading from these versions, the recommended workaround is unnecessary.

Admin Password Hash Change (Post-7.2.0)

The admin user password hash is changed from SHA1 to SHA256 starting from version 7.2.0. If you upgrade from versions earlier than 7.2.0, the hash will remain the same as before, but if the admin user changes their password or if new admin users are added, the password hash will be updated to SHA256.

Port 995 Disabled (Pre-7.2.0)

If upgrading from versions earlier than 7.2.0, port 995 will be switched to a disabled state. Remember to manually enable it in **System > Admin > Settings** if required for configuration synchronization.

VLAN and IP Address Conflicts Post-7.2.3 Upgrade

VLAN interfaces/interfaces with overlapping IP addresses and the VIP/Server Policy bound to them cannot be imported (while loading the config file) after upgrading to 7.2.3 and later due to the implementation of an IP overlap check in this release.

Workaround: Downgrade to an earlier version through booting from the alternate partition (see "Booting from the alternate partition"). The old configuration can be restored through this method, edit IP addresses to eliminate overlapping, and then upgrade to 7.6.2.

Maintenance for 6.4.x

We do not provide maintenance for 6.4.x releases unless major errors occur. We recommend upgrading 6.4.x to later versions.

Configuration Reset on Upgrades Before 6.0

When upgrading from releases prior to version 6.0, the "Retain Packet Payload" settings in Log & Report > Log Config > Other Log Settings will be reset to new defaults. This means that the following features — JSON Protection, Syntax-Based Detection, Malicious Bots, Known Good Bots, Mobile API Protection, and API Management — will be disabled. If you had these options enabled prior to the upgrade, please remember to re-enable them if they are still required.

FortiWeb-VM Specific Notes

VM License Upgrade Requirement

- 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 on -VMs deployed on public cloud platforms since 6.3.6. If you upgrade from versions earlier than that, these configurations will be removed.

FortiWeb-VM Troubleshooting for Persistent Issues

If issues persist after the upgrade, consider deploying a new FortiWeb-VM instance with the 7.6.8 image and a trial license. You can download necessary database files from the support site to maintain valid services temporarily.

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

VM Image integrity is also verified when the FortiWeb is booting up. the running OS will generate signatures and compare them with the signatures attached to the image. If the signatures do not match, the running OS will be shutdown.

To download the Customer Service & Support image checksum tool

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

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

Supported upgrade paths

This section discusses the general paths to upgrade FortiWeb from previous releases.

If you are upgrading from a version that is 7.6.1 or lower, then you will need to upgrade to version 7.6.2 before proceeding with subsequent updates.

For example, to upgrade from 7.2.1 to 7.6.5, you will follow the upgrade path below:

7.2.1 → 7.6.2 → 7.6.5

Version 7.6.2 introduces an expanded partition size. Ensure the log disk has at least 1.5 GB of free space before upgrading.

For details, refer to the FortiWeb 7.6.2 Release Notes.

To upgrade to FortiWeb 7.6.8

Upgrade to version 7.6.2 before proceeding to upgrade to version 7.6.8.

To upgrade from FortiWeb 7.6.0/7.6.1 to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 7.4.x to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 7.2.x to 7.6.2

Upgrade directly.

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

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

To upgrade from FortiWeb 7.0.x to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 6.4.x to 7.6.2

Upgrade directly.

To upgrade from FortiWeb 6.3.x to 7.6.2

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 to 7.6.2

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 7.6.8 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.6.8 instead of upgrading to 7.6.8. 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 to 7.6.2

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 7.6.8 from versions earlier than 6.3.0. You need to install FortiWeb-VM 7.6.8 instead of upgrading to 7.6.8. 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 to 7.6.2

Before the upgrade:

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

After the upgrade:

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

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

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

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

To upgrade from FortiWeb 5.4.x to 7.6.2

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 to 7.6.2

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 to 7.6.2

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.
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 7.6.8.
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 18.

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 18.

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 Supported upgrade paths on page 12.

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 19
   - To detach the log disk from a Microsoft Hyper-V VM on page 19
   - To detach the log disk from a KVM VM on page 19
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 19
   - To attach the log disk to a Microsoft Hyper-V VM on page 19
   - To attach the log disk to a KVM VM on page 19
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

We don't recommend performing a downgrade because unexpected results may occur. If you insist on a downgrade, please first contact FortiWeb Technical Support team.

Please be aware that both uploading and switching to a lower version image are considered a downgrade operation.

Data disk size restriction for FortiWeb 400F and 600F

On FortiWeb 400F and 600F appliances equipped with a 64 GB data disk, firmware downgrades to versions lower than 8.0.6, 7.6.8, or 7.4.13 are blocked or will result in a system boot failure. This occurs because legacy firmware images lack the necessary storage configuration logic to recognize or support data disk capacities greater than 16 GB, causing initialization to fail during the bootloader phase.

ML based modules data loss

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

Log compatibility issue

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

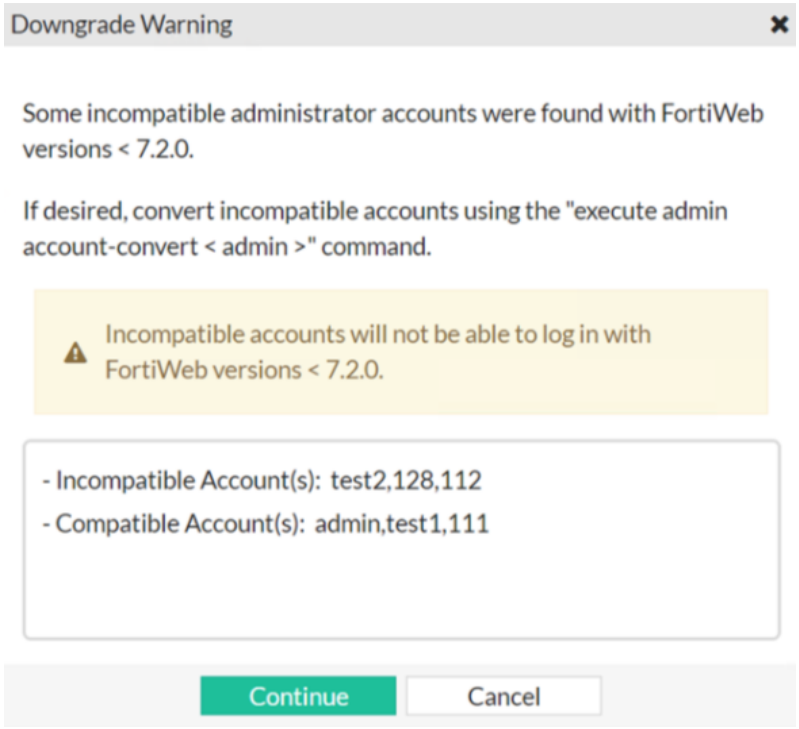
Basic configuration preserved if downgrading to 5.1 or 5.0

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

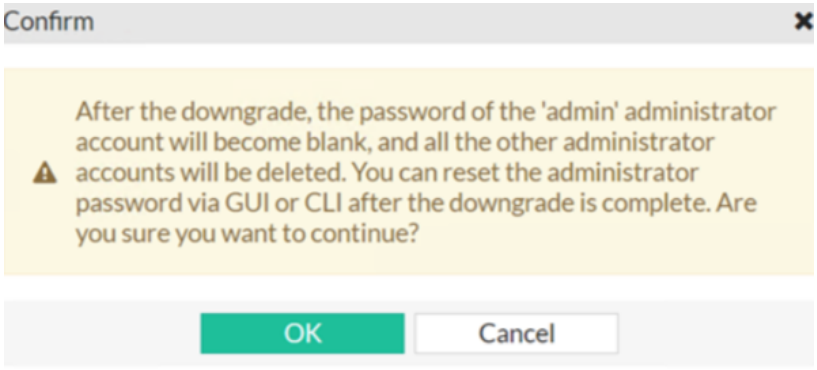
Admin user password hash change

The admin user password hash is changed from sha1 to sha256 since 7.2.0. **System > Admin > Administrators**

If you downgrade to 7.0.x and 7.1.x, you may need to convert password hash otherwise the admin users can't log in with their credentials. The following message will prompt after downgrading:



If you downgrade to versions earlier than 7.0, you need to recreate the lost accounts **System > Admin > Administrators**. The following message will prompt after downgrading:



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

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

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

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

Resolved issues

This section lists issues that have been fixed in version 7.6.8. For inquires about a particular bug, please contact Fortinet Customer Service & Support: https://support.fortinet.com

Bug ID	Description
1289473	High-volume transaction environments may experience severe traffic latency and packet drops due to sudden WAF CPU utilization spikes caused by an unoptimized hash deletion function during `proxyd` active script processing cleanup.
1287453	Public websites protected by FortiWeb may become randomly unreachable with SSL/TLS handshake signature errors due to a deadlocked `proxyd` process caused by a database writing routine incorrectly holding a statistics data list lock during bot mitigation analysis.
1283575	On Oracle Cloud Infrastructure (OCI) platforms, console connection logins using the default Oracle Cloud Identifier (OCID) password fail with a "login incorrect" error. This occurs because an incorrect serial console baud rate misinterprets character inputs during the authentication phase.
1281396	The `proxyd` daemon may crash unexpectedly and trigger a high availability (HA) failover under heavy signature inspection loads. This occurs because an invalid pointer subtraction corrupts signature match offset calculations when using dynamically allocated buffers, resulting in a critical memory buffer overrun.
1279977	Under HTTP/2 traffic loads, the `proxyd` daemon may crash unexpectedly and cause intermittent service interruptions. This occurs because specific HTTP/2 traffic patterns cause a single data frame to be simultaneously linked to two separate tracking lists, resulting in an internal parser failure when processing the duplicate frame references.
1275794	Custom cipher configurations in server pools failed to apply correctly if TLSv1.2 was disabled. This prevented legacy applications from using specific ciphers (such as `AES128-SHA`) for TLSv1.0 connections, causing backend communication to fail after upgrading. The system now allows custom cipher selection regardless of the TLSv1.2 status.
1274541	This occurs because the FTP proxy subsystem incorrectly rewrites server responses based on the address family, generating a standard passive mode 227 response for IPv4 connections instead of maintaining the RFC-compliant 229 Extended Passive Mode format received from the backend server.
1273971	FortiWeb failed to inspect or block HTTPS traffic when operating in **Transparent Inspection** or **Offline Protection** modes. This occurred because the internal cache buffer for the ClientHello packet was limited to 512 bytes, causing decryption failures for modern browsers that send larger handshake requests. The buffer size has been increased to support current SSL/TLS negotiation standards.

Bug ID	Description
1271811	High log disk utilization may occur unexpectedly and fill the /var/log partition even when attack and traffic disk logging are disabled. This occurs due to an underlying application crash within the Antivirus engine (version 7.0.47) that continuously writes core dumps or diagnostic error loops to the local storage file system.
1269957	In High Availability (HA) active-passive or active-active configurations, mutual TLS (mTLS) client certificate verification may fail on the secondary unit with a certificate-expired error. This occurs because the CRL update daemon (crl_updated) does not run on secondary replicas; although the updated Certificate Revocation List (CRL) file content synchronizes from the primary node, the unchanged configuration parameters fail to trigger a server policy reload or update the active CRL groups within the proxy process.
1265487	FortiWeb experienced a parser failure and subsequent traffic disruption (TCP handshake failures) when processing requests containing long strings of special characters. This occurred when the special characters were split across two packets, preventing the parser from correctly validating the sequence across packet boundaries.
1263126	FortiWeb units operating in True Transparent Proxy (TTP) mode experienced intermittent application outages where traffic was received on the ingress port but failed to egress. This resulted from a reference counting error that caused the SSL context to be freed prematurely, leading to a breakdown in SSL processing and forced connection resets.
1262693	The Multi-Factor Authentication (MFA) token input field on the FortiWeb login page displayed characters in plain text. This presented a potential security risk during administrative logins via LDAP or RADIUS. The field has been updated to mask input with asterisks, consistent with standard password field behavior.
1261777	FortiWeb units occasionally sent an immediate `RST,ACK` response to client `SYN` requests without logging the event in traffic or attack logs. This was caused by memory corruption within the **Advanced Bot Protection (ABP)** module, leading to intermittent process crashes.
1259039	The event log warning "Stop HA corefile failover" may be generated unexpectedly and server pools may momentarily flap even when corefile failover is disabled. This occurs because an incorrect node deletion method in the server persistence subsystem causes a `proxyd` daemon crash during session expiration routines.
1255594	The **REST API** returned a generic "500 Internal Server Error" instead of a meaningful error message when a `PUT` request was sent to the `/server-policy/policy` endpoint without the required `mkey` parameter. The API has been updated to handle missing parameters gracefully and return an appropriate "400 Bad Request" response.

Bug ID	Description
1255550	The `proxyd` daemon may hang and cause HTTP/HTTPS traffic to time out, preventing administrative access to the web management portal. This occurs because an infinite loop vulnerability within the biometric detection module prevents client event monitoring for keyboard inputs and mouse clicks from exiting, deadlocking the system when a configuration reload is executed simultaneously.
1254524	SafeNet Luna Hardware Security Module (HSM) integrations fail to add group members or generate Certificate Signing Requests (CSR) due to client incompatibility with newer server partition configurations. This is resolved by updating the internal client to version 10.9.1 and adding a serial number configuration field to ensure accurate partition mapping.
1252805	In environments running Machine Learning (ML) features, the Redis server process may experience a rapid memory leak that drives system utilization to 99% and causes intermittent traffic drops. This occurs because the ML API task and sample processing Lua scripts lack data validation and capacity caps, allowing abnormal tasks and oversized sample sets to accumulate indefinitely within the Redis database.
1251548	License activation fails with a certificate revocation error due to a server hostname mismatch during SSL connections to FortiGuard Distribution Servers (FDS). When anycast is enabled, the system intermittently fails to present the correct Server Name Indication (SNI), leading to a certificate validation failure and missing OCSP stapling data.
1251525	FortiWeb units experienced a total loss of configuration and unexpected HA failovers due to a memory leak in the configuration database service (`cmdbsvr`). The leak occurred during shared memory mapping (mmap), eventually preventing the system from allocating enough memory to load the configuration. This resulted in "CLI parsing errors" during synchronization and service outages.
1248500	FortiWeb units occasionally displayed erroneous Bot Protection error messages on the console following an upgrade or HA failover. These false-positive logs were caused by stale session data and incomplete bot analysis synchronization between cluster members.
1241677	**CAPTCHA** and **reCAPTCHAv3** challenges failed to validate, leading to unexpected client blocks. This was caused by two primary factors: background browser requests for `favicon.ico` triggering unintended **Real Browser Enforcement (RBE)** redirections, and overlapping bot confirmation settings between **Custom Access** and **Threshold-Based Detection policies**. The RBE engine now handles favicon requests as empty data to prevent verification failure, and session management logic has been improved to ensure correct bot confirmation state across multiple policy types.
1239065	The CLI incorrectly rejects valid certificates during installation while the GUI accepts them. This inconsistency is caused by a buffer management error where the content buffer fails to refresh after normalizing a key. Because the system appends data to the existing buffer instead of overwriting it, the resulting

Bug ID	Description
	malformed content causes the CLI validation to fail.
1237875	The ACME daemon incorrectly initiates connections to Let's Encrypt servers even when no certificates are configured. This occurs because the system fails to handle error codes when querying certificate tables across VDOMs; specifically, an unchecked -1 return value from the query API is incorrectly included in the certificate count, triggering unnecessary outbound traffic.
1228883	**SQL/XSS Syntax Based Detection** incorrectly triggered "Arithmetic Operation Based Boolean Injection" blocks for legitimate traffic containing domain names (e.g., `uae.abd-dymgabcd.com`). This regression occurred in version 7.6.5 due to an overly sensitive parsing of hyphenated domain strings. The detection engine has been tuned to correctly distinguish between domain name formatting and arithmetic SQL injection attempts.
1217435	**gRPC** traffic over HTTP/2 experienced intermittent failures and "Bad Firstline" parse errors during streaming sessions. This occurred because the internal parser incorrectly attempted to reset the HTTP/1.1 selector while processing gRPC request bodies, causing subsequent streams to be misinterpreted and closed. The parser logic has been updated to correctly maintain the HTTP/2 state for gRPC body data.
1181025	High CPU utilization spikes up to 90% may occur and require a system reboot when processing connections under heavy traffic or high concurrent session volumes. This occurs because when FortiWeb receives a TCP FIN packet from a client while a large volume of response data is still pending, the socket enters a CLOSE_WAIT state where the `epoll_wait()` system call continuously triggers unhandled `EPOLLOUT` events in an infinite loop.
1173248	FortiWeb incorrectly appends a trailing forward slash (`/`) to the SCEP request path, causing SCEP servers to return a 404 error and triggering a "read certificate error" on the device. This occurs because the client-side URL formatting logic assumes a directory-style path is required, which is incompatible with many modern SCEP servers.
1142492	In High Availability (HA) topologies leveraging dedicated HA management interfaces, FortiWeb fails to establish a Security Fabric connection to the root FortiGate. This occurs because the Security Fabric daemon incorrectly routes authorization and synchronization data through standard traffic interfaces instead of matching the active management router policy specified for downstream Fabric communications.

Known issues

The following issues have been identified in version 7.6.8. To inquire about a particular bug or report a bug, please contact Fortinet Customer Service & Support: https://support.fortinet.com.

Bug ID	Description
1292133	On FortiWeb **400F** and **600F** appliances equipped with a 64 GB data disk, firmware downgrades to versions lower than **8.0.6**, **7.6.8**, or **7.4.13** are blocked or will result in a system boot failure. This occurs because legacy firmware images lack the necessary storage configuration logic to recognize or support data disk capacities greater than 16 GB, causing initialization to fail during the bootloader phase.

www.fortinet.com