FORTINET®

FortiWeb Release Notes

VERSION 6.1.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

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

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

June 19, 2019

FortiWeb 6.1.0 Release Notes

3rd Edition

Change log

03/27/2019	Initial release.
05/22/2019	Update the "Known issues" section.
06/19/2019	Added offline license description in "What's new" section.

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 6.1.0, build 0383.

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 6.1.0 offers the following new features and enhancements.

New features

AI-based machine learning bot detection

FortiWeb now offers AI-based machine learning bot detection that complements the existing signature and threshold based rules. With this new capability, you can deploy FortiWeb to detect sophisticated bots that can sometimes go undetected.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=bot_detection_policy.

AD FS proxy

FortiWeb can act as an AD FS proxy to safely allow access requests to your AD FS server from the internet. Web protection profiles can be applied to protect your AD FS servers from vulnerability exploits, bots, malware uploads, DoS attacks, advanced persistent threats (APTs), and zero day attacks.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=adfs_policies_add.

High Availability (HA) new features

FortiWeb now supports reserving multiple network interfaces on each HA cluster member. The configurations of the reserved interfaces are not synchronized to other members in the HA cluster. You can create static routes and policy routes that are used only by a specific cluster member.

FortiWeb runs health check for the server policies applied to the HA cluster. It reports event logs if the connection between the HA cluster member and the back-end server is not available.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=ha.

TACACS+ support

TACACS+ authentication is now supported for FortiWeb admin users.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=tacacsPlusUsers_view.

Enforcement of new FortiGuard signature updates

FortiWeb now allows to deploy new signature updates in alert mode. This provides a mechanism for customers to first test new signatures in their environment before setting them to block mode.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=stage_signature.

Multiple local certificate support

You can now combine RSA, DSA, and ECDSA certificates in Multi-certificate, and reference it in server policy in Reverse Proxy mode and pserver in True Transparent Proxy mode.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=cert_multi_list.

Q-in-Q VLAN tunneling

In True Transparent Proxy mode, to expand the VLAN space, Q-in-Q is introduced for FortiWeb to stack 802.1Q and 802.1ad headers in the Ethernet frame, so that multiple VLANs can be reused in a core VLAN.

For more information ,see http://help.fortinet.com/fweb/610/index.htm#cshid=interface_list.

Traffic mirror

In Reverse Proxy mode and True Transparent Proxy mode, you can configure FortiWeb to send traffic to third party IPS/IDS devices through network interfaces for traffic monitoring.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=traffic_mirror_view.

SNI Support in offline mode

Offline SNI is introduced in pserver of server pool in Offline Inspection mode or Transparent Inspection mode. FortiWeb uses the server certificate to decrypt SSL-secured connections for the website specified by domain.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=sni.

Comments supported for an attack log

You can now add or edit comments for an attack log.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=log_access.

Flags supported for an attack log

You can set any of the three flags "Action Required", "Action Taken", and "Dismissed" for an attack log.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=log_access.

Enhancements

Web Vulnerability Scan (WVS) module optimized and enhanced

- Show, stop, and repeat buttons are added in **Web Vulnerability Scan Policy** tab.
- Scan templates are added in **Scan Profile** tab to pre-define the scan profile.
- Configuration items are optimized in **Scan Profile > Scan Profile** tab.
- The display interface of **Scan History** tab is modified.
- XML format of scan report is added to support scanner integration.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=wvs_policy_list.

Machine Learning: Enhanced HTTP request method learning algorithm

- Up to 1024 samples are required to build the model.
- A time range can be set to specify the minimum duration of the sample collection period.
- The Trust and Black IP lists are used to limit or block samples from certain IP ranges.
- Support rebuilding the machine learning model for HTTP request methods.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=machine_learning_policy.

Machine Learning: Support database synchronization in Active-Passive mode

In Active-Passive mode, the machine learning database can be synchronized from the master node to the slave node.

Machine Learning: Add additional samples from attack logs

If the attack reported by the anomaly detection model is in fact legitimate traffic, you can now add the triggered pattern to the machine learning model directly. The system rebuilds the model accordingly so that the traffic with the similar characteristics will not be reported as attacks anymore.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=machine_learning_policy.

Add predefined rules for Exchange 2019

Predefined rules are added for Exchange 2019 in Signatures and HTTP Protocol Constraints.

HTTP Protocol Constraints enhancement

FortiWeb now supports setting Threat Weight for Odd and Even Space Attack, Malformed URL, and Illegal Chunk Size.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=protocolConstraints_edit.

Cookie Security enhancement

In Cookie Security Policy, it's now supported to set the Allow Suspicious Cookies option when the Security Mode is Signed.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=cookie_security_policy.

Custom Rule enhancements

FortiWeb has enhanced the Custom Rule to provide more flexible access control:

- Support filtering out the traffic with null HTTP header value.
- Support using regular expression to match the HTTP header name.
- Add Geo IP filter to match the traffic from specified countries.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=advanced_access_rule.

Support forwarding username in the HTTP header

FortiWeb supports setting custom HTTP header in Site Publish Rule to forward username to the back-end server.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=site_publish.

Cookieless support in Site Publish

In Site Publish, it's now supported to authenticate clients without using cookies. HTTP Basic delegation, Kerberos delegation, and No Delegation are allowed for the cookieless authentication.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=site_publish.

Support special characters in user tracking rule

It's now allowed to enter special characters in the Username Field, Password Field, and Log Off URL in the User Tracking Rule. FortiWeb stops detecting Cross-site Scripting attacks for the values of these options.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=userTrackingRule_add.

Route requests based on Geo IP

FortiWeb now supports routing requests to back-end servers based on IP addresses from selected countries.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=http_content_routing_policy.

Support displaying the original source IP and country in traffic logs

FortiWeb displays the original source IP and country in traffic logs if the Use X-Header to Identify Original Client's IP option is enabled in the X-Forwarded-For rule referenced by a server policy.

Add administrative access to aggregation or redundant interfaces

FortiWeb now supports configuring administrative access to aggregation or redundant interfaces.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=interface_edit.

Support generating event logs when concurrent connections reach the limit

When the concurrent connections to the back-end server reach the maximum number, FortiWeb generates warning-level event logs and blocks any further connections.

Support for HTTP Headers in signature exceptions

You can now create signature exceptions for HTTP headers.

For more information, see http://help.fortinet.com/fweb/610/index.htm#cshid=serverProtectionException_view.

Support setting a timeout value for the DNS proxy cache

A CLI command is added to set the timeout value for the DNS proxy cache. The DNS proxy renews the DNS records stored in its cache if the current ones expire.

For more information, see http://help.fortinet.com/fweb/610/cli/index.htm#FortiWeb/CLI-reference/system_network_option.htm.

Firewall policy modifications

- The connection requests from FortiWeb to the DNS server are allowed by default.
- Firewall configurations are allowed to be modified even if the license is expired.

SAN support in Certificate Signing Request (CSR)

FortiWeb supports adding at most ten Subject Alternative Names (SAN) to specify additional host names (domain names, IP addresses, and email addresses).

More SNI policies

FortiWeb now supports up to 1024 SNI policies.

Support setting Alert Only for up to 1024 signatures

It's now supported to set Alert Only for up to 1024 signatures in one administrative domain.

V-zone interface limit lifted

FortiWeb now supports configuring VLAN (including 802.1Q and 802.1ad) and physical interface in one V-zone.

Offline license Support

A FortiWeb license type specially designed for the closed network environment is now available for FortiWeb-VMs on Microsoft Hyper-V.

Support FARGATE on AWS ECS

The FARGATE launch type is supported when deploying FortiWeb container on AWS ECS.

For more information, see https://docs.fortinet.com/vm/aws/fortiweb/6.1/deploying-fortiweb-container-on-ecs/6.1.0/779171/creating-virtual-private-cloud-vpc.

Change and performance notices

Auto learn module removed

Since FortiWeb 6.1 release, auto learn module has been removed, and you can use the machine learning module instead.

File uncompress rule removed

The file uncompress rule is removed. FortiWeb automatically uncompresses the response body accordingly.

Encrypt Log Transmission option removed from Log&Report > Log Policy > FortiAnalyzer Policy

Logs sent to FortiAnalyzer now supports only encrypted transmission. The log transmission mode configuration has been removed from both GUI and CLI console.

Secure Connection option removed from System > Config > FortiSandbox

FortiSandbox now supports only encrypted transmission. The transmission mode configuration has been removed from both GUI and CLI console.

Upgrade instructions

Hardware , VM, and cloud platforms support

Supported Hardware:

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

Supported hypervisor versions:

- VMware vSphere Hypervisor ESX/ESXi 4.0/4.1/5.0/5.1/5.5/6.0/6.5/6.7
- Citrix XenServer 6.2/6.5/7.1
- Open source Xen Project (Hypervisor) 4.0.1, 4.1, 4.2, 4.4
- 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 18.03.1 or higher versions, and the equivalent Docker Engine EE versions

Supported cloud platforms:

- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure)

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

To upgrade from FortiWeb 6.0 or 6.0.x

After the upgrade:

- If you upgrade from 6.0, there might be database compatibility issue after the upgrade, because the MariaDB 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.
- 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.

> If you upgrade from 6.0, or downgrade from 6.1.0 to 6.0, the machine learning data will be cleared.

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 6.1.0, 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 MariaDB 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.

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.

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 MariaDB 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.

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.

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 MariaDB 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.

- 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.

To upgrade from a version previous to FortiWeb 5.3

FWB5.3.exe is a Microsoft Windows executable script that automatically migrates your FortiWeb 5.2.x configuration settings to a 5.3.x configuration.

1. If your version is 5.0.x or 5.1.x, upgrade to FortiWeb 5.2.x.
2. Use **System > Maintenance > Backup & Restore** to back up your FortiWeb configuration. Fortinet recommends that you use the **Backup entire** configuration option.

   Note: If you forget to back up the configuration before you upgrade to FortiWeb 5.3, you can use the **Boot into alternate firmware** option to downgrade to the previous version, and then backup its configuration. For details, see the *FortiWeb Administration Guide*:

   http://docs.fortinet.com/fortiweb/admin-guides
3. To obtain the upgrade script, log in to the Fortinet Customer Service & Support website:

   https://support.fortinet.com

   In the menus at the top of the page, click **Download**, and then click **Firmware Images**.
4. For product, select **FortiWeb**. Then, on the Download tab, navigate to the following folder:

   ```
   /FortiWeb/v5.00/5.3/Upgrade_script/
   ```
5. Download the .zip compressed archive (for example, `FWB5.3Upgrade_v1.9.zip`) to a location you can access from your Windows PC.
6. In Windows, extract the .zip archive's contents, and then use a command line interface to execute the upgrade script.

   For example, in the directory where the file `FWB5.3Upgrade.exe` and your backup configuration file are located, execute the following command:

   ```
   FWB5.3Upgrade.exe -i YOUR_CONFIG_NAME.conf -o 5.3_new.conf
   ```

   The script removes the Domain Server, Physical Server, Server Farm, Content Routing policy configurations and generates a new configuration file named `5.3_new.conf`.
7. Resize your FortiWeb hard disk partitions. See Repartitioning the hard disk.
8. Upgrade to FortiWeb 6.1.0.
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 MariaDB 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.

- 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.

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 17.

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.
4. Continue with the instructions in "Upgrading from previous releases" on page 14.

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 18
   - "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

When you downgrade your FortiWeb 6.1.0 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.

If you downgrade from 6.1.0 to 6.0, the machine learning database will be cleared.

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

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

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

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

Resolved issues

This section lists issues that have been fixed in version 6.1.0. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0544535	Default customizable cipher list is inconsistent between GUI and CLI console.
0543250	Unable to see logs from TA Topology for master application in HA.
0538680	Manage FortiWeb using the aggregate interface by adding the administrative access to the interface.
0537796	Radius server configuration via GUI fails with error "fac01.sepik.local is not a valid IP address or domain name."
0536474	Reply message of Radius server is updated when using site publish rules.
0536436	No log is generated when the concurrent connection number reaches the limitation.
0533844	CSR status is pending due to space characters in the CSR file name.
0502506	Application confd sometimes crashes when saving the FortiWeb configurations.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
0462990	FortiWeb 6.1.0 is no longer vulnerable to the following CVE-Reference: CVE-2017-14191.
0545689	FortiWeb 6.1.0 is no longer vulnerable to the following CVE-Reference: CVE-2019-5590.

Known issues

This section lists known issues in version 6.1.0, 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
0559143	Azure HA: Application Password in Azure Resource Setting will be lost after any HA configuration is changed.
0556937	Alert email policy in Web Anti-Defacement stops working when the firmware version is upgraded from 6.0.2 to 6.1.0.
0545742	If the Request URL and Post URL are the same in an MiTB rule, error may occur.
0542770	Unable to create partition on FortiWeb to connect to HSM server.
0542018	Email policy fails when the users clicks Apply and Test in GUI.
0541244	The system displays an error when users types the regular expression `?` in the CLI.
0540915	Server certificate verification doesn't work well after TSL CA is updated. The new TSL CA can't be reloaded.
0539156	The Regular/Extended Virus can't be updated from FortiGuard.
0537090	For FortiWeb deployed on GCP, the server policies whose HTTP service is 8080 will be lost after upgrading from 601 to 610.
0531337	High Memory usage on FortiWeb 1000E.
0501451	The mysql database is lost after running the `execute db rebuild` command.
0483785	The SFP Transreciever on FortiWeb Finisar FTLF8519P3BNL does not come up on FortiWeb 600D.

FORTINET

High Performance Network Security

Copyright© 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.