FortiWeb Release Notes

VERSION 6.0.2

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

January 31, 2019

FortiWeb 6.0.2 Release Notes

1st Edition

Change log

11/14/2018	Initial release.
01/31/2019	Update the "Known issues" and "Resolved issues" sections.

TABLE OF CONTENTS

Introduction

This document provides information about new and enhanced features, installation instructions, resolved issues, and known issues for FortiWeb 6.0.2, build 0056.

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 provides the following capabilities, among others:

- 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 6.0.2 offers the following new features and enhancements.

Protection for APIs

FortiWeb now provides additional protection to APIs by blocking access not according to the API schema. Current support is for OpenAPI 3.0 framework.

OWASP Top 10 Reference in Logs and FortiView

Policies are now categorized into the OWASP Top 10 list so that the attack logs and FortiView present which of the Top 10 the violation falls under.

Protection for Man-in-the-browser (MiTB) attacks

FortiWeb now provides protection against MiTB. New rules are added, among others, to obfuscate and encrypt certain fields to help protect user sensitive data.

WebSocket Security

FortiWeb now secures WebSocket traffic with a variety of security controls such as allowed formats, frame and message size, and signature detection.

FortiWeb-VM on Oracle Cloud Infrastructure (OCI)

You can now deploy FortiWeb-VM on Oracle Cloud Infrastructure (OCI) with BYOL licensing type. See FortiWeb-VM Deployment Guide for OCI for more information.

Machine Learning: Disable sample collection for Allow methods

You can use the **HTTP Method Setting** to exclude all the Allow Methods from the machine learning model, or use `set allow-method-exceptions` command to specify any Allow Method(s) that you want to exclude. The system will not build machine learning models and detect anomalies based on them. The feature is useful for the HTTP methods which are rarely used but should be treated as normal, such as HEAD, OPTIONS.

Machine Learning: Restrict or exclude sample collection from IP/Range

You can now limit or exclude sample collection to a specific IP or IP range.

Machine Learning: Back up machine learning data

You can include the machine learning data when backing up the entire configuration.

Server Certificate Verification

FortiWeb can now verify the validity of the back end server certificate and block access to the server if its certificate isn't verified.

High Availability support on OpenStack Platform

FortiWeb-VM on OpenStack platform has added support for HA in regular network type and UDP (User Datagram Protocol) tunnel network type.

Support file synchronization in HA mode

In HA mode, when you upload files to the master device, the files can be synchronized to the slave device.

Additional SNMP traps for HA

FortiWeb replaces the SNMP trap "HA heartbeat failed" with the following three traps to indicate more details: "HA cluster status is changed", "HA member join", and "HA member leave".

Support setting engine ID for SNMPv3

FortiWeb supports adding Engine ID in the SNMP traps. Among other benefits, it helps you to easily identify the SNMP traps from the devices in the same HA group.

Add multicast snooping for Vzone

You can enable or disable multicast snooping for Vzone through CLI.

DHCP support for DNS and Gateway IP

If you use DHCP server to allocate IP addresses for network interfaces, the system can automatically get the DNS server address and the gateway IP address from the DHCP server. If you want to use a different DNS server address and gateway IP address, you can enter the addresses manually, then set a higher priority for the manually entered addresses through CLI.

Support `grep` in `get` and `show` commands

You can use `grep` in `get` and `show` commands to further refine the results. For example, entering `get router all | grep -w port1` to display router information only for port1.

Password Control

FortiWeb now provides more granular password control abilities, including forcing password change and locking account upon login failures.

Interval configuration for email sending

We have enhanced the log sending feature. Now the system can send logs based on a configurable interval.

Add Matched field and Matched Pattern in the log file

When forwarding logs to FortiAnalyzer the fields "matched_field" and "matched_pattern" are added.

Docker deployment script enhanced

FortiWeb now supports more port mapping options in the docker deployment script `docker-fwb.sh`. Moreover, with the newly added script `docker-fwb-portmap.sh`, you can have the flexibility to add or delete the container's port mapping after deployment.

Support setting password when deploying FortiWeb-VM docker container

The password setting mechanism is enhanced for FortiWeb-VM docker container. The `-e` parameter is introduced in the `docker-fwb.sh` script to support password setting during deployment.

For FortiWeb docker container on AWS ECS, the default password is the last 12 characters of the task ID if the FWB_ADMIN_PASSWORD variable is not set during the deployment process.

User and Password Configuration on Azure

You can add new user names and passwords, or reset passwords for existing users for FortiWeb-VM instances on Azure GUI. You can also add new user and SSH public key, or reset the SSH public keys for existing users.

Support serial console for FortiWeb-VM instances on Azure

FortiWeb now supports serial console for FortiWeb-VM instances on Azure.

Change and performance notices

`Execute backup cli-config command` is changed

You can use `execute backup cli-config` to back up the core configuration file and `execute backup web-protection-profile` to back up the web protection profiles. The `entire` and `profile` options in `execute backup cli-config` are no longer in use.

The default web administrative port numbers are modified

The default web administrative port numbers of FortiWeb-VM on public cloud platforms were 80 and 443. Now they are changed to 8080 and 8443. This change applies to the FortiWeb-VM deployed on AWS, Azure. GCP, and OCI.

Change password when you first log in to FortiWeb-VM on AWS, GCP and OCI

When you first log in to FortiWeb-VM on AWS, GCP and OCI through CLI or GUI, you need to change the password for the admin account.

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
- 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)
- KVM (Linux kernel 2.6, 3.0, or 3.1)
- OpenStack Liberty 12.0.0
- Docker Engine CE 18.03.1 or higher versions, and the equivalent Docker Engine EE versions

Supported cloud platforms:

- AWS (Amazon Web Services)
  - EC2
  - ECS
- 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 6.0.1

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 database format in 6.0.2.

If you upgrade from 6.0, or downgrade from 6.0.2 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 6.0.2, 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 6.0.2.
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 15.

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

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

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

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

You can use this image to upgrade an HA cluster by following the same procedure you use for a regular firmware upgrade. For details, see "Updating firmware on an HA pair" in the *FortiWeb Administration Guide*:

http://docs.fortinet.com/fortiweb/admin-guides

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

1. Perform a complete backup of your FortiWeb configuration.

Although the repartitioning firmware image automatically saves your FortiWeb configuration, Fortinet recommends that you also manually back it up. For details, see the *FortiWeb Administration Guide*:

http://docs.fortinet.com/fortiweb/admin-guides

2. Contact Fortinet Technical Support to obtain the special repartitioning firmware image: special build 5.4.1, build 6066.

3. Follow one of the same procedures that you use to install or upgrade firmware using a standard image:

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

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

4. Continue with the instructions in "Upgrading from previous releases" 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 16
   - "To detach the log disk from a Microsoft Hyper-V VM" on page 17
   - "To detach the log disk from a KVM VM" on page 17

3. Deploy a new FortiWeb 5.5 or later virtual machine on the same platform.

4. Use the instructions for your hypervisor platform to attach the log disk you detached earlier to the new VM:

   - "To attach the log disk to a Citrix XenServer VM" on page 17
   - "To attach the log disk to a Microsoft Hyper-V VM" on page 17
   - "To attach the log disk to a KVM VM" on page 17

5. Restore the configuration you backed up earlier to the new VM.

6. When you are sure that the new VM is working properly with the required configuration and log data, delete the old VM.

To detach the log disk from a Citrix XenServer VM

1. In Citrix XenCenter, connect to the VM.

2. In the settings for the VM, on the Storage tab, select **Hard disk 2**, and then click **Properties**.

3. For **Description**, enter a new description, and then click **OK**.

4. Select **Hard disk 2** again, and then click **Detach**.

5. Click **Yes** to confirm the detach task.

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

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

To detach the log disk from a KVM VM

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

To attach the log disk to a Citrix XenServer VM

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

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

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

To attach the log disk to a KVM VM

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

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

8. For **Device type**, select **Virtio disk**, for **Storage format**, select **qcow2**, and then click **Finish**.
9. Start the new virtual machine.

Upgrading an HA cluster

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

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

Downgrading to a previous release

When you downgrade your FortiWeb 6.0.2 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 6.0.2 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 6.0.2. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Bug ID	Description
0523090	An issue occurs with the traffic forwarding when the content routing and HTTP and HTTPS servers are used in the server pool.
0522844	If the deployment mode is HTTP content routing, the 503 error message may display. It is caused by the HTTP parsing error when the request package is large.
0521126	The FortiWeb-VM deployed on AWS in China region can't be connected.
0515443	Serial console access is not supported for FortiWeb-VM deployed on Azure.
0515142	The decryption doesn't work for certain policies so that there isn't any traffic or attack logs generated.
0512870	If the policies created in the CLI contain special characters in the name field, they can't be edited in GUI. Error message "Entry not found" is displayed.
0512444	In TTP/TI mode, the configurations set by the `config system setting` command can't be saved.
0512243	Report contains results outside of the configured time range due to the daylight saving changes.
0511960	In case of HA fail-over, the master and slave nodes both crash.
0511933	FortiWeb responds with the status code "503" for the subsequent request coming in the same TCP stream.
0511242	The hasync CPU usage reaches up to 100% on one core randomly.
0511122	Error message displays when `AddressSanitizer` is executed to check the proxyd output.
0510476/0415766	FortiWeb doesn't send alert emails strictly per the interval configured in the Log Policy.
0509322	While executing FortiWeb reboot, MySQL errors occasionally appear on the CLI Console.
0507229	Proxyd Crash: Stack overflow occurs in FortiWeb.
0506199	If the file name or the directory name contains special characters, unexpected elogs are displayed when the `config wad website` command is executed.

Bug ID	Description
0504186	Incorrect country names are displayed in FortiWeb.
0504152	When HTTP/2 is enabled, FortiWeb resets the connection intermittently. Error message such as "This site can’t be reached' is displayed on the user's browser.
0504105	HTTPS has a lot of zombie processes, and FortiWeb can not be accessed via the management port.
0501154	When running "`diag sys ha confd_status`", it shows the slave unit is in initial status.
0500775	When `shutdown` command is executed on the HA master node, the SNMP trap `fwTrapHaHBFail` is not sent as expected.
0495445	FortiWeb does not support getting the DNS server IP from the DHCP server.
0493502	HA can't be set to Tunnel mode on OpenStack platform.
0488212	The **FortiView > Topology** page doesn't display any data.
0479178	Static routes and policy routes are lost after upgrade.

Common Vulnerabilities and Exposures

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

Bug ID	CVE references
0473369	FortiWeb 6.0.2 is no longer vulnerable to the following CVE-Reference: CVE-2015-9251.
0473369	FortiWeb 6.0.2 is no longer vulnerable to the following CVE-Reference: CVE-2012-6708.

Known issues

This section lists known issues in version 6.0.2, 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
0531921	HA synchronization fails on the slave node because `config system fortisandbox-statistics` should only be executed by the sandbox deamon.
0522957	If a server certificate fails the validation and the URL redirection is triggered according to the **Redirect URL** settings, loop redirection will occur.
0507225	Importing/exporting machine learning data in policy level changes the order of domains.
0503587	Machine Learning: CLI crashes when domain-name is added in Machine Learning.
0502898	The error message `"undefined"` appears when the user logs into FortiWeb.
0502506	Application confd sometimes crashes when saving the FortiWeb configuration.
0501154	When running `"diag sys ha confd_status"`, it shows the slave unit is in initial status.
0483785	The SFP Transreciever on FortiWeb Finisar FTLF8519P3BNL does not come up on FortiWeb 600D.

High Performance Network Security