

# FortiWeb Trouble-shooting Guide

VERSION 7.4.3

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET COOKBOOK**

<https://cookbook.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)

April 05, 2024

FortiWeb 7.4.3 Trouble-shooting Guide

1st Edition

# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>7</b>
<b>Troubleshooting outline</b> .....	<b>8</b>
Establishing a system baseline .....	8
Determining the source of the problem .....	8
Planning & access privileges .....	9
<b>Diagnosing server-policy connectivity issues</b> .....	<b>10</b>
Diagnosing Network Connectivity Issues .....	10
Checking hardware connections .....	11
Examining the ARP table .....	11
Checking routing .....	11
Examining the routing table .....	19
Checking port assignments .....	20
Performing a packet trace .....	20
Debugging the packet processing flow .....	21
Diagnosing server-policy access issues .....	21
Server-policy access failure .....	21
Server-policy access failure .....	22
Server policy intermittently inaccessible .....	23
Server-policy outage .....	27
Checking backend server status & issues .....	30
Diagnosing debug flow .....	31
Debugging traffic flow at user level with diagnose commands .....	31
How to capture network packets in FortiWeb .....	33
Error codes displayed when visiting server policy .....	33
Error code 503 (Server Unavailable) .....	33
Error code 500 (Internal Server Error) .....	35
Visiting Server-Policy Has Long Response Time .....	35
Checking Attack/Traffic/Event logs .....	37
FAQ .....	38
How to check attack logs in FortiWeb .....	42
How to check traffic logs in FortiWeb .....	44
Forwarding non-HTTP/HTTPS traffic .....	45
FAQ .....	45
How to forward non-HTTP/HTTPS traffic .....	46
<b>Diagnosing system issues</b> .....	<b>47</b>
System boot-up issues .....	47
Hard disk corruption or failure .....	47
Power supply failure .....	49
System login & authentication issues .....	51
FAQ .....	51
How do I recover the password of the admin account? .....	51
Can one system administrator account manage multiple ADOMs? .....	51
Login common issues .....	52
When an administrator account cannot log in from a specific IP .....	52

Remote authentication query failures .....	52
WebUI authentication issues .....	52
Certificate-based WebUI login failure .....	54
Resetting passwords .....	55
SAML SSO Login issues .....	56
System license issues .....	57
How do I upload and validate a license for FortiWeb-VM? .....	57
Firmware upgrade failures .....	60
How do I reformat the boot device (flash drive) when I restore or upgrade the firmware? .....	60
Troubleshooting firmware upgrade failures .....	60
DB version&update info .....	61
Why did the FortiGuard service update fail? .....	64
How to do DB core files integrity check? .....	64
Cryptographic Key .....	65
FAQ .....	65
Resetting the configuration .....	65
Restoring firmware ("clean install") .....	66
Checking System Resource Issues .....	68
Checking CPU information&Issues .....	68
Checking memory usage .....	73
Diagnosing memory leak issues .....	76
Diagnosing kernel memory leak issues .....	79
Checking disk information & issues .....	81
Retrieving system&debug logs .....	82
Retrieving system logs in backend system .....	82
Customizing and downloading debug logs .....	86
Diagnose Crash & Coredump issues .....	90
Common troubleshooting steps .....	90
Checking core files and basic coredump information .....	90
Collecting core/coredump files and logs .....	93
What to do when coredump files are truncated or damaged .....	97
Diagnose memory violation issues .....	98
<b>Diagnose software function issues .....</b>	<b>101</b>
Server policy .....	101
FAQ .....	102
SSL/TLS .....	108
FAQ .....	108
Diagnosing SSL/TLS handshake failures .....	113
Decrypting SSL packets to analyze traffic issues .....	116
Application Delivery - URL Rewriting .....	123
Why does URL rewriting not work? .....	123
How will multiple rules in one rewrite policy be matched? .....	127
How will multiple match-conditions in one rewrite rule be matched? .....	127
How will FortiWeb handle duplicate headers that are matched by rewrite rules? .....	127
Why sometimes URL rewriting rules cause Loop in browser visiting? .....	127
Application Delivery - Site Publish .....	129

FAQ .....	129
Troubleshoot Site-Publish Issues .....	132
Application Delivery - Caching .....	145
FAQ .....	145
Troubleshoot for caching issues .....	146
Application Delivery - Lua Script .....	149
FAQ .....	149
Application Delivery - Waiting Room .....	150
Web Protection - General Issues .....	152
FAQ .....	152
Web Protection - Known Attack .....	158
FAQ .....	158
Web Protection - Advanced Protection .....	162
FAQ .....	162
Web Protection - Input Validation .....	168
FAQ .....	168
Web Protection - Bot Mitigation .....	169
FAQ .....	169
Web Protection - API Protection .....	170
FAQ .....	170
Web Protection - IP Protection .....	171
FAQ .....	171
Machine Learning - Anomaly Detection .....	172
FAQ .....	173
Machine learning trouble-shooting .....	177
ZTNA troubleshooting and debugging .....	180
HA issues .....	195
FAQ .....	196
HA trouble-shooting .....	199
Log&Report issues .....	216
Common troubleshooting methods for issues that Logs cannot be displayed on GUI .....	216
Step-by-step troubleshooting for log display on FortiWeb GUI failures .....	222
Logs cannot be displayed on FortiAnalyzer .....	224
Replacement message .....	226
FAQ .....	226
<b>Diagnose hardware issues .....</b>	<b>228</b>
Using diagnose commands .....	228
Diagnosing Power Supply issues .....	229
Diagnosing hard disk issues .....	229
Collecting below information for further analysis: .....	230
Diagnosing SSL Card issues .....	231
Diagnosing NIC issues .....	234
<b>System tools &amp; diagnose commands .....</b>	<b>236</b>
Diagnostic Commands .....	236
Diagnose debug .....	236
Diagnose network .....	237

---

Diagnose policy .....	237
Execute Commands .....	238
Execute session-cleanup .....	238
Execute smart .....	238
Ping & Traceroute .....	238
Packet capture .....	239
Packet capture via CLI command .....	240
Packet capture via Web UI .....	244
Diff .....	245
Run backend-shell commands .....	246
Login to backend shell on 6.4 or 6.3 builds .....	247
Login to backend shell on 7.0.0 and later builds .....	247
Use “fnsysctl” in CLI to execute backend commands .....	247
Upload a file to or download a file from FortiWeb .....	248

# Introduction

This guide is composed of the following parts:

## **Troubleshooting outline**

This section outlines some basic concepts and skills for FortiWeb troubleshooting.

## **Diagnosing server-policy connectivity issues**

This section focuses on troubleshooting methods and analysis steps on typical connectivity issues, including failing to visit an access-policy in different conditions, troubleshooting failures of special return code, connecting to backend servers failures, as well as SSL/TLS failures.

## **Diagnosing system issues**

Critical connectivity issues are often caused by system level issues. Sometimes even though connectivity is normal, the system resource becomes abnormal. This may cause potential issues. This section summarizes the front-end and back-end commands to check and analyze system resources, logs, daemon, and kernel crashes.

## **Diagnose software function issues**

This section focuses on diagnosing methods for troubleshooting functional and feature level issues, and also summarizes some frequently asked questions (FAQ).

## **Diagnose hardware issues**

This section focuses on troubleshooting methods for potential hardware issues related to hard disk, power supply, SSL card, etc.

## **System tools & diagnose commands**

This section focuses on the important diagnose commands, explaining the detailed usage and providing some examples, but it doesn't include those commands that are listed and easy to be understood from the CLI Guide description.

# Troubleshooting outline

## Establishing a system baseline

Before you can define an **abnormal** operation, you need to know what **normal** operation is. When there is a problem, a baseline for normal operation helps you to define what is wrong or changed.

Baseline information can include:

- Logging (see "Enabling log types, packet payload retention, & resource shortage alerts" in FortiWeb Administration Guide.)
- Monitoring performance statistics such as memory usage (see "System Resources widget" and "SNMP traps & queries" in FortiWeb Administration Guide.)
- Regular backups of the FortiWeb appliance's configuration (see "Backups" in FortiWeb Administration Guide)

If you accidentally change something, the backup can help you restore normal operation quickly and easily. Backups also can aid in troubleshooting: you can use a tool such as [diff](#) to find the parts of the configuration that have changed.

## Determining the source of the problem

To know which solutions to try, you first need to locate the source of the problem. Occasionally, a problem has more than one possible source. To find a working solution, you will need to determine the exact source of the problem.

- Did FortiWeb's hardware and software both start properly? If not, see [System boot-up issues on page 47](#).
- Are you having Login issues? For details, see [System login & authentication issues on page 51](#).
- What has recently changed?

Do not assume that nothing has changed in the network. Use [Diff](#) and Backups (see "Backup & restore" in FortiWeb Administration Guide) to check if something changed in the configuration, and Logging (see "Logging" FortiWeb Administration Guide) to check if an unusual condition occurred. If the configuration did change, see what the effect is when you roll back the change.

- Does your configuration involve HTTPS?  
If yes, make sure your certificate is loaded and valid.
- Are any web servers down?  
See "Policy Status dashboard" FortiWeb Administration Guide.
- Is a policy disabled?
- Does the problem originate on the camera, FortiWeb, or your computer? There are two sides to every connection. For details, see [Diagnosing Network Connectivity Issues](#).
- Does the problem affect only specific clients or servers? Are they all of the same type?
- Is the problem intermittent or random? Or can you reproduce it reliably, regardless of which camera or computer you use to connect to FortiWeb?

If the problem is intermittent, you can use the "System Resources widget" in FortiWeb Administration Guide to see whether the problem corresponds to FortiWeb processor or RAM exhaustion. For details, see [Diagnosing system issues](#).

You can also view the event log. If there is no event log, someone may have disabled that feature. For details, see "Enabling log types, packet payload retention, & resource shortage alerts" in FortiWeb Administration Guide.

- Is your system under attack?

View the "Attack Log widget" in FortiWeb Administration Guide.

## Planning & access privileges

Create a checklist so that you know what you have tried, and what is left to check.

If you need to contact Fortinet Technical Support, it helps to provide a list of what data you gathered and what solutions you tried. This prevents duplicated efforts, and minimizes the time required to resolve your ticket.

If you need access to other networking equipment such as switches, routers, and servers to help you test, contact your network administrator. Fortinet Technical Support will not have access to this other equipment. However, they may need to ask you to adjust a setting on the other equipment.

If you are not using the `admin` account on FortiWeb, verify that your account has the permissions you need to run all diagnostics.

# Diagnosing server-policy connectivity issues

One of your first tests when configuring a new policy should be to determine whether allowed traffic is flowing to your web servers.

- Is there a server policy applied to the web server or servers FortiWeb was installed to protect? If it is operating in Reverse Proxy mode, FortiWeb will not allow any traffic to reach a protected web server unless there is a matching server policy that permits it.
- If your network utilizes secure connections (HTTPS) and there is no traffic flow, is there a problem with your certificate?
- If you run a test attack from a browser aimed at your website, does it show up in the attack log?

To verify, configure FortiWeb to detect the attack, then craft a proof-of-concept that will trigger the attack sensor. For example, to see whether directory traversal attacks are being logged and/or blocked, you could use your web browser to go to:

```
http://www.example.com/login?user=../../../../..
```

Under normal circumstances, you should see a new attack log entry in the attack log console widget of the system dashboard. For details, see "Attack Log widget" in FortiWeb Administration Guide.

---

<b>Diagnosing Network Connectivity Issues</b> .....	<b>10</b>
<b>Diagnosing server-policy access issues</b> .....	<b>21</b>
<b>Diagnosing debug flow</b> .....	<b>31</b>
<b>Error codes displayed when visiting server policy</b> .....	<b>33</b>
<b>Visiting Server-Policy Has Long Response Time</b> .....	<b>35</b>
<b>Checking Attack/Traffic/Event logs</b> .....	<b>37</b>
<b>Forwarding non-HTTP/HTTPS traffic</b> .....	<b>45</b>

## Diagnosing Network Connectivity Issues

One of your first tests when configuring a new policy should be to determine whether allowed traffic is flowing to your web servers.

- Is there a server policy applied to the web server or servers FortiWeb was installed to protect? If it is operating in Reverse Proxy mode, FortiWeb will not allow any traffic to reach a protected web server unless there is a matching server policy that permits it.
- If your network utilizes secure connections (HTTPS) and there is no traffic flow, is there a problem with your certificate?
- If you run a test attack from a browser aimed at your website, does it show up in the attack log?

To verify, configure FortiWeb to detect the attack, then craft a proof-of-concept that will trigger the attack sensor. For example, to see whether directory traversal attacks are being logged and/or blocked, you could use your web browser to go to:

```
http://www.example.com/login?user=../../../../..
```

Under normal circumstances, you should see a new attack log entry in the attack log console widget of the system dashboard.

## Checking hardware connections

If there is no traffic flowing from the FortiWeb appliance, it may be a hardware problem.

### To check hardware connections

- Ensure the network cables are properly plugged in to the interfaces on the FortiWeb appliance.
- Ensure there are connection lights for the network cables on the appliance.
- Change the cable if the cable or its connector are damaged or you are unsure about the cable's type or quality.
- Connect the FortiWeb appliance to different hardware to see if that makes a difference.
- In the web UI, go to **Status > Network > Interface** and ensure that the link status is up for the interface. If the status is down (down arrow on red circle), click **Bring Up** next to it in the **Status** column.

You can also enable an interface in CLI, for example:

```
config system interface
  edit port2
    set status up
  end
```

If any of these checks solve the problem, it was a hardware connection issue. You should still perform some basic software tests to ensure complete connectivity.

If the hardware connections are correct and the appliance is powered on but you cannot connect using the CLI or web UI, you may be experiencing bootup problems. See [System boot-up issues](#).

## Examining the ARP table

When you have poor connectivity, another good place to look for information is the address resolution protocol (ARP) table. A functioning ARP is especially important in high-availability configurations.

To check the ARP table in the CLI, enter:

```
diagnose network arp list
```

## Checking routing

`ping` and `tracert` are useful tools in network connectivity and route troubleshooting.

Since you typically use these tools to troubleshoot, you can allow ICMP, the protocol used by these tools, in firewall policies and on interfaces only when you need them. Otherwise, disable ICMP for improved security and performance.

By default, the FortiWeb appliance will forward only HTTP/HTTPS traffic to your protected web servers. (That is, routing/IP-based forwarding is disabled.) For information on enabling forwarding of FTP or other protocols, see the `config router setting` command in the *FortiWeb CLI Reference*:

<https://docs.fortinet.com/product/fortiweb/>

By default, FortiWeb appliances will respond to `ping` and `traceroute`. However, if the appliance does not respond, and there are no firewall policies that block it, ICMP type 0 (`ECHO_RESPONSE`) might be effectively disabled.

## To enable ping and traceroute responses from FortiWeb

### 1. Go to **Network > Interface**.

To access this part of the web UI, you must have **Read** and **Write** permission in your administrator's account access profile to items in the **Router Configuration** category. For details, see "[Permissions](#)" on page 1.

### 2. In the row for the network interface which you want to respond to ICMP type 8 (`ECHO_REQUEST`) for `ping` and UDP for `traceroute`, click **Edit**.

A dialog appears.

### 3. Enable **PING** (page 1).



Disabling **PING** (page 1) only prevents FortiWeb from **receiving** ICMP type 8 (`ECHO_REQUEST`) and traceroute-related UDP and responding to it. It does **not** disable FortiWeb CLI commands such as `execute ping` or `execute traceroute` that **send** such traffic.

### 4. If **Trusted Host #1** (page 1), **Trusted Host #2** (page 1), and **Trusted Host #3** (page 1) have been restricted, verify that they include your computer or device's IP address. Otherwise FortiWeb will not respond.

### 5. Click **OK**.

The appliance should now respond when another device such as your management computer sends a `ping` or `traceroute` to that network interface.

## To verify routes between clients and your web servers

### 1. Attempt to connect **through** the FortiWeb appliance, from a client to a protected web server, via HTTP and/or HTTPS.

If the connectivity test fails, continue to the next step.

### 2. Use the `ping` command on both the client and the server to verify that a route exists between the two. Test traffic movement in both directions: from the client to the server, and the server to the client. Web servers do not need to be able to initiate a connection, but must be able to send reply traffic along a return path.



In networks using features such as asymmetric routing, routing success in one direction does **not** guarantee success in the other.

If the routing test **succeeds**, continue with [For application-layer problems, on the FortiWeb, examine the: on page 13](#).

If the routing test **fails**, continue to the next step.

3. Use the `tracert` or `traceroute` command on both the client and the server (depending on their operating systems) to locate the point of failure along the route.

If the route is broken when it reaches the FortiWeb appliance, first examine its network interfaces and routes. To display network interface addresses and subnets, enter the CLI command:

```
show system interface
```

To display all recently-used routes with their priorities, enter the CLI command:

```
diagnose network route list
```

You may need to verify that the physical cabling is reliable and not loose or broken, that there are no IP address or MAC address conflicts or blocklisting, misconfigured DNS records, and otherwise rule out problems at the physical, network, and transport layer.

If these tests **succeed**, a route exists, but you cannot connect using HTTP or HTTPS, an application-layer problem is preventing connectivity.

4. For application-layer problems, on the FortiWeb, examine the:
  - matching server policy and all components it references
  - certificates (if connecting via HTTPS)
  - web server service/daemon (it should be running, and configured to listen on the port specified in the server policy for HTTP and/or HTTPS, for virtual hosts, they should be configured with a correct `Host: name`)

On routers and firewalls between the host and the FortiWeb appliance, verify that they permit HTTP and/or HTTPS connectivity between them.

## Testing for connectivity with ping

The `ping` command sends a small data packet to the destination and waits for a response. The response has a timer that may expire, indicating that the destination is unreachable via ICMP.



Connectivity via ICMP only proves that a route exists. It does **not** prove that connectivity also exists via other protocols at other layers such as HTTP.

---

ICMP is part of Layer 3 on the OSI Networking Model. `ping` sends Internet Control Message Protocol (ICMP) `ECHO_REQUEST` (“ping”) packets to the destination, and listens for `ECHO_RESPONSE` (“pong”) packets in reply.

Some networks block ICMP packets because they can be used in a ping flood or denial of service (DoS) attack if the network does not have anti-DoS capabilities, or because `ping` can be used by an attacker to find potential targets on the network.

Beyond basic existence of a possible route between the source and destination, `ping` tells you the amount of packet loss (if any), how long it takes the packet to make the round trip (latency), and the variation in that time from packet to packet (jitter).

If `ping` shows **some** packet loss, investigate:

- cabling to eliminate loose connections
- ECMP, split horizon, or network loops
- all equipment between the ICMP source and destination to minimize hops

If `ping` shows **total** packet loss, investigate:

- cabling to eliminate incorrect connections
- all firewalls, routers, and other devices between the two locations to verify correct IP addresses, routes, MAC lists, trusted hosts, and policy configurations

If `ping` finds an outage between two points, use `tracert` to locate exactly where the problem is.

## To ping a device from the FortiWeb CLI

1. Log in to the CLI via either SSH, Telnet, or you can ping from the FortiWeb appliance in the **CLI Console** accessed from the web UI.
2. If you want to adjust the behavior of `execute ping`, first use the `execute ping options` command. For details, see the *FortiWeb CLI Reference*:  
<https://docs.fortinet.com/product/fortiweb/>
3. Enter the command:  
`execute ping <destination_ipv4>`

where `<destination_ipv4>` is the IP address of the device that you want to verify that the appliance can connect to, such as `192.168.1.1`.



To verify that routing is bidirectionally symmetric, you should **also** ping the appliance. For details, see [To enable ping and traceroute responses from FortiWeb on page 12](#) and [To ping a device from a Microsoft Windows computer on page 15](#) or [To ping a device from a Linux or Mac OS X computer on page 15](#).

If the appliance **can** reach the host via ICMP, output similar to the following appears:

```
PING 192.0.2.96 (192.0.2.96): 56 data bytes
64 bytes from 192.0.2.96: icmp_seq=0 ttl=253 time=6.5 ms
64 bytes from 192.0.2.96: icmp_seq=1 ttl=253 time=7.4 ms
64 bytes from 192.0.2.96: icmp_seq=2 ttl=253 time=6.0 ms
64 bytes from 192.0.2.96: icmp_seq=3 ttl=253 time=5.5 ms
64 bytes from 192.0.2.96: icmp_seq=4 ttl=253 time=7.3 ms

--- 192.0.2.96 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 5.5/6.5/7.4 ms
```

If the appliance **cannot** reach the host via ICMP, output similar to the following appears:

```
PING 192.0.2.108 (192.0.2.108): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...

--- 192.0.2.108 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

“100% packet loss” and “Timeout” indicates that the host is not reachable.

For details, see the *FortiWeb CLI Reference*:

<https://docs.fortinet.com/product/fortiweb/>

## To ping a device from a Microsoft Windows computer

1. Click the **Start** (Windows logo) menu to open it.  
If the host is running Windows XP, instead, go to **Start > Run...**
2. Type `cmd` then press **Enter**.  
The Windows command line appears.
3. Enter the command:  

```
ping <options_str> <destination_ipv4>
```

where:

- `<destination_ipv4>` is the IP address of the device that you want to verify that the computer can connect to, such as `192.0.2.1`.
- `<options_str>` are zero or more options, such as:
  - `-t`—Send packets until you press Control-C.
  - `-a`—Resolve IP addresses to domain names where possible.
  - `-n x`—Where `x` is the number of packets to send.

For example, you might enter:

```
ping -n 5 192.0.2.1
```

If the computer **can** reach the destination, output similar to the following appears:

```
Pinging 192.0.2.1 with 32 bytes of data:  
Reply from 192.0.2.1: bytes=32 time=7ms TTL=253  
Reply from 192.0.2.1: bytes=32 time=6ms TTL=253  
Reply from 192.0.2.1: bytes=32 time=11ms TTL=253  
Reply from 192.0.2.1: bytes=32 time=5ms TTL=253
```

```
Ping statistics for 192.0.2.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 5ms, Maximum = 11ms, Average = 7ms
```

If the computer **cannot** reach the destination, output similar to the following appears:

```
Pinging 192.0.2.1 with 32 bytes of data:  
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.  
  
Ping statistics for 192.0.2.1:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
"100% loss" and "Request timed out." indicates that the host is not reachable.
```

## To ping a device from a Linux or Mac OS X computer

1. Open a command prompt.



Alternatively, on Mac OS X, you can use the Network Utility application.

---

2. Enter the following command:

```
ping <options_str> <destination_ipv4>
```

where:

- <destination\_ipv4> is the IP address of the device that you want to verify that the computer can connect to, such as 192.0.2.1.
- <options\_str> are zero or more options, such as:
  - -w **y**—Wait **y** seconds for ECHO\_RESPONSE.
  - -c **x**—Where **x** is the number of packets to send.

If the command is not found, you can either enter the full path to the executable or add its path to your shell environment variables. The path to the ping executable varies by distribution, but may be /bin/ping.

If you do **not** supply a packet count, output will continue until you terminate the command with Control-C. For more information on options, enter `man ping`.

For example, you might enter:

```
ping -c 5 -W 2 192.0.2.1
```

If the computer **can** reach the destination via ICMP, output similar to the following appears:

```
PING 192.0.2.1 (192.0.2.1) 56(84) bytes of data.
64 bytes from 192.0.2.1: icmp_seq=1 ttl=253 time=6.85 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=253 time=7.64 ms
64 bytes from 192.0.2.1: icmp_seq=3 ttl=253 time=8.73 ms
64 bytes from 192.0.2.1: icmp_seq=4 ttl=253 time=11.0 ms
64 bytes from 192.0.2.1: icmp_seq=5 ttl=253 time=9.72 ms

--- 192.0.2.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4016ms
rtt min/avg/max/mdev = 6.854/8.804/11.072/1.495 ms
```

If the computer **cannot** reach the destination via ICMP, if you specified a wait and packet count rather than having the command wait for your Control-C, output similar to the following appears:

```
PING 192.0.2.15 (192.0.2.15) 56(84) bytes of data.

--- 192.0.2.15 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 5999ms
"100% packet loss" indicates that the host is not reachable.
```

Otherwise, if you terminate by pressing Control-C (^C), output similar to the following appears:

```
PING 192.0.2.15 (192.0.2.15) 56(84) bytes of data.
From 192.0.2.2 icmp_seq=31 Destination Host Unreachable
From 192.0.2.2 icmp_seq=30 Destination Host Unreachable
From 192.0.2.2 icmp_seq=29 Destination Host Unreachable
^C
--- 192.0.2.15 ping statistics ---
41 packets transmitted, 0 received, +9 errors, 100% packet loss, time 40108ms
pipe 3
"100% packet loss" and "Destination Host Unreachable" indicates that the host is
not reachable.
```

## Testing routes & latency with traceroute

`traceroute` sends ICMP packets to test each hop along the route. It sends three packets to the destination, and then increases the time to live (TTL) setting by one, and sends another three packets to the destination. As

the TTL increases, packets go one hop farther along the route until they reach the destination.

Most `traceroute` commands display their maximum hop count—the maximum number of steps it will take before declaring the destination unreachable—before they start tracing the route. The TTL setting may result in routers or firewalls along the route timing out due to high latency.

Where `ping` only tells you if the signal reached its destination and returned successfully, `traceroute` shows each step of its journey to its destination and how long each step takes. If you specify the destination using a domain name, the `traceroute` output can also indicate DNS problems, such as an inability to connect to a DNS server.

By default, `traceroute` uses UDP with destination ports numbered from 33434 to 33534. The `traceroute` utility usually has an option to specify use of ICMP `ECHO_REQUEST` (type 8) instead, as used by the Windows `tracert` utility. If you have a firewall and you want `traceroute` to work from both machines (Unix-like systems and Windows) you will need to allow **both** protocols inbound through your firewall (UDP ports 33434 - 33534 and ICMP type 8).

## To trace the route to a device from the FortiWeb CLI

1. Log in to the CLI via either SSH, Telnet, or you can ping from the FortiWeb appliance in the **CLI Console** widget of the web UI.
2. Enter the command:

```
execute traceroute {<destination_ipv4> | <destination_fqdn>}
```

where {<destination\_ipv4> | <destination\_fqdn>} is a choice of either the device's IP address or its fully qualified domain name (FQDN).

For example, you might enter:

```
execute traceroute www.example.com
```

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
traceroute to www.fortinet.com (192.0.2.150), 32 hops max, 84 byte packets
 1 192.0.2.87 0 ms 0 ms 0 ms
 2 192.0.2.221 <static-209-87-254-221.storm.ca> 2 ms 2 ms 2 ms
 3 192.0.2.129 <core-2-g0-1-1104.storm.ca> 2 ms 1 ms 2 ms
 4 192.0.2.161 2 ms 2 ms 3 ms
 5 192.0.2.17 <core2-ottawa23_POS13-1-0.net.bell.ca> 3 ms 3 ms 2 ms
 6 192.0.2.234 <core2-ottawatc_POS5-0-0.net.bell.ca> 20 ms 20 ms 20 ms
 7 192.0.2.58 <core4-toronto21_POS0-12-4-0.net.bell.ca> 24 ms 21 ms 24 ms
 8 192.0.2.154 <bx4-toronto63_so-2-0-0-0.net.bell.ca> 8 ms 9 ms 8 ms
 9 192.0.2.145 <bx2-ashburn_so2-0-0.net.bell.ca> 23 ms 23 ms 23 ms
10 192.0.2.9 23 ms 22 ms 22 ms
11 192.0.2.238 <cr2.wswdc.ip.att.net> 100 ms 192.0.2.130 <cr2.wswdc.ip.att.net>
    101 ms 102 ms
12 192.0.2.21 <cr1.cgcil.ip.att.net> 101 ms 100 ms 99 ms
13 192.0.2.121 <cr1.sffca.ip.att.net> 100 ms 98 ms 100 ms
14 192.0.2.118 <cr81.sj2ca.ip.att.net> 98 ms 98 ms 100 ms
15 192.0.2.105 <gar2.sj2ca.ip.att.net> 96 ms 96 ms 96 ms
16 192.0.2.42 94 ms 94 ms 94 ms
17 192.0.2.10 88 ms 87 ms 87 ms
18 192.0.2.130 90 ms 89 ms 90 ms
19 192.0.2.150 <fortinet.com> 91 ms 89 ms 91 ms
20 192.0.2.150 <fortinet.com> 91 ms 91 ms 89 ms
```

Each line lists the routing hop number, the IP address and FQDN (if any) of that hop, and the 3 response times from that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
traceroute to 192.0.2.1 (192.0.2.1), 32 hops max, 84 byte packets
 1 192.0.2.2 0 ms 0 ms 0 ms
 2 192.0.2.10 0 ms 0 ms 0 ms
 3 * * *
 4 * * *
```

The asterisks ( \* ) indicate no response from that hop in the network routing. For details, see the *FortiWeb CLI Reference*:

<https://docs.fortinet.com/product/fortiweb/>

## To trace the route to a device from a Microsoft Windows computer

1. Click the **Start** (Windows logo) menu to open it.  
If the host is running Windows XP, instead, go to **Start > Run...**
2. Type `cmd` then press Enter.  
The Windows command line appears.
3. Enter the command:

```
tracert {<destination_ipv4> | <destination_fqdn>}
```

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
Tracing route to www.fortinet.com [192.0.2.34]
over a maximum of 30 hops:

 1 <1 ms <1 ms <1 ms 192.0.2.2
 2 2 ms 2 ms 2 ms static-192-0-2-221.storm.ca [192.0.2.221]

 3 2 ms 2 ms 22 ms core-2-g0-1-1104.storm.ca [192.0.2.129]
 4 3 ms 3 ms 2 ms 67.69.228.161
 5 3 ms 2 ms 3 ms core2-ottawa23_POS13-1-0.net.bell.ca [192.0.2.17]
(Output abbreviated.)
15 97 ms 97 ms 97 ms gar2.sj2ca.ip.att.net [192.0.2.105]
16 94 ms 94 ms 94 ms 192.0.2.42
17 87 ms 87 ms 87 ms 192.0.2.10
18 89 ms 89 ms 90 ms 192.0.2.130
19 89 ms 89 ms 90 ms fortinet.com [192.0.2.34]
20 90 ms 90 ms 91 ms fortinet.com [192.0.2.34]

Trace complete.
```

Each line lists the routing hop number, the 3 response times from that hop, and the IP address and FQDN (if any) of that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
Tracing route to 192.0.2.1 over a maximum of 30 hops

 1 <1 ms <1 ms <1 ms 192.0.2.2
 2 <1 ms <1 ms <1 ms 192.0.2.10
 3 * * * Request timed out.
 4 * * * Request timed out.
 5 ^C
```

The asterisks ( \* ) and "Request timed out." indicate no response from that hop in the network routing.

## To trace the route to a device from a Linux or Mac OS X computer

1. Open a command prompt.



Alternatively, on Mac OS X, you can use the Network Utility application.

---

2. Enter:

```
tracert /> <destination_ip> | <destination_fqdn>
```

**Note:** the path to the executable may vary by distribution.

If the appliance **has** a complete route to the destination, output similar to the following appears:

```
tracert to www.fortinet.com (192.0.2.34), 30 hops max, 60 byte packets
 1 192.0.2.2 (192.0.2.2) 0.189 ms 0.277 ms 0.226 ms
 2 static-192-0-2-221.storm.ca (192.0.2.221) 2.554 ms 2.549 ms 2.503 ms
 3 core-2-g0-1-1104.storm.ca (192.0.2.129) 2.461 ms 2.516 ms 2.417 ms
 4 192.0.2.161 (192.0.2.161) 3.041 ms 3.007 ms 2.966 ms
 5 core2-ottawa23_POS13-1-0.net.bell.ca (192.0.2.17) 3.004 ms 2.998 ms 2.963 ms
 (Output abbreviated.)
16 192.0.2.42 (192.0.2.42) 94.379 ms 94.114 ms 94.162 ms
17 192.0.2.10 (192.0.2.10) 122.879 ms 120.690 ms 119.049 ms
18 192.0.2.130 (203.78.181.130) 89.705 ms 89.411 ms 89.591 ms
19 fortinet.com (192.0.2.34) 89.717 ms 89.584 ms 89.568 ms
```

Each line lists the routing hop number, the IP address and FQDN (if any) of that hop, and the 3 response times from that hop. Typically a value of <1ms indicates a local router.

If the appliance **does not** have a complete route to the destination, output similar to the following appears:

```
tracert to 192.0.2.1 (192.0.2.1), 30 hops max, 60 byte packets
 1 * * *
 2 192.0.2.10 (192.0.2.10) 4.160 ms 4.169 ms 4.144 ms
 3 * * *
 4 * * *^C
```

The asterisks ( \* ) indicate no response from that hop in the network routing.

Relatedly, if the computer's DNS query cannot resolve the host name, output similar to the following appears:

```
example.lab: Name or service not known
Cannot handle "host" cmdline arg `example.lab' on position 1 (argc 1)
```

## Examining the routing table

When a route does not exist, or when hops have high latency, examine the routing table. The routing table is where the FortiWeb appliance caches recently used routes.

If a route is cached in the routing table, it saves time and resources that would otherwise be required for a route lookup. If the routing table is full and a new route must be added, the oldest, least-used route is deleted to make room.

To check the routing table in the CLI, enter:

```
diagnose network route list
```

## Checking port assignments

If you are attempting to connect to FortiWeb on a given network port, and the connection is expected to occur on a different port number, the attempt will fail. For a list of ports used by FortiWeb, see "[Appendix A: Port numbers](#)" on page 1. For ports used by your own HTTP network services, see "[Defining your network services](#)" on page 1.

## Performing a packet trace

When troubleshooting malformed packet or protocol errors, it helps to look inside the protocol headers of packets to determine if they are traveling along the route you expect, and with the flags and other options you expect.



If you configure virtual servers on your FortiWeb appliance, packets' destination IP addresses will be those IP addresses, not the physical IP addresses (i.e., the IP address of port1, etc.). An ARP update is sent out when a virtual IP address is configured.



For Offline Protection mode, it is usually normal if HTTP/HTTPS packets do not egress. The nature of this deployment style is to listen only, except to reset the TCP connection if FortiWeb detects traffic in violation.

---

If the packet trace shows that packets **are** arriving at your FortiWeb appliance's interfaces but no HTTP/HTTPS packets egress, check that:

- Physical links are firmly connected, with no loose wires
- Network interfaces/bridges are brought up (see "Configuring the network interfaces" in FortiWeb Administration Guide)
- Link aggregation peers, if any, are up (see "Link aggregation" in FortiWeb Administration Guide)
- VLAN IDs, if any, match (see "Adding VLAN subinterfaces" in FortiWeb Administration Guide)
- Virtual servers or V-zones exist, and are enabled (see "Configuring a bridge (V-zone)" and "Configuring virtual servers on your FortiWeb" in FortiWeb Administration Guide)
- Matching policies exist, and are enabled (see "Configuring basic policies" in FortiWeb Administration Guide)
- If using HTTPS, valid server/CA certificates exist (see "How to offload or inspect HTTPS" in FortiWeb Administration Guide)
- IP-layer, and HTTP-layer routes, if necessary, match (see "Adding a gateway" and "Routing based on HTTP content" in FortiWeb Administration Guide)
- Web servers are responsive, if server health checks are configured and enabled (see "Configuring server up/down checks" in FortiWeb Administration Guide)

- Load balancers, if any, are defined (see "Defining your proxies, clients, & X-headers" in FortiWeb Administration Guide)
- Clients are not blocklisted (see "Monitoring currently blocked IPs" in FortiWeb Administration Guide)



For Offline Protection mode, it is usually normal if HTTP/HTTPS packets do not egress. The nature of this deployment style is to listen only, except to reset the TCP connection if FortiWeb detects traffic in violation.

---

If the packet is accepted by the policy but appears to be dropped during processing, see "Debugging the packet processing flow" in FortiWeb Administration Guide.

## Debugging the packet processing flow

If you have determined that network traffic is not entering and leaving the FortiWeb appliance as expected, or not flowing through policies and scans as expected, you can debug the packet flow using the CLI.

For example, the following commands enable debug logs and the logs timestamp, and set other parameters for debug logging:

```
diagnose debug enable
diagnose debug console timestamp enable
diagnose debug application proxy 7
diagnose debug flow filter flow-detail 5
diagnose debug flow trace start
diagnose debug flow filter server-ip 192.0.2.20
```

## Diagnosing server-policy access issues

### Server-policy access failure

1. Check if FortiWeb is accessible:
  - Check the network connectivity stated in [Diagnosing server-policy connectivity issues](#) to guarantee that FortiWeb can be accessed from the client
  - Check if DNS can be resolved successfully and correctly specified to the VIP of server-policy;
  - Bypass CDN/DNS (set a host entry in local machine/pc) and check if FortiWeb VIP is accessible;
    - Add a host entry in local machine/pc:
    - Win: C:\Windows\System32\drivers\etc\hosts
    - Linux: /etc/hosts
    - Or visit with `curl --resolve:`
    - `curl -I http://<domain> --resolve <domain>:<port>:<IP address>`
2. Check configuration on FortiWeb:
  - Check the `opmode` in `show system settings`; (different modes may have special limitation or requirement)

- If HTTP & HTTPS are all enabled;
  - If HTTP/HTTPS service ports are correctly configured or can be successfully accessed;
  - If **Redirect HTTP to HTTPS** is enabled; (if yes, you may disable it and try whether HTTP and HTTPS access has different response);
  - If back-end server is correctly configured: pay special attention to port & SSL, single-server mode;
  - If HTTP2 is enabled; (if yes, you may disable it and test again);
  - If Cache&Compression are enabled; (if yes, you may disable it and test again);
  - If Machine-Learning is enabled; (if yes, you may disable it and test again);
3. Check back-end server status:
    - If health check is ON, check if back-end server status is up & stable;
    - If health check is OFF or it's configured as single-server, visit the back-end server from a client or from the backend shell of FortiWeb to check the actual status of back-end server;
  4. Capture packets on FortiWeb:  
Use **GUI > Network > Packet Capture** or `tcpdump` under CLI/root (or `diagnose network sniffer`) to check:
    - The request from client is correctly received by FortiWeb and forwarded to back-end servers;
    - The TCP packets can be received and TCP connection is established;
    - The SSL handshakes are successful.
    - Check HTTP traffic.
  5. Check if the access is blocked by WAF modules:
    - Check attack logs to see why a request is blocked: main&sub types, signature types&ID, message details&matched pattern.
    - Remove the web protection profile or features included from the server-policy, and visit again;
    - Set `noparse enable` in `server-policy policy` to bypass WAF functions.  
Notes: this option applies to Reverse Proxy or True Transparent Proxy mode only, and please do not enable it on content routing, otherwise content routing will not work.
  6. Collect diagnose output & debug logs for further support analysis:
    - Turn on traffic-log with enable packet-log option to check HTTP request packet details;
    - Diagnose debug flow to check traffic flow processing details;
    - Capture traffic on FortiWeb at the same time and download the pcap files;
    - Turn `/proc/tproxy/debug` levels and check packets process in kernels:
    - Export configuration files and download debug logs via GUI.

## Server-policy access failure

1. Check if FortiWeb is accessible:
  - Check the network connectivity stated in [Diagnosing server-policy connectivity issues](#) to guarantee that FortiWeb can be accessed from the client
  - Check if DNS can be resolved successfully and correctly specified to the VIP of server-policy;
  - Bypass CDN/DNS (set a host entry in local machine/pc) and check if FortiWeb VIP is accessible;  
Add a host entry in local machine/pc:  
Win: C:\Windows\System32\drivers\etc\hosts  
Linux: /etc/hosts

Or visit with `curl --resolve:`  
`curl -I http://<domain> --resolve <domain>:<port>:<IP address>`

2. Check configuration on FortiWeb:
  - Check the `opmode` in `show system settings`; (different modes may have special limitation or requirement)
  - If HTTP & HTTPS are all enabled;
  - If HTTP/HTTPS service ports are correctly configured or can be successfully accessed;
  - If **Redirect HTTP to HTTPS** is enabled; (if yes, you may disable it and try whether HTTP and HTTPS access has different response);
  - If back-end server is correctly configured: pay special attention to port & SSL, single-server mode;
  - If HTTP2 is enabled; (if yes, you may disable it and test again);
  - If Cache&Compression are enabled; (if yes, you may disable it and test again);
  - If Machine-Learning is enabled; (if yes, you may disable it and test again);
3. Check back-end server status:
  - If health check is ON, check if back-end server status is up & stable;
  - If health check is OFF or it's configured as single-server, visit the back-end server from a client or from the backend shell of FortiWeb to check the actual status of back-end server;
4. Capture packets on FortiWeb:
 

Use **GUI > Network > Packet Capture** or `tcpdump` under CLI/root (or `diagnose network sniffer`) to check:

  - The request from client is correctly received by FortiWeb and forwarded to back-end servers;
  - The TCP packets can be received and TCP connection is established;
  - The SSL handshakes are successful. (Refer to [SSL/TLS on page 108](#) for detailed troubleshooting methods)
  - Check HTTP traffic. (Refer to [SSL/TLS on page 108](#) for how to decrypt SSL/TLS packets)
5. Check if the access is blocked by WAF modules:
  - Check attack logs to see why a request is blocked: main&sub types, signature types&ID, message details&matched pattern.
  - Remove the web protection profile or features included from the server-policy, and visit again;
  - Set `noparse enable` in `server-policy policy` to bypass WAF functions.  
 Notes: this option applies to Reverse Proxy or True Transparent Proxy mode only, and please do not enable it on content routing, otherwise content routing will not work.
6. Collect diagnose output&debug logs for further analysis:
  - Turn on traffic-log with `enable packet-log` option to check HTTP request packet details;
  - Diagnose debug flow to check traffic flow processing details;
  - Capture traffic on FortiWeb at the same time and download the pcap files;
  - Turn `/proc/tproxy/debug` levels and check packets process in kernels:
  - Export configuration files and download debug logs via GUI.

## Server policy intermittently inaccessible

If a server-policy is accessible most of the time, but it may become inaccessible sometimes, perform the following steps to trouble shoot.

1. Check if networking connection is stable:
  - Ping continuously from a remote client to see if any failures or long response time;
  - Ping the back-end server from FortiWeb to see if any failures or long response time;
  - Visit the back-end server continuously from a remote client to see if any failures or long response time;
  - Visit the back-end server from FortiWeb to see if any failures or long response time when accessing the server-policy from remote client fails.

2. Check if back-end servers' status in server-pool are stable:

- If server health check is ON, check Event logs to confirm the health check down/up events;
- If server health check is OFF, check the logs on the back-end server (Apache/Nginx logs or other monitor system) if possible;
- Visit the back-end server continuously from FortiWeb to see if any failures or long response time from time to time or when the connectivity issue occurs.

You can use curl on FortiWeb back-end shell to visit the back-end server, and check the response time.

Samples:

```
curl -o /dev/null -s -w %{time_total}\n http://<back-end server_IP>:<port>
curl -v https://<domain/IP>/ -A "check_HTTP" -so /dev/null --resolve
  <domain>:<port>:<IP> -k -w %{time_namelookup}::%{time_connect}::%{time_starttransfer}::%{time_total}::%{speed_download}"\n"
```

You can run a script on FortiWeb back-end shell (upload the script via **System > Maintenance > Backup&Restore > GUI File Download/Upload > Upload** and chmod to add the execute permission) to visit the back-end server periodically and record the return code&response time. However, it's not recommended when traffic is heavy.

3. Check if FortiWeb system has resource shortage;
  - Check FortiWeb event logs to see if there is any high CPU or Memory usage when the issue occurs; Find logs like below in **Log&Report > Event > Filter > Action > check-resource**:

```
CPU usage too high,CPU usage is 64, process cmdbsvr.
```

For more information, see [Checking System Resource Issues](#).

- Check other system logs such as NMON files "debug\_<function name>.txt" to see if CPU or Memory usage were abnormal when the issue occurred;

For information, see [Retrieving system logs in backend system](#).

- Check if a high volume of logs are generated or sent to external logs servers such as FortiAnalyzer. With heavy traffic load, especially high RPS or CPS numbers, the CPU usage may get extremely high if traffic logs are enabled and a high volume of logs are generated, written to disk or sent to FortiAnalyzer or other remote log servers.

In these situations, you can run `diagnose system top` to see if CPU usage of logd, indexd or mysqld is high.

4. Check if the server policy configurations are set as below:

- The deployment-mode is HTTP-content-routing, and;
- **Match Once** is disabled, and;
- **Client Real IP** is enabled, and;
- The **IP/IP Range** of **Client Real IP** is not specified.

Server policy may become intermittently inaccessible with the above configurations. To solve this issue, enable `client-real-ip-random-port` to allow FortiWeb using a random port for the client real IP to connect to back-end servers.

```
config server-policy policy
```

```

edit <policy_name>
  set deployment-mode http-content-routing
  set prefer-current-session disable
  set client-real-ip enable
  set client-real-ip-random-port enable
next
end

```

5. Check if traffic reaches FortiWeb's performance bottlenecks; CPU or Memory exhausted events are often caused by traffic reaching performance bottleneck, traffic burst or DDoS. You can double check with the methods below.
  - Check if any real-time performance numbers are overloaded when the issue occurs. For example, the number of the Concurrent Connection, Connection Per second, Transactions Per second and Throughput.  
For more information, see [Checking CPU information&Issues](#).
  - You can also check other 3rd party network monitor systems (if available) to confirm if there was any traffic bursts, overload or bandwidth exhausted events.

6. Check if the FortiWeb TCP ports used to connect the pserver exhausted;
  1. This issue usually happens when the number of concurrent connections reaches the TCP ports limitation especially when there is only one FortiWeb IP used to connect to a single backend server. The maximum connection number from a single FortiWeb IP to one pserver is 64500.
  2. This issue may also happen when concurrent connections are occupied by a large number of TIME\_WAIT connections. If you find the number of TIME\_WAIT keeps very large, it might be a hint that new TCP connections could hardly be established, thus causing new request failures.
  3. The established concurrent connection number can be found in **Dashboard > Total Connection** or through CLI `diagnose policy total-session list`. And the TIME\_WAIT number can be seen in the backend shell with `netstat`.
  4. Please note that the established connections can be also shown by `netstat`, while the number is doubled because FortiWeb establishes bi-direction connections with the client and pserver respectively.

```

5. /# netstat -antp | grep ESTABLISH | wc -l
19094
/# netstat -antp | grep TIME_WAIT | wc -l
38688
/# netstat -nat | awk '{print $6}' | sort | uniq -c | sort -r
56338 TIME_WAIT
33940 ESTABLISHED
427 SYN_SENT
251 LISTEN
221 FIN_WAIT1
196 FIN_WAIT2
5 SYN_RECV
1 established)
1 Foreign

```

### Solution

To alleviate or solve such issue, you can increase the maximum number of connection by adding IP addresses used to connect to the back-end servers:

- a. Add secondary IPs to the interface connected to the back-end server:  
Secondary IPs are necessary for both below methods.

```

FortiWeb # sho sys interface port1
config system interface
edit "port3"

```

```

set type physical
set ip 10.13.4.254/24
set allowaccess ping ssh snmp HTTP HTTPS FortiWeb-manager
config secondaryip
edit 1
  set ip 10.13.4.253/24
next
edit 2
  set ip 10.13.4.252/24
next
end
end

```

- b. **Method 1:** Enable `ip-src-balance` or `ip6-src-balance` to allow FortiWeb to connect to back-end servers using multiple IPv4 addresses configured as above. This is a global option that affects all server policies. FortiWeb uses round-robin algorithm between all primary&secondary IPs to distribute connections to back-end servers:

```

config system network-option
  set ip-src-balance enable
  set ip6-src-balance enable
End

```

**Method 2:** Enable `client-real-ip` and add available secondary IPs configured above to IP ranges, then traffic matching the specific policy will connect to back-end servers using these secondary IPs added to IP/IP Range:

To ensure FortiWeb receives the server's response, configure FortiWeb as the back-end server's gateway.

This option is available only for Reverse Proxy mode.

```

FortiWeb # show server-policy policy
config server-policy policy
  edit "Test_Policy"
    ...
    set client-real-ip enable
    set real-ip-addr 10.13.4.253
  next
end

```

7. Check if kernel or daemon core dump files are generated when the issue occurred.

Check `core*` or `coredump*` files via **System > Maintenance > Backup & Restore > GUI File Download/Upload** or `"/var/log/gui_upload"`.

Please note that kernel core dump files cannot be displayed by `diagnose debug crashlog show` on 7.0.1 and earlier builds, while they can be shown on 7.0.2 and newer builds.

8. 7. Collect other debug logs or files for further investigation.

- Execute `diagnose system top` and `diagnose system perf` several times to find the top CPU-consuming processes;
- Collect `pstack` information of `proxyd` to check where `proxyd` may stuck at;

On 6.3:

```

FortiWeb # fn sh
/#
/# pidof proxyd
8602

```

```
/# pstack 8602 #replace with the actual proxyd_pid ... ..
```

From 7.0.0 to 7.0.3:

```
FortiWeb # fn pidof proxyd
28913
```

```
FortiWeb # fn pstack 28913 #replace with the actual proxyd_pid
```

... ..

On 7.0 to 7.4.0 builds, you need to configure shell-access and use an SSH client to login to the back-end shell before collecting pstack information. Please refer to [Run backend-shell commands](#) for how to configure shell-access.

```
/# pidof proxyd
```

```
28913
```

```
/# pstack 28913 #replace with the actual proxyd_pid
```

... ..

If you are using FortiWeb 7.4.1 and later, run the following:

```
FortiWeb # diagnose process pidof proxyd
```

```
28913
```

```
FortiWeb # diagnose process pstack 28913 #replace it with the actual proxyd_
pid
```

If proxyd gets stuck for 5 or 60 seconds (on different builds this value varies), watchdog files like "watchdog-proxyd-3991-1658580435.bt" will be generated and will be zipped to the debug log "console\_log.tar.gz". For more information on pstack, see [Retrieving system logs in backend system](#).

- Check the output on console terminal;

Some critical system messages will be printed to console but not written to system logs, so sometimes the console output is very useful for locating the problem. But keep in mind that printing a large amount of messages to console may reduce system performance.

- Download system debug logs, including the one-click download debug log "console\_log.tar.gz" and other logs that require to be manually downloaded.

Most of the necessary system logs are included in the archived "console\_log.tar.gz", while some require to be downloaded manually especially on FortiWeb old versions.

For more information on collecting "console\_log.tar.gz", see [Collecting core/coredump files and logs on page 93](#).

for more information on the content of these logs, see [Retrieving system logs in backend system](#).

The more complete logs you collect, the better it will help for further analysis.

## Server-policy outage

Similar to server policy intermittently inaccessible problems, traffic outage also means service access interruption, but mainly refers to sudden break off, and all services do not respond to requests. So though the troubleshooting steps are similar, there are a few special emphasis.

1. Check if all services on FortiWeb are not available, including the HTTPS/SSH service to the management portal, and the HTTP/HTTPS access to the server policies;
2. Check if reboot, crash or coredump occurred when the issue happened;
  - Check system uptime or event logs to see if power off or reboot ever occurred;
  - Check core\* or coredump\* files via **GUI > System > Maintenance > Backup & Restore > GUI File Download/Upload** or "/var/log/gui\_upload".

Please note that kernel coredump files cannot be displayed by `diagnose debug crashlog show` on 7.0.1 and earlier builds, while they can be shown on 7.0.2 and newer builds.

3. Check if any new operation is performed or configuration are changed before the issue happened; Event logs can be checked for configuration change event, while detailed CLIs are not included.
4. Check if FortiWeb has system resource shortage; Outage may occur when available system resources are extremely low. For example, the memory size of a FortiWeb VM is 4G or lower (not recommended), or the system is configured with too many configuration entries such as server policies or other policies/rules, or OOM (out of memory) happens. Please refer to similar steps in [Server policy intermittently inaccessible](#).
5. Check if traffic reaches FortiWeb's performance bottlenecks  
Check if there is any traffic (CPS/Throughput/Attack) burst or shift when the issue happened; Traffic burst usually leads to high CPU usage, so you can check the Event logs, nmon records, or 3rd party network monitoring history to confirm.  
Please refer to similar steps in [Server policy intermittently inaccessible](#).
6. Collect other debug logs or files for further investigation.

- Execute `diagnose system top` and `diagnose system perf` several times to find the top CPU-consuming processes;
- Collect `pstack` information of `proxyd` to check where `proxyd` may stuck at;

On 6.3:

```
FortiWeb # fn sh
/#
/# pidof proxyd
8602
/# pstack 8602 #replace with the actual proxyd_pid ... ..
```

On 7.0 to 7.4.0 builds:

```
FortiWeb # fn pidof proxyd
28913
FortiWeb # fn pstack 28913 #replace with the actual proxyd_pid ... ..
```

If you are using FortiWeb 7.4.1 and later, run the following:

```
FortiWeb # diagnose process pidof proxyd
28913
FortiWeb # diagnose process pstack 28913 #replace it with the actual proxyd_
pid
```

If `proxyd` gets stuck for 5 seconds, watchdog files like "watchdog-proxyd-3991-1658580435.bt" will be generated and will be zipped to the debug log "console\_log.tar.gz". For more information on `pstack`, see [Retrieving system logs in backend system](#).

- Check the output on console terminal;  
Some critical system messages will be printed to console but not written to system logs, so sometimes the console output is very useful for locating the problem. But keep in mind that printing a large amount of messages to console may reduce system performance.
- Download system debug logs, including the one-click download debug log "console\_log.tar.gz" and other logs that require to be manually downloaded.

Most of the necessary system logs are included in the archived "console\_log.tar.gz", while some require to be downloaded manually especially on FortiWeb old versions.

For more information on collecting "console\_log.tar.gz", see [Collecting core/coredump files and logs on page 93](#).

for more information on the content of these logs, see [Retrieving system logs in backend system](#).

The more complete logs you collect, the better it will help for further analysis.

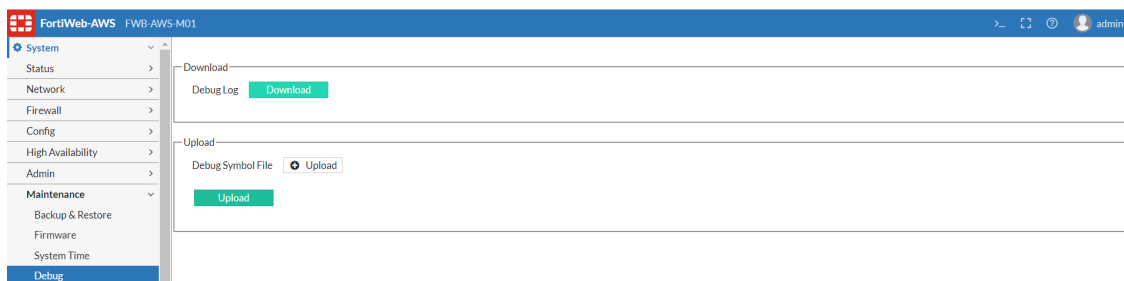
- 7. Check if a high volume of logs generated or sent to FortiAnylazer or other outside log servers (may be CPU consuming)

### Temporary Actions/Solution

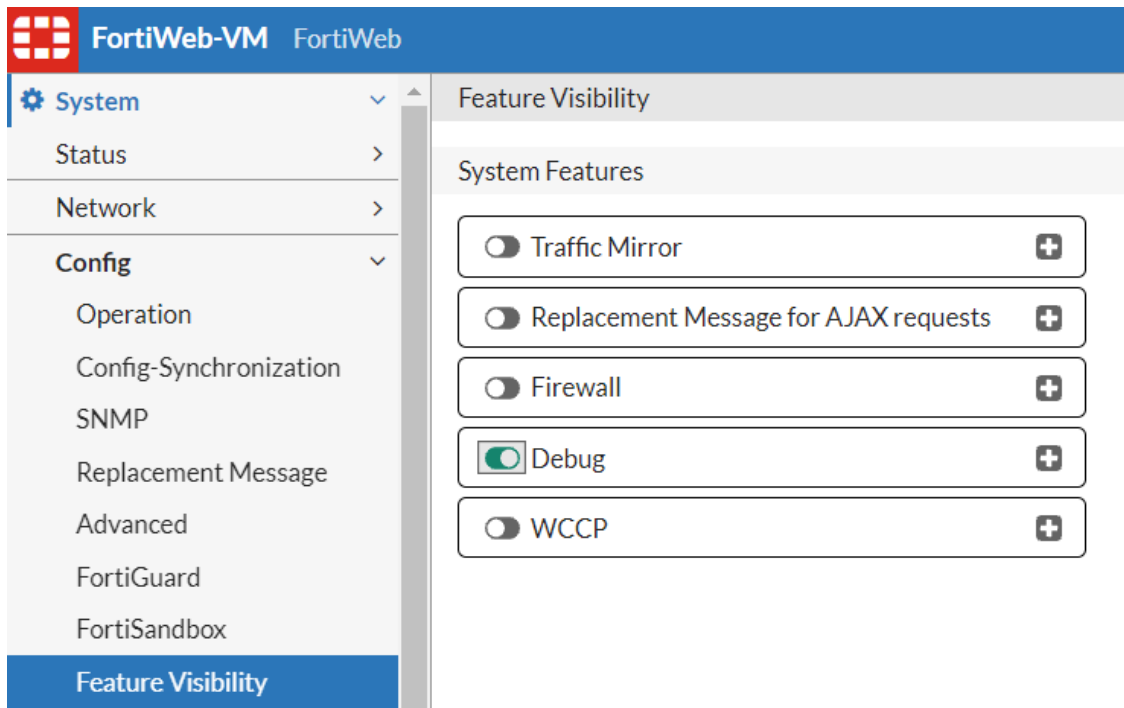
- Check the status of proxyd with `ps | grep proxyd;`
- Execute `exec session-cleanup` to restart proxyd or other processes.  
You can also execute “kill <pidof\_proxyd>” on the backeend shell or “fn kill <pidof\_proxyd>” on the front-end CLI to restart proxyd. Just note that from 7.0.4, you need to enable shell-access and login into the back-end shell for this.

Please to [Run backend-shell commands](#) for how to configure shell-access.

- Collect system and debug logs for further support analysis:
  - Most important system logs can be fetched by one-click download via **GUI > System > Maintenance > Debug > Download:**

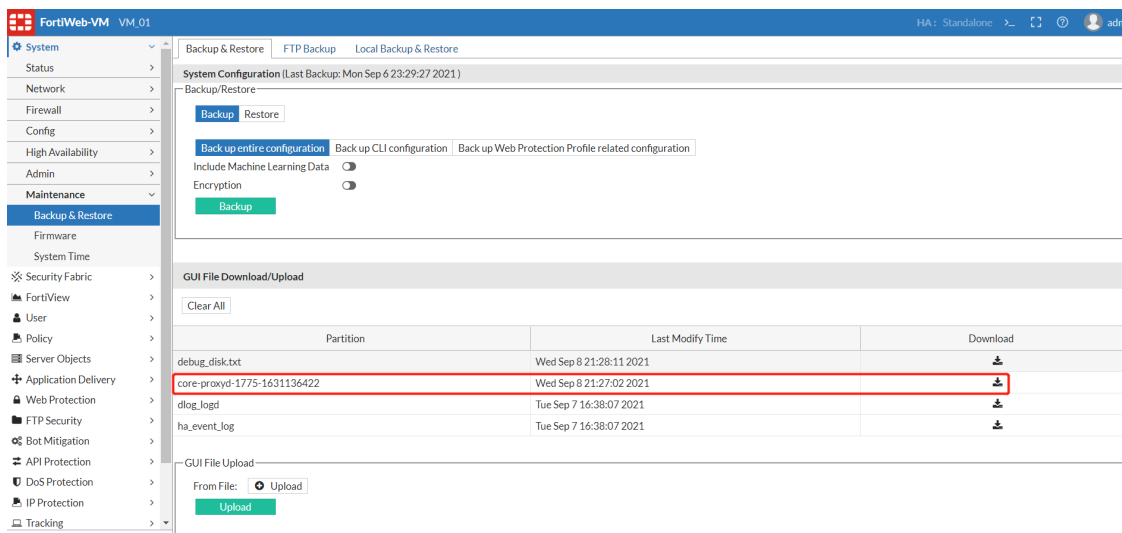


Please note that you need to enable **GUI > System > Config > Feature Visibility > Debug** before seeing such option:



- Sometimes newly-added debug logs may not be included in the archive file downloaded through above method, then it's better to check and download such logs via **GUI > System > Maintenance >**

### Backup & Restore > GUI File Download/Upload:



Similarly, you need to enable the GUI File Download/Upload via CLI:

```
config system settings
  set enable-file-upload enable
end
```

## Checking backend server status & issues

1. Check if the server health-check is ON;

Check current server status with diagnose:

diagnose policy backend back-end server list <Server Pool>

```
FortiWeb # diagnose policy server-pool list root. SP_01
policy(SP_01)
server-pool(RS_01) sp_id(14718170086418654778):
total = 2
server[0]
  server table id: 1
  server random id: 14419242131006337869
  ip: x.x.x.x
  port: 80
  alive:
  1
  session: 0
  idle: 0
  status: 1
  backup: 0
server[1]
  server table id: 2
  server random id: 3111587693898389030
  ip: y.y.y.y
  port: 8080
  alive:
  0
  session: 0
  idle: 0
  status: 1
```

```

    backup: 0
  alive server 1:
    server[0]
  alive backup server 0:

```

2. Check event logs for history status if server-pool health check is ON: **Add Filter > Action > Check-Resource**. You'll see like this:

```
Physical Server 1 [3.89.138.120:80] in server pool RS_01 status change from up to
down
```

3. If server-pool health check is OFF or you doubt the back-end server status is not stable, you may use curl to visit the back-end server (IP or FQDN) under FortiWeb root:

```

/# curl -I http://x.x.x.x/
/# curl -I https://x.x.x.x/
/# curl -I --recursive https://x.x.x.x/

```

**Note:** Using “execute telnettest x.x.x.x:80” under FortiWeb shell or “telnet x.x.x.x:80” may not work well because the HTTP headers cannot be fully sent and parsed.

If you can successfully receive responses from backend servers using Curl, but the health check status still shows OFF, this could be due to network latency. To address this, utilize monitoring or probing tools to track the latency values at various times throughout the day. Then, adjust the health check's timeout value to match the highest recorded network latency. Be aware that this approach will consider backend servers with long network latencies as healthy and include them in traffic processing, potentially degrading user experience. Therefore, it is recommended to set a reasonable timeout value for the health checks to exclude servers with excessively long network latencies from handling traffic.

For how to set health check, see `config server-policy health` in FortiWeb CLI Reference.

4. Check if the request might be limited by “Connection Limit”.

## Diagnosing debug flow

### Debugging traffic flow at user level with diagnose commands

The most commonly used diagnose debug flow commands are combined as below:

#### Reset enabled diagnose settings, turn on debug log output with timestamp

```

diagnose debug reset
diagnose debug timestamp enable

```

#### Add filters and start the flow trace

```

diagnose debug flow filter flow-detail 7 #Enables messages from each packet
  processing module and packet flow traces
diagnose debug flow filter HTTP-detail 7 #HTTP parser details
diagnose debug flow filter module-detail <module> #Specify all or specific module(s)
diagnose debug flow filter server-IP 192.168.12.12 #The VIP in RP mode or the real
  server IP in TP/TI mode
diagnose debug flow filter client-IP 192.168.12.1 #The client IP
diagnose debug flow filter pserver-ip <C.C.C.C> #The real server IP for RP mode only;
  supported from 6.3.21 and 7.0.3
diagnose debug flow trace start
diagnose debug enable

```

#### Stop output

```
diagnose debug flow trace stop
```

Diagnose debug disable

Please note the following:

- Client-IP & server-IP are supported on all 6.3.x and 7.0.x builds; pserver-ip is supported on 6.3.21 and later, and 7.0.x builds.
- The relationship of IP filters (client-IP, server-IP and pserver-IP) for diagnose debug flow are different on different FortiWeb builds. Please check the following description.
- Logical relationship between IP filters on 6.3.20, 7.0.1 and earlier builds:
  - Only client-IP and server-IP are supported on these builds;
  - The logic relationship between the client-IP and server-IP are AND, that is to say, only logs for traffic flows matching both filters will be printed out;
 

Example 1: When only one IP filter, either client-IP or server-IP, is specified, diagnose logs for the traffic flow matching the IP filter will be printed out.

Example 2: When all two IP filters are set, diagnose logs for the traffic flow matching the both IP filters will be printed out.
  - A known limitation is that when TLS 1.3 is deployed on the back-end side (between FortiWeb and the real back-end servers) and any IP flow filter is specified, the SSL pre-master secrets for the back-end side will not be printed out. You need to remove all IP filters to retrieve the TLS 1.3 secrets.
 

Please refer to [Decrypting SSL packets to analyze traffic issues](#) to analyze traffic issues for more details.

- Logical relationship between IP filters on 6.3.21, 7.0.3 and later 7.0.x builds:
  - Three IP filters (client-IP, server-IP and pserver-IP) are supported.
  - If only the front-end IP filters (client-IP or/and server-IP) are configured, the logic relationship between the two front-end filters is AND, but please note now log print only includes front-end TLS key but not back-end TLS key.
  - If both the front-end filters (client-IP or/and server-IP) and the back-end filter pserver-IP is specified, the relationship between the front-end filters and the back-end filter is OR, that is to say the flows either matching the front-end or back-end IP filters will be printed out, and the debug print will include TLS key of both front-end and back-end.

For example, with the following filters specified:

```
diagnose debug flow filter client-IP <A.A.A.A>
diagnose debug flow filter server-IP <B.B.B.B>
diagnose debug flow filter pserver-IP <C.C.C.C>
```

These traffic flows will be printed in diagnose logs:

```
From A.A.A.A to B.B.B.B, and distributed to pserver C.C.C.C
From A.A.A.A to B.B.B.B, and distributed to pserver D.D.D.D #the client side
    flow from A.A.A.A to B.B.B.B will be printed, while the server side flow
    from FortiWeb to D.D.D.D will NOT be printed
From E.E.E.E to F.F.F.F, and distributed to pserver C.C.C.C #the server side
    flow from FortiWeb to C.C.C.C will be printed, while the client side flow
    from E.E.E.E to F.F.F.F will NOT be printed
```

These traffic flows will NOT be printed in diagnose logs:

```
From A.A.A.A to F.F.F.F, and distributed to pserver D.D.D.D
```

- Diagnose debug flow usually results in a large amount of prints and impacts the performance. So if the traffic is heavy or the system resources has been highly occupied, you should enable diagnose debug flow with caution.

Some basic recommendations:

- Enable diagnose in the SSH terminal instead of the Serial Console.
- Under normal circumstances, enabling the filter client-IP only is recommended when debugging issues in the production environment.  
Avoid just specifying the server-IP or pserver-IP, because there might be excessive output on SSH or Console terminals.
- Just set a low log priority level, and don't enable unnecessary filters.  
For example, if you intend to retrieve SSL pre-master secrets to decrypt SSL traffic, just set `diagnose debug flow filter flow-detail 4` and do not enable `module-detail`.
- Don't forget to execute `diagnose debug disable` or `diagnose debug reset` after debug is done.

## How to capture network packets in FortiWeb

Capturing network packets is a useful and direct method when troubleshooting network issues, including TCP connection establishment issues, SSL handshake issues or analyzing HTTP issues.

Usually it's better to enable `diagnose debug flow` and capture packets at the same time, then analyze them together.

## Error codes displayed when visiting server policy

There are some predefined web pages with error codes that will replace HTML pages:

Go to **System > Config > Replacement Message**, click the Predefined or User Defined items to check details.

Name	HTTP Response Code	Description	Modified
<b>Captcha Enforcement</b>			
Captcha Enforcement Page	200	Replacement HTML for Captcha Enforcement Page	
Captcha Block Page	200	Replacement HTML for Captcha Block Page	
<b>Security</b>			
Attack Block Page	500	Replacement HTML for Attack Block Page	
Server Unavailable Message	503	Replacement HTML for Server Unavailable Message	
<b>Site Publish Authentication</b>			
Login Page	200	Replacement HTML for Authentication Login Page	
Token Page	200	Replacement HTML for Token Authentication Page	
RSA SecurID Login Page	200	Replacement HTML for RSA SecurID Authentication Page	
RSA SecurID Challenge Page	200	Replacement HTML for RSA SecurID Challenge Page	
Change Password Page	200	Replacement HTML for Change Password Page	
Account Lockout Page	500	Replacement HTML for Account Lockout Page	
Account Failed Authentication page	500	Replacement HTML for Account Authentication Failed Page	

## Error code 503 (Server Unavailable)

### Possible causes

1. Server Health Check is ON while the back-end server status is Down.
2. Server Health Check is OFF and the back-end server status is Down.
3. When `replacemsg-on-connect-failure` is enabled, and the back-end server status is unstable, in this situation the health check is still UP while the connection to back-end server may be failed.

Please note that the predefined HTTP HC is set with Interval 10, Timeout 3, and Retry\_Times 3, so the back-end server status may change from UP to Down in 23 (the 1st HC starts just when back-end server gets down) or 30 seconds (the back-end server gets down just after the previous HC succeeds).

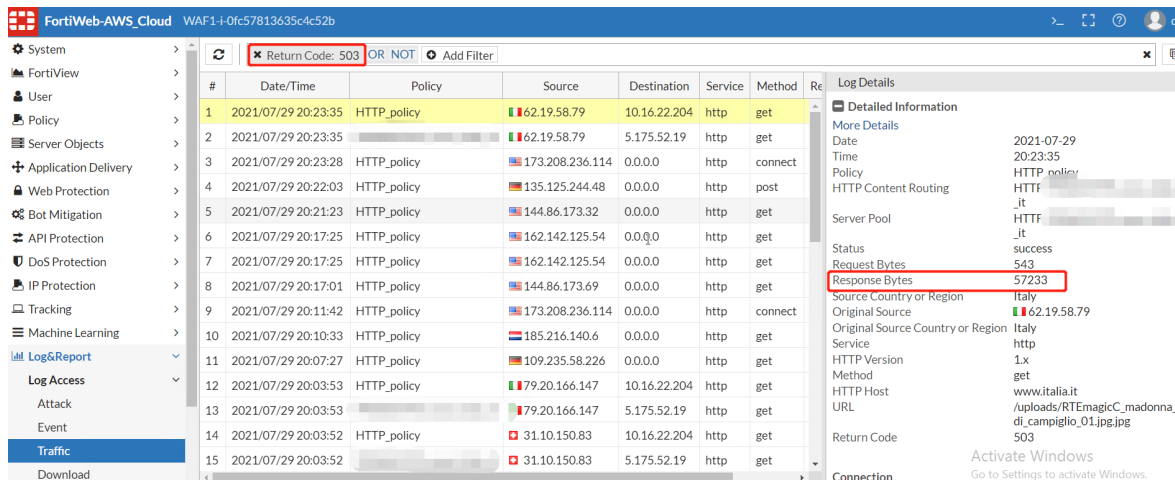
```
config server-policy policy
  edit "1"
    set replacemsg-on-connect-failure enable
    set tcp-conn-timeout 10
  next
end
```

4. Server policy uses content routing without setting default and no content route is matched.

**Troubleshooting methods**

1. How to judge whether the error code 503 is returned by the back-end server or by FortiWeb?
 

The Response Bytes in Traffic log is usually larger than 1K when it's from FortiWeb. This is a simple way (but not always correct) to judge when you cannot see the response page.



2. Disable replacement-on-connect-failure
 

If this option is enabled, when the health check is disabled and the backend server is not responsive, FortiWeb will send the 503 error code to the client.

When enabled, you should also configure `tcp-conn-timeout` to specify the timeout value. When the health check is disabled and the back-end server is not responsive, FortiWeb will wait for such specified time until it sends the 503 error code.

```
config server-policy policy
  edit "1270571790_api_test_com"
    set replacemsg-on-connect-failure disable
  next
end
```

3. Remove the web protection profile or modules included in the server-policy
4. Bypass waf functions:

```
config server-policy policy
  edit "1270571790_api_test_com"
    set noparse enable
  next
```

end

Please note: do not enable noparse on content routing, otherwise content routing will not work.

## Error code 500 (Internal Server Error)

1. This error is returned when the visit is recognized as an attack and denied by WAF modules.
2. Sometimes when WAF features fail to process the traffic flow, for example, when a rewrite/redirect rule is configured but failed to correctly handle the request, FortiWeb will respond 500. In this situation, please collect `diagnose debug flow` logs for further analysis.

## Visiting Server-Policy Has Long Response Time

1. Confirm the issue:
  - Check if the issue only occurs on one policy or impact all policies on the same FortiWeb;
  - Check if the issue happens on HTTP/HTTPS only or both service;
  - Check when the issue happens, if all services on FortiWeb are not available, including the HTTPS/SSH service to the management portal and the HTTP/HTTPS access to the server-policy;
2. Confirm the response time:
  - Use curl to check the response time when visiting the back-end server from FortiWeb, or run a script on FortiWeb to visit the back-end server periodically and record the return code & response time:
 

```
curl -o /dev/null -s -w %{time_total}\n http://<back-end server_IP>:<port>
```

```
curl -v https://<domain/IP>/ -A "check_HTTP" -so /dev/null --resolve <domain>:<port>:<IP> -k -w %{time_namelookup}::%{time_connect}::%{time_starttransfer}::%{time_total}::%{speed_download}"\n"
```

```
#* Added direct.ama01.com:443:3.96.215.58 to DNS cache
* Hostname direct.ama01.com was found in DNS cache
* Trying 3.96.215.58:443...
* Connected to direct.ama01.com (3.96.215.58) port 443 (#0)
... ..
0.000052::0.076644::0.353207::0.353298::0.000
```
  - Use other tools to test and show the response time when visiting from a client:
 

E.g. install a python tool named HTTPStat (actually uses curl with parameters) to better show the test result:

```
test@utmaserver01:~$ sudo pip install HTTPStat
test@utmaserver01:~$ HTTPStat http://<test_domain>/
```

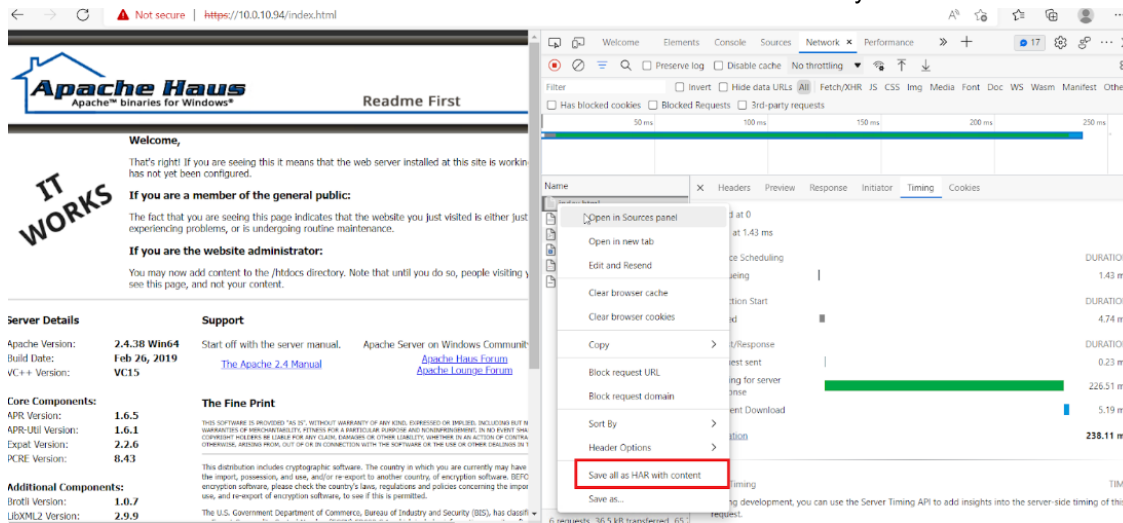
```
Connected to 192.168.12.12:80 from 192.168.12.1:51772
HTTP/1.1 200 OK
Date: Tue, 21 Sep 2021 00:44:51 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: user=runoob
Vary: Accept-Encoding
Content-Length: 593
Content-Type: text/html; charset=UTF-8

Body stored in: /tmp/tmp1go_avt7

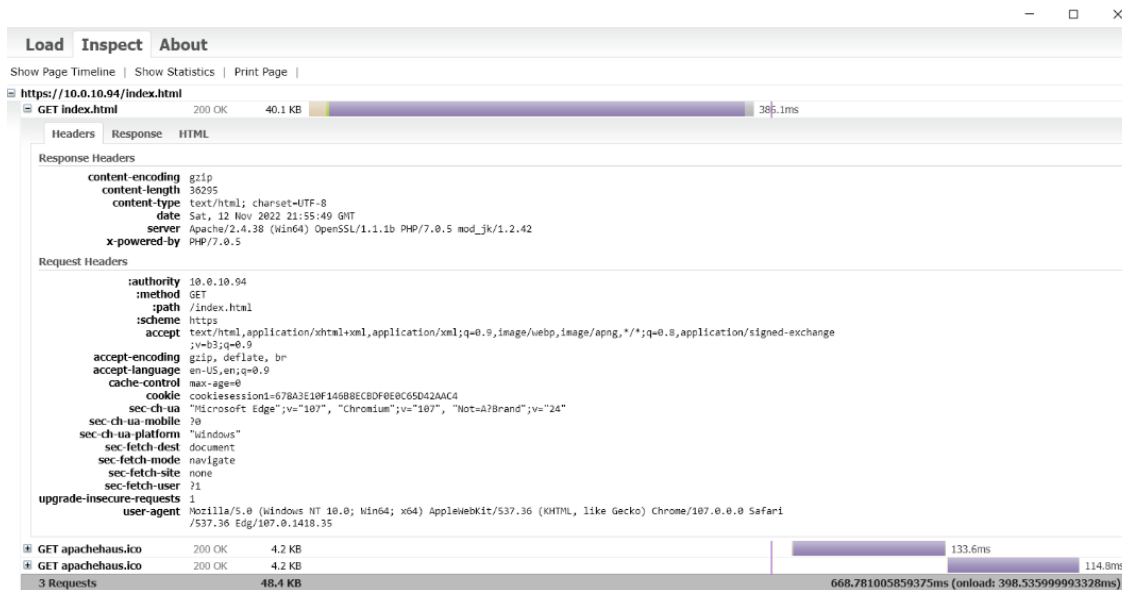
DNS Lookup      TCP Connection  Server Processing  Content Transfer
[ 0ms          | 1ms            | 1ms              | 0ms             ]
  namelookup:0ms          connect:1ms      starttransfer:2ms
                                                                total:2ms
```

- Save the visit as an HAR file:

All major browsers including Chrome, Edge and Firefox support saving a visit as an HAR file. The saved HAR file records the timeline of loading each visited page resource, and can be imported to an HAR viewer such as Chrome extension HTTP Archive Viewer for further analysis.



View with HTTP Archive Viewer:



3. Check the system resources (CPU, Memory usage) when the issue happens;
4. Collect diagnose output and debug logs for further support analysis:
  - Diagnose debug flow to check traffic flow processing details;
  - Capture traffic on FortiWeb at the same time and download the pcap files;
  - Turn `/proc/tproxy/debug` levels and check packets process in kernels;
  - Export configuration files and download debug logs via GUI.
5. Check special configuration and take action to try:
  - If cache or compression is enabled - can disable and test again;
  - Remove web protection profile or modules included from the server-policy, and visit again;
  - Set `noparse enable` in `server-policy policy` to bypass waf functions.

**Note:** Do not enable `noparse` on content routing, otherwise content routing will not work.

## Checking Attack/Traffic/Event logs

Log messages often contain clues that can aid you in determining the cause of a problem. FortiWeb appliances can record log messages when errors occur that cause failures, upon significant changes, and upon processing events.

Depending on the type, log messages may appear in either the event, attack, or traffic logs. The FortiWeb appliance must be enabled to record event, attack, and traffic log messages; otherwise, you cannot analyze the log messages for events of that type. To enable logging of different types of events, go to `Log&Report > Log Config > Other Log Settings`.

During troubleshooting, you may find it useful to reduce the logging severity threshold for more verbose logs, to include more information on less severe events. To configure the severity threshold, go to `Log&Report > Log Config > Global Log Settings`.

## FAQ

### Why do I not see HTTP traffic in the logs?

Successful HTTP traffic logging depends on both FortiWeb configuration and the configuration of other network devices. If you do not see HTTP traffic in the traffic log, ensure that the configuration described in the following tables is correct.

Reverse Proxy mode

Configuration	What to look for	See
Logging	Ensure logging is enabled and configured. By default, logging is not enabled.	"Configuring logging" on page 1
Servers	Ensure that the IP address of your physical server and the IP address of your virtual server are correct.	"Defining your web servers" on page 1 "Configuring virtual servers on your FortiWeb" on page 1
Server policy	Ensure that the server policy associates the appropriate virtual server with the correct physical servers (as members of a server pool).	"Configuring a server policy" on page 1
Network interfaces	Go to Network > Interface and ensure the ports for inbound and outbound traffic are up. Use sniffing (packet capture) to ensure that you can see traffic on both inbound and outbound network interfaces. Ensure that the network interfaces are configured with the correct IP addresses. In a typical configuration, port1 is configured for management (web UI access) and the remaining ports associated with the required subnets.	"Configuring the network interfaces" on page 1 How can I sniff FortiWeb packets (packet capture)? on page 21 (overview) or Packet capture on page 29
VLANs (if used)	Make sure that the VLAN is associated with the correct physical port (Interface setting).	"Adding VLAN subinterfaces" on page 1
Firewalls & routers	Communications between the FortiWeb appliance, clients, protected web servers, and FortiGuard Distribution Network (FDN) require that any routers and firewalls between them permit specific protocols and port numbers.	"Appendix A: Port numbers" on page 1
Load balancers	If the load balancer is in front of FortiWeb, the physical IP addresses on it are the FortiWeb virtual IP addresses. If the Load Balancer is behind the FortiWeb, the FortiWeb physical server is the virtual IP for the load balancer's virtual IP.	"External load balancers: before or after?" on page 1

Configuration	What to look for	See
Web server	Ensure that the web server is up and running by testing it without FortiWeb on the network.	Checking routing on page 39

## Transparent modes

Configuration	What to look for	See
Logging	Ensure logging is enabled and configured. By default, logging is not enabled.	"Configuring logging" on page 1
Server/server pool	Ensure that the configuration for the physical server in the server pool contains the correct IP address.	"Defining your web servers" on page 1 "Creating a server pool" on page 1
Server policy	Ensure that the server policy associates the appropriate virtual server with the correct physical servers (as a member of a server pool).	"Configuring a server policy" on page 1
Bridge (v-zone)	Ensure the v-zone is configured using the correct FortiWeb ports.  In the list of network interfaces (Global > Network > Interface), the Status column identifies interfaces that are members of a v-zone.  To ensure that the bridge is forwarding traffic, in the list of v-zones, under Interface, look for the status "forwarding" following the names of the ports.	"Configuring a bridge (V-zone)" on page 1
VLANs (if used)	Make sure that the VLAN is associated with the correct physical port (Interface setting).	"Adding VLAN subinterfaces" on page 1
Firewalls & routers	Communications between the FortiWeb appliance, clients, protected web servers, and FortiGuard Distribution Network (FDN) require that any routers and firewalls between them permit specific protocols and port numbers.	"Appendix A: Port numbers" on page 1
Web server	Ensure that the web server is up and running by testing it without FortiWeb on the network.	Checking routing on page 39

## Offline mode

Configuration	What to look for	See
Logging	Ensure logging is enabled and configured. By default, logging is not enabled.	"Configuring logging" on page 1

Configuration	What to look for	See
Server/server pool	Ensure that the configuration for the physical server in the server pool contains the correct IP address.	"Defining your web servers" on page 1 "Creating a server pool" on page 1
Server policy	Ensure that the server policy associates the appropriate virtual server with the correct physical servers (as members of a server pool).	"Configuring a server policy" on page 1
Bridge (v-zone)	Ensure the v-zone is configured using the correct FortiWeb ports. In the list of network interfaces (Global > Network > Interface), the Status column identifies interfaces that are members of a v-zone. To ensure that the bridge is forwarding traffic, in the list of v-zones, under Interface, look for the status "forwarding" following the names of the ports.	"Configuring a bridge (V-zone)" on page 1
VLANs (if used)	Make sure that the VLAN is associated with the correct physical port (Interface setting).	"Adding VLAN subinterfaces" on page 1
Network interfaces	Use sniffing (packet capture) to ensure that you can see traffic on both inbound and outbound network interfaces.	"Configuring the network interfaces" on page 1 How can I sniff FortiWeb packets (packet capture)? on page 21 (overview) or Packet capture on page 29
Web server	Ensure that the web server is up and running by testing it without FortiWeb on the network.	Checking routing on page 39

### Why do I see HTTP traffic in the logs but not HTTPS traffic?

Use the following steps to troubleshoot HTTPS traffic logging:

- 1.Ensure FortiWeb has the certificates it needs to offload or inspect HTTPS.
- 2.Use sniffing (packet capture) to look for errors in HTTPS traffic.

### How do I store traffic log messages on the appliance hard disk?

You can configure FortiWeb to store traffic log messages on its hard disk.

In most environments, and especially environments with high traffic volume, enabling this option for long periods of time can cause the hard disk to fail prematurely. Do not enable it unless it is necessary and disable it as soon as you no longer need it.

To enable logging to the hard disk via the CLI, log in using an account with either w or rw permission to the loggrp area and enter the following commands:

```
config log traffic-log
  set disk-log enable
```

Use the following commands to verify the new configuration:

```
get log traffic-log
```

A response that is similar to the following message is displayed:

```
status : enable
packet-log : enable
disk-log : enable
```

Alternatively, use the following command to display a sampling of traffic log messages:

```
diagnose log tlog show
```

A response that is similar to the following message is displayed:

```
Total time span is 39.252285 seconds
  Time spent on waiting is 13.454448 seconds
  Time spent on preprocessing is 3.563218 seconds
  traffic log processed: 69664
```

where:

- Total time span is the total amount of time of the logd process handle logs (that is, receiving messages from other process, filtering messages, outputting in standard format, writing the logs to the local database, and so on).
- Time spent on waiting is the amount of time of the logd process waited to receive messages from other processes.
- Time spent on preprocessing is the amount of time the logd process spent filtering and formatting messages.
- traffic log processed is the total number of logs that the logd process handled in this cycle.

For more information about the `config log traffic-log` and `diagnose log tlog show` commands, see the FortiWeb CLI Reference: <https://docs.fortinet.com/product/fortiweb/>

## Why is the most recent log message not displayed in the Aggregated Attack log?

If recent log messages do not appear in the Aggregated Attack log as expected, complete the following troubleshooting steps:

1. Use the dashboard to see if the appliance is busy.

When FortiWeb generates an attack log, the appliance writes it to and reads it from the hard disk and then updates the logging database.

The process that retrieves Aggregated Attack log information from the database (indexd) has a lower priority than the processes that analyze and direct traffic. Therefore, increased demand for FortiWeb processing resources (for example, when traffic levels increase) can delay updates to the log.

2. Rebuild the logging database.

Events such as a power outage can corrupt the logging database. Use the following command to rebuild it:

```
exec db rebuild
```

### Why is the number of cookies reported in my attack log message different from the number of cookies that message detail displays?

When FortiWeb generates an attack log message because a request exceeds the maximum number of cookies it permits, the message value includes the number of cookies found in the request. In addition, the message details include the actual cookie values.

For performance reasons, FortiWeb limits the size of the attack log message. If the amount of cookie value information exceeds the limit for cookies in the attack log, the appliance displays only some of the cookies the message detail.

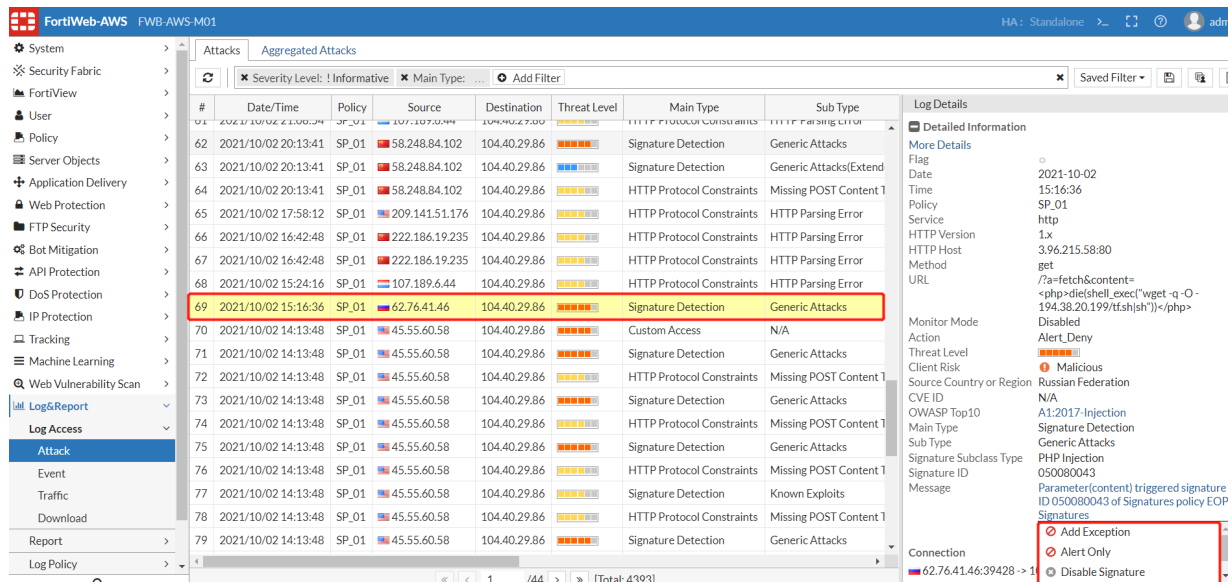
### Why does the attack log message display the virtual server IP address as the destination IP instead of the IP address of the back-end server that was the target of the attack?

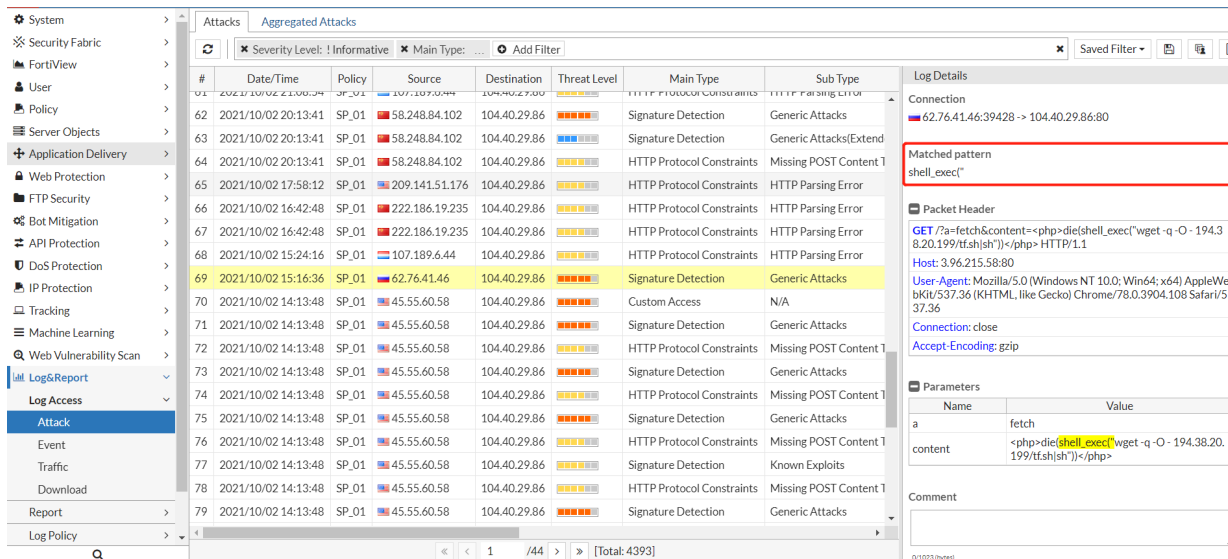
In some cases, FortiWeb blocks attacks before the packet is routed to a server pool member. When this happens, the destination IP is the virtual server IP.

## How to check attack logs in FortiWeb

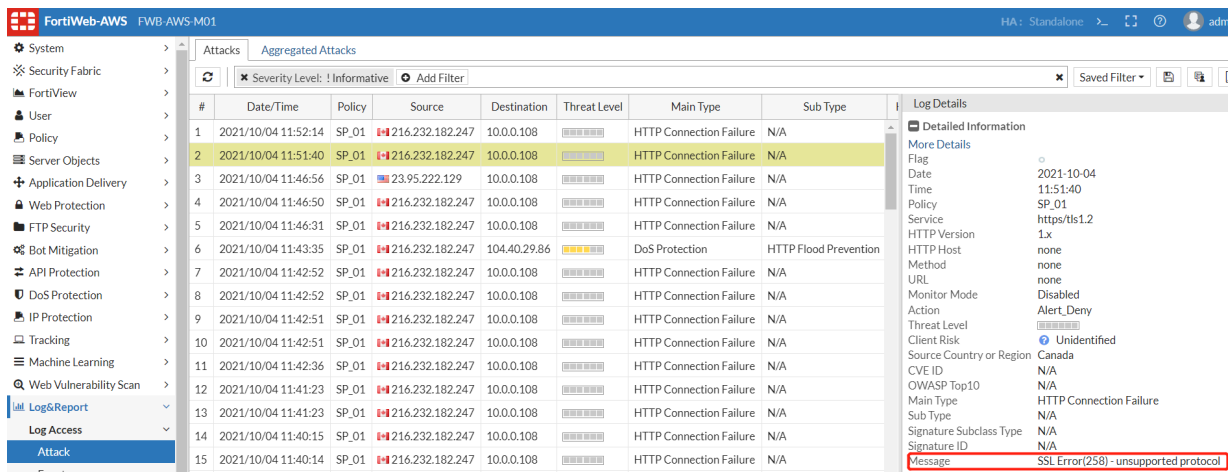
Attack logs keep records of the violations of attack policies, such as server information disclosure, attack signature matches, Dos protection, HTTP protocol constraint, etc.

1. A log for a php injection sample is as below. You can see the attack types, matched pattern, Signature ID and Message. Different attack log types may have particular fields.
2. For some types of logs such as signature, you can create an exception rule or do some other operation by clicking the Message field of attack logs.





3. When you encounter SSL handshake issues, you can disable Ignore SSL Errors in **Log&Report > Log Config > Other Log Settings**, then check SSL failures in attack log messages:



4. Avoid recording log messages using low log severity thresholds

Using low log severity thresholds may cause several negative effects:

1. Frequent local hard disk writing thus likely cause premature failure.
2. Frequent disk I/O may also cause high CPU usage.
3. If syslogs are configured to send to remote log servers, it may also cause heavy network traffic.

This principle applies to attack log, event log, and traffic log.

5. Log rate limit for Dos protection

When FortiWeb is defending your network against a DoS attack, log messages will likely be repetitive and may actually be distracting from other unrelated attacks.

To optimize logging performance and help you to notice important new information, FortiWeb will only make one log entry for these repetitive events in a specific time range. It will not log every occurrence, but only record identical log messages during an ongoing attack.

FortiWeb # show full system advanced

```
config system advanced
  set max-dos-alert-interval 180    #default value
end
```

Type the maximum amount of time that FortiWeb will converge into a single log message during a DoS attack or padding oracle attack.

## How to check traffic logs in FortiWeb

Traffic logs display traffic flow information, such as HTTP/HTTPS requests and responses.

### Enabling Traffic Log

We need to avoid recording highly frequent log types such as traffic logs to the local hard disk for an extended period of time. Excessive logging frequency can cause undue wear on the hard disk and may cause premature failure. So if not necessary or the application traffic is heavy, it's better to keep the traffic log disabled by default.

On 6.4.15 and previous builds, traffic log can be enabled by just turning on the global option via CLI or GUI:

```
FWB # show log traffic-log
config log traffic-log
set status enable
end
```

On 6.4.16 / 7.0.0 and later builds, besides turning on the global option, traffic log needs to be also enabled per server-policy via CLI:

```
FWB # show full-configuration server-policy policy
config server-policy policy
  edit "SP_01"
    set tlog enable
  next
end
```

On 7.0.1 and newer builds, the global traffic-log option is removed from GUI so can be only set via CLI.

### Enabling Traffic Packet Log

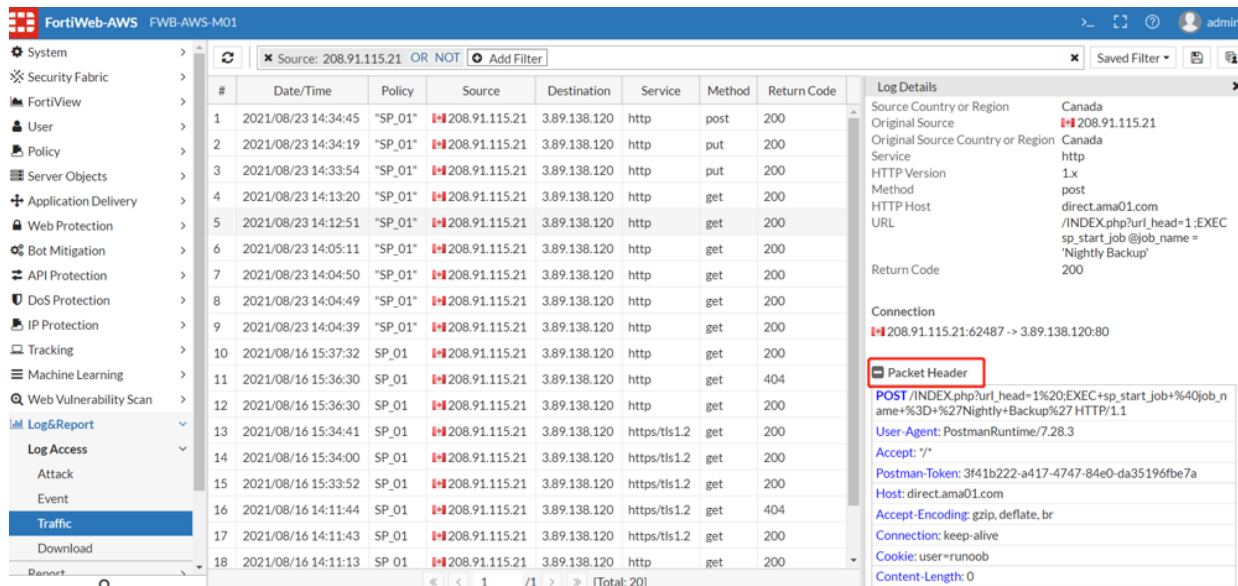
By default, traffic logs only display headers, while you can also enable packet-log to check more details for body contents. It may help you to fine-tune your regular expressions to prevent false negatives, or to examine changes to attack behavior for subsequent forensic analysis.

Unlike attack packet payloads, only HTTP request traffic packets are retained (not HTTP responses), and only the first 4 KB of the payload from the buffer of FortiWeb's HTTP parser.

Please note that retaining traffic packet payloads is resource intensive, so only enable it when necessary.

You can enable this option via **Log&Report > Log Config > Other Log Settings** or CLI as below:

```
FWB # show log traffic-log
config log traffic-log
  set status enable
  set packet-log enable
end
```



## Enabling Retain Packet Payload For

If you enabled retention of packet payloads from FortiWeb’s HTTP parser for attack and traffic logs, you can view a part of the payload as dissected by the HTTP parser, in table form, via the web UI.

Packet payload tables display the decoded packet payload associated with the log message that it caused. This supplements the log message by providing the actual data that triggered the regular expression, which may help you to fine-tune your regular expressions to prevent false positives, or aid in forensic analysis.

## Forwarding non-HTTP/HTTPS traffic

### FAQ

#### Why is FortiWeb not forwarding non-HTTP traffic (for example, RDP, FTP) to back-end servers even though set ip-forward is enabled?

The config router setting command allows you to change how FortiWeb handles non-HTTP/HTTPS traffic when it is operating in Reverse Proxy mode.

When the setting ip-forward is enabled, for any non-HTTP/HTTPS traffic with a destination other than a FortiWeb virtual server (for example, a back-end server), FortiWeb acts as a router and forwards it based in its destination address.

However, any non-HTTP/HTTPS traffic destined for a virtual server on the appliance is dropped.

Therefore, if you require clients need to reach a back-end server using FTP or another non-HTTP/HTTPS protocol, ensure the client uses the back-end server's IP address.

For more detailed information about this setting and a configuration that avoids this problem, see the “Router setting” topic in the FortiWeb CLI Reference:

<https://docs.fortinet.com/product/fortiweb/>

## How to forward non-HTTP/HTTPS traffic

If FortiWeb is operating in Reverse Proxy mode, by default, it does not forward non HTTP/HTTPS protocols to protected servers.

However, you can use the following command to enable IP-based forwarding (routing):

```
config router setting
    set ip-forward {enable | disable}
end
```

## Diagnosing system issues

Sometimes the connectivity issues are caused by abnormal system resource usage, daemon coredump or kernel coredump. This section provides tools and common methods to check system resources and analyze these issues.

---

<b>System boot-up issues</b> .....	<b>47</b>
<b>System login &amp; authentication issues</b> .....	<b>51</b>
<b>System license issues</b> .....	<b>57</b>
<b>Firmware upgrade failures</b> .....	<b>60</b>
<b>DB version&amp;update info</b> .....	<b>61</b>
<b>Cryptographic Key</b> .....	<b>65</b>
<b>Resetting the configuration</b> .....	<b>65</b>
<b>Restoring firmware (“clean install”)</b> .....	<b>66</b>
<b>Checking System Resource Issues</b> .....	<b>68</b>
<b>Retrieving system&amp;debug logs</b> .....	<b>82</b>
<b>Diagnose Crash &amp; Coredump issues</b> .....	<b>90</b>
<b>Diagnose memory violation issues</b> .....	<b>98</b>

### System boot-up issues

While FortiWeb is booting up, hardware and firmware components must be present and functional, or startup will fail. Depending on the degree of failure, FortiWeb may appear to be partially functional. You may notice that you cannot connect at all. If you can connect, you may notice that features such as reports and anti-defacement do not work. If you have enabled logging to an external location such as a Syslog server or FortiAnalyzer, or to memory, you should notice this log message:

```
log disk not mounted
```

Depending on the cause of failure, you may be able to fix the problem.

### Hard disk corruption or failure

FortiWeb appliances usually have multiple disks. FortiWeb stores its firmware (operating system) and configuration files in a flash disk, but most models of FortiWeb also have an internal hard disk or RAID that is used to store non-configuration/firmware data such as logs, reports, and website backups for anti-defacement.

During startup, after FortiWeb loads its boot loader, FortiWeb will attempt to mount its data disk. If this fails due to errors, you will have the opportunity to attempt to recover the disk.

To determine if one of FortiWeb's internal disks may either:

- Have become corrupted
- Have experienced mechanical failure

view the event log. If the data disk failed to mount, you should see this log message:

```
date=2012-09-27 time=07:49:07 log_id=00020006 msg_id=000000000002 type=event
subtype="system" pri=alert device_id=FV-1KC3R11700136 timezone="(GMT-5:00)Eastern
Time(US & Canada)" msg="log disk is not mounted"
```

Connect to FortiWeb's CLI via local console, then supply power. After the boot loader starts, you should see this prompt:

```
Press [enter] key for disk integrity verification.
```

Pressing the Enter key will cause FortiWeb to check the hard disk's file system to attempt to resolve any problems discovered with that disk's file system, and to determine if the disk can be mounted (mounted disks should appear in the internal list of mounted file systems, /etc/mtab). During the check, FortiWeb will describe any problems that it finds, and the results of disk recovery attempts, such as:

```
ext2fs_check_if_mount: Can't detect if filesystem is mounted due to missing mtab
file while determining where /dev/sda1 is mounted.
/dev/sda1: recovering journal
/dev/sda1: clean, 56/61054976 files, 3885759/244190638 blocks
```

If the problem occurs while FortiWeb is still running (or after an initial reboot and attempt to repair the file system), in the CLI, enter:

```
diagnose hardware harddisk list
```

to display the number and names of mounted file systems.

For example, on a FortiWeb 1000C with a single properly functioning internal hard disk plus its internal flash disk, this command should show two file systems:

```
name size(M)
sda 1000204.89
sdb 1971.32
```

where sda, the larger file system, is from the hard disk used to store non-configuration/firmware data.

If that command does not list the data disk's file system, FortiWeb did not successfully mount it. Try to reboot and run the file system check.

If the data disk's file system is listed and appears to be the correct size, FortiWeb could mount it. However, there still could be other problems preventing the file system from functioning, such as being mounted in read-only mode, which would prevent new logs and other data from being recorded. To determine this, enter:

```
diagnose hardware logdisk info
```

to display the count, capacity, RAID status/level, partition numbers, and read-write/read-only mount status.

For example, on a FortiWeb-1000C with a single properly functioning data disk, this command should show:

```
disk number: 1
disk[0] size: 976.76GB
raid level: raid1
partition number: 1
mount status: read-write
```



To prevent file system corruption in the future, and to prevent possible physical damage, always make sure to shut down FortiWeb's operating system before disconnecting the power.

You can also display the status of each individual disk in the RAID array:

```
FortiWeb # diag hardware raid list
disk-number size(M) level
0(OK),1(OK), 1877274 raid1
```

If the file system could not be fixed by the file system check, it may be physically damaged or components may have worn out prematurely. Most commonly, this is caused by either:

Failing to shut down FortiWeb's operating system before disconnecting the power (e.g. someone pulled the power plug while FortiWeb was running)

Logging misconfiguration (e.g. logging very frequent logs like traffic logs or debug logs for an extended period of time to the local hard drive)

For hardware replacement, contact Fortinet Customer Service & Support:

## Power supply failure

If you have supplied power, but the power indicator LEDs are **not** lit and the hardware has not started, the power supply may have failed. Contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

After powering on, if the power indicator LEDs **are** lit but a few minutes have passed and you still cannot connect to the FortiWeb appliance through the network using CLI or the web UI, you can either:

- Restore the firmware. For details, see [Restoring firmware \("clean install"\) on page 66](#). This usually solves most typically occurring issues.
- Verify that FortiWeb can successfully complete bootup.



Always halt the FortiWeb OS before disconnecting the power. Power disruption while the OS is running can cause damage to the disks and/or software.

To verify bootup, connect your computer directly to FortiWeb's local console port, then on your computer, open a terminal emulator such as PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>). Configure it to log all printable console output to a file so that you have a copy of the console's output messages in case you need to send it to Fortinet Customer Service & Support:

<https://support.fortinet.com>

Once connected, power cycle the appliance and observe the FortiWeb's output to your terminal emulator. You will be looking for some specific diagnostic indicators.

1. Are there console messages but text is garbled on the screen? If yes, verify your terminal emulator's settings are correct for your hardware. Typically, however, these are baud rate 9600, data bits 8, parity none, stop bits 1.

2. Does the hardware successfully complete the hardware power on self test (POST) and BIOS memory tests?

If not, you may need to replace the hardware. For assistance, contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

3. Does the boot loader start? You should see a message such as:

```
FortiBootLoader
FortiWeb-1000C (17:52-09.08.2011)
Ver:00010018
Serial number:FV-1KC3R11700094
Total RAM: 3072MB
Boot up, boot device capacity: 1880MB.
Press any key to display configuration menu...
```

If the boot loader does not start, you may need to restore it. For assistance, contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

4. When pressing a key during the boot loader, do you see the following boot loader options?

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
```

Enter G,F,B,Q,or H:

Please connect TFTP server to Ethernet port "1".

If the boot loader does not start, you may need to restore it. For assistance, contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

5. Can the boot loader read the image of the OS software in the selected boot partition (primary or backup/secondary, depending on your selection in the boot loader)? You should see a message such as the following:

```
Reading boot image 2479460 bytes.
Initializing FortiWeb...?
System is started.
```

If not, the image may be corrupted. Reboot and use the boot loader to switch to the other partition, if any. For details, see ["Booting from the alternate partition"](#) on page 1.

If this is not possible, you can restore the firmware. If the firmware cannot be successfully restored, format the boot partition, and try again. For details, see [Restoring firmware \("clean install"\)](#) on page 66.

If you still cannot restore the firmware, there could be either a boot loader or disk issue. Contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

6. Does the login prompt appear? You should see a prompt like this:

```
FortiWeb login:
```

If not, or if the login prompt is interrupted by error messages, restore the OS software. If you recently upgraded the firmware, try downgrading by restoring the **previously** installed, last known good, version.

For details, see [Restoring firmware \(“clean install”\) on page 66](#).

If restoring the firmware does not solve the problem, there could be a data or boot disk issue. Contact Fortinet Customer Service & Support:

<https://support.fortinet.com>

If you **can** see and use the login prompt on the **local** console, but **cannot** successfully establish a session through the **network** (web UI, SSH or Telnet), first examine a backup copy of the configuration file to verify that it is not caused by a misconfiguration. The network interface and administrator accounts must be configured to allow your connection and login attempt. For details, see [“Configuring the network settings”](#) on page 1 and [Trusted Host #1](#) (page 1).

If the configuration appears correct, but no network connections are successful, first try restoring the firmware to rule out corrupted data that could be causing problems. For details, see [Restoring firmware \(“clean install”\) on page 66](#). You can also use this command to verify that resource exhaustion is not the problem:

```
diagnose system top delay 5
```

The process system usage statistics continues to refresh and display in the CLI until you press `q` (quit).

## System login & authentication issues

---

### FAQ

#### How do I recover the password of the admin account?

If you forget the password of the `admin` administrator, you cannot recover it.

However, you can use the local console to reset the password. For details, see "Resetting passwords" in FortiWeb Administration Guide.

Alternatively, you can reset the FortiWeb appliance to its default state (including the default administrator account and password) by restoring the firmware. For details, see "Restoring firmware (“clean install”)” in FortiWeb Administration Guide.

#### Can one system administrator account manage multiple ADOMs?

On 7.0.1 and previous builds, a system administrator can only manage one ADOM.

From 7.0.2, a system administrator can manage multiple ADOMs. Currently you can enable multiple ADOMs via CLI:

```
FortiWeb # show global system admin
name admin user name
admin
dev_adom
sales_adom
FortiWeb # show global system admin dev_adom
```

```
config system admin
  edit "dev_admin"
    set access-profile custom_profile_01
    set domains dev_adom sales_adom #set multiple allowed ADOMs
  next
end
```

## Login common issues

If the person cannot access the login page at all, it is usually actually a connectivity issue (see "Configuring the network settings" in FortiWeb Administration Guide) **unless** all accounts are configured to accept logins only from specific IP addresses.

If an administrator can connect, but cannot log in, even though providing the correct account name and password, and is receiving this error message:

```
Too many bad login attempts or reached max number of logins. Please try again in a
few minutes. Login aborted.
```

This may be because the single administrator mode may have been enabled. For details, see "Enable Single Admin User login" in FortiWeb Administration Guide.

## When an administrator account cannot log in from a specific IP

If an administrator is entering his or her correct account name and password, but cannot log in from some or all computers, examine that account's trusted host definitions (see [Trusted Host #1](#) (page 1)). It should include all locations where that person is allowed to log in, such as your office, but should **not** be too broad.

## Remote authentication query failures

If your network administrators' or other accounts reside on an external server (e.g. Active Directory or RADIUS), first switch the account to be locally defined on the FortiWeb appliance.

If the local account **fails**, correct connectivity between the client and appliance (see [Login common issues on page 52](#)).

If the local account **succeeds**, troubleshoot connectivity between the appliance and your authentication server.

If routing exists but authentication still fails, you can verify correct vendor-specific attributes and other protocol-specific fields by running a packet trace (see "[Packet capture](#)" on page 1).

## WebUI authentication issues

When a local or remote administration account login fails, WebUI usually prompts an authentication failure message.

## Authentication failure. Please try again...

### Possible causes:

- The local or remote administrator name exists, but the password is wrong;
- The remote administrator name exists on FortiWeb, but the remote server (User > Remote Server) is not added into the corresponding Admin User Group; that is to say, the member in the selected group in **User > User Group > Admin Group** is empty.
- The remote administrator name exists on FortiWeb, but the remote server added into the **Admin User Group** is not reachable;
- The remote administrator name exists on FortiWeb, but does not exist on the remote server;
- For remote users, you can capture packets on FortiWeb to see if auth query is sent to the remote server, or check error logs on the remote server to find possible reasons;
- For remote users, you can click the "Test LDAP", "Test Radius" or "Test TACACS+" button in **User > Remote Server > LDAP/Radius/TACACS+ Server** to test if the remote user/administrator can be verified successfully.

If the test fails, the **Test** page will display an error message that can help to make a quick judgment about the possible cause. Possible Cause are listed as below.

### Radius Server:

- **Invalid credentials:** Unsupported Authentication Scheme configured, or used incorrect username or password to test;
- **Failed to receive RADIUS response:** Unreachable server IP/Domain or port configured;
- **Bad response from RADIUS server:** Incorrect Server Secret configured;
- **Radius server auth failed:** Usually occurs when the remote user is set up with an OTP authentication but the Test does not support doing OTP verification in a pop-up window at present. (e.g. FortiToken, Email, EMS, etc.).

### LDAP Server:

- **Failed to connect to LDAP server:** Incorrect server IP / Domain or port configured;
- **Failed to search user DN:** Incorrect Common Name Identifier, Distinguished Name or Filter configured; or correct LDAP server configuration, but used an incorrect username to test;
- **Failed to bind LDAP server:** Correct LDAP server configuration, but used an incorrect password (correct username) to test;
- **Failed to login to LDAP server:** Incorrect User DN or Password configured.

### TACACS+ Server:

- **Invalid Credentials:** Incorrect Server Secret configured; used an incorrect username or password to test, or the remote user is set up with an OTP authentication (e.g. FortiToken, Email, EMS, etc.);
- **Server test error:** Unreachable server IP/Domain configured.



The "Test LDAP", "Test Radius", or "Test TACACS+" button does not work when the remote user is set up on FortiAuthentication with an OTP authentication method such as FortiToken, because OTP auth requires to input the challenge code but the Test window does not support redirecting to a new window.

---

## Invalid username or password

### Possible causes:

- The local administrator name does not exist on FWB.
- The local or remote administrator name exists on FWB, but the password is incorrect.

## Certificate-based WebUI login failure

FortiWeb supports the certificate-based authentication for administrators' Web UI login. FortiWeb controls an administrator's login by verifying its certificate if it connects to the Web UI through HTTPS.

### Common configuration flow for PKI user (Certificate based WebUI login)

1. Upload the CA's certificate of the administrator's certificate.
2. Create a PKI user.
3. Add the PKI user to an Admin group.
4. Apply the Admin group to an administrator

### Certificate based WebUI Login Logic:

- If you connect to the Web UI through HTTPS, FortiWeb first verifies the certificate you provided.
  - If your certificate is valid, then your access to Web UI will be granted (the username/password login page will not be displayed).
  - If you fail in the certificate authentication, you will be directed to the username/password login page.
- If you connect to the Web UI through HTTP, FortiWeb will only verify your access by the username/password.
- You can configure FortiWeb to only apply the certificate-based authentication through the CLI as below. Then If certification authentication fails, WebUI login will fail.

```
config system global
  set admin-HTTPS-pki-required {enable | disable}
end
```

### Login failure and troubleshootin

- Check if the browser prompts you to select a certificate when connecting to WebUI through HTTPS.
  - If the client certificate is not listed for selecting, you will need to check if it has been imported successfully to the client system.  
For example, on a Windows PC, you need to import a pfx/p12 format certificate instead of a .cert/.der/.crt certificate, because the private key is required by Windows system, otherwise you may import a .cer certificate successfully while cannot see it selectable when using the browser to visit FortiWeb WebUI.
  - If you can select the specific certificate while login still fails, FortiWeb will be redirected to the username/password login page. (Refer to above section [Certificate based WebUI Login Logic:](#) )
- Check FortiWeb event logs to double confirm the login failure is caused by certificate authentication error:

When certificate authentication fails, an Event log will be generated as "Login failed! Check certificate error! from GUI(172.30.212.60)"

As a comparison, below is the log when login succeeds:

```
User admuser logged in successfully from GUI->HTTPS(172.30.212.127)
```

- Follow below steps to do further troubleshooting:
  - Ensure related configuration are added correctly by following the steps in the above section [Common configuration flow for PKI user \(Certificate based WebUI login\)](#);
  - Ensure the CA certificate is selected correctly;
  - Ensure the Subject string is input correctly;
    - If you have input multiple subject fields, try to leave only one or two and test again;
    - On 6.x and 7.0.1 builds, all Subject RDNs with the correct order are required:
      - E.g
      - C = CA, ST = BC, L = Burnaby, O = Fortinet, CN = 34B6A45C8 can be matched
      - CN = 34B6A45C8, C = CA, ST = BC, L = Burnaby, O = Fortinet cannot be matched
    - On 6.x and 7.0.1 builds, the type of RDNs are also case sensitive, while on later builds (schedule in 7.0.2), the type is case insensitive, while the value is still case sensitive:
      - E.g
      - c = CA, t = BC, l = Burnaby, o = Fortinet, cn = 34B6A45C8 can be matched
      - C = ca, ST = bc, L = burnaby, O = fortinet, CN = 34b6a45c8 cannot be matched
    - For the type stateOrProvinceName, please input ST instead of just S.
  - Use openssl command to verify if the CA and client certificate match:
    - This is a case for verification failure:

```
root@ubuntu:/# openssl verify -verbose -CAfile ca.crt Win10.OA.cer
C = CA, ST = BC, L = Burnaby, O = Fortinet, CN = Win10.OA
error 18 at 0 depth lookup: self signed certificate
error Win10.OA.cer: verification failed
```
  - Test with a different pair of client & CA certificates; It's better to guarantee they work well on other service environment.

## Resetting passwords

If you forget the password, or want to change an account's password, the `admin` administrator can reset the password.

If you forget the password of the `admin` administrator, you can either:

- Login via other account with `prof_admin` permission only by CLI console.
- Remove the admin password from the backup configuration file by web UI.

### To reset an account's password

1. Log in as the `admin` administrator account to web UI.
2. Go to **System > Admin > Administrators**.
3. Click the row to select the account whose password you want to change.
4. Click **Change Password**.
5. In the **New Password** and **Confirm Password** fields, type the new password.

**6. Click OK.**

The new password takes effect the next time that account logs in.

**To reset the admin account's password****Option 1:**

1. Connect to the CLI console with an account of `prof_admin` permission.
2. Run the following commands:

```
config system admin
edit admin
set password a
end
```

**Option 2:**

1. Login to the web UI with an account of `prof_admin` permission.
2. Go to **Maintenance > Backup & Restore > Backup**.
3. Click **Backup** to download the backup file.
4. Decompress the .zip file, and open the **FortiWeb\_system.conf** file with the editor. You are recommended to use Notepad++.
5. Locate the `config system admin` command lines, remove the `set password XXX` line, and save the file.
6. Go to **Maintenance > Backup & Restore > Restore**.
7. Click **Choose File** to upload the updated backup file.
8. Click **Restore**.

## SAML SSO Login issues

**On 7.0.1**, you can configure **Security Fabric > Fabric Connectors** to use Single Sign-On (SSO) to log in to FortiWeb with FortiGate's administrator accounts.

Please refer to "Fabric Connector: Single Sign On with FortiGate" in [FortiWeb Administration Guide](#) for detailed configuration steps.

Configuration Tips:

- On FortiGate, "Security Fabric role" should be selected as "Serve as Fabric Root";
- On FortiWeb, "Configuration Sync" should be set as "Default", which means when fabric connection with FortiGate is established, the Single Sign-On mode would be enabled automatically and FortiGate would enable synchronizing SAML Single-Sign-On related settings with the FortiWeb device.

Please note if multiple FortiWeb appliances are deployed in HA modes, SAML SSO configuration will be synchronized but not the IdP certificate. As a result, if HA failover happens, the new primary FortiWeb needs to be authorized on FortiGate again.

**On 7.0.2**, FortiWeb enhances this feature and supports Azure AD SSO and FortiAuthenticator as SAML IdP directly.

Configuration Tips:

- FortiWeb only supports one IdP server;
- To configure Azure AD or FortiAuthenticator as SAML IdP, “Status” should be disabled, and “Configuration Sync” needs to be “Local”.
- Upload IdP certificate via the corresponding button.
- 2FA with FortiToken is supported when FortiAuthenticator is configured as IdP.

**Common troubleshooting steps:**

1. Check if IdP (on FortiGate, FortiAuthenticator or Azure AD) and SP configuration (on FortiWeb) are correct and accurate;
2. Check if the “Connection Status” is Authorized when IdP is FortiGate;  
When IdP is not FortiGate, the “Connection Status” is always N/A because “Status” is disabled.
3. Check if the IdP certificate is uploaded successfully;  
You can check if `/var/log/debug/nstd/cert.pem` is available or updated.  
When IdP is FortiGate, IdP certificate will be downloaded automatically;  
When IdP is Azure AD or FortiAuthenticator, IdP certificate needs to be downloaded from the IdP and uploaded to FortiWeb.
4. Check diagnose debug logs:  

```
diagnose debug application samld 7  
diagnose debug enable
```
5. Check logs on IdPs such as FortiAuthenticator.

## System license issues

### How do I upload and validate a license for FortiWeb-VM?

FortiWeb-VM includes a free 15-day trial license that includes all features except:

- High availability (HA)
- FortiGuard updates
- Technical support

Once the trial expires, most functionality is disabled. You need to purchase a license to continue using FortiWeb-VM.

When you purchase a license for FortiWeb-VM, Fortinet Customer Service & Support (<https://support.fortinet.com>) provides a license file that you can use to convert the trial license to a permanent, paid license.

You can upload the license via the web UI. For versions lower than 7.0, the uploading process does not interrupt traffic or trigger an appliance reboot. If you are using version 7.0 and higher, the system will reboot and the whole process will take about 3 minutes.



FortiWeb-VM requires an Internet connection to periodically re-validate its license. It cannot be evaluated in offline, closed network environments. If FortiWeb-VM cannot contact Fortinet’s FDN for 24 hours, it locks access to the web UI and CLI.

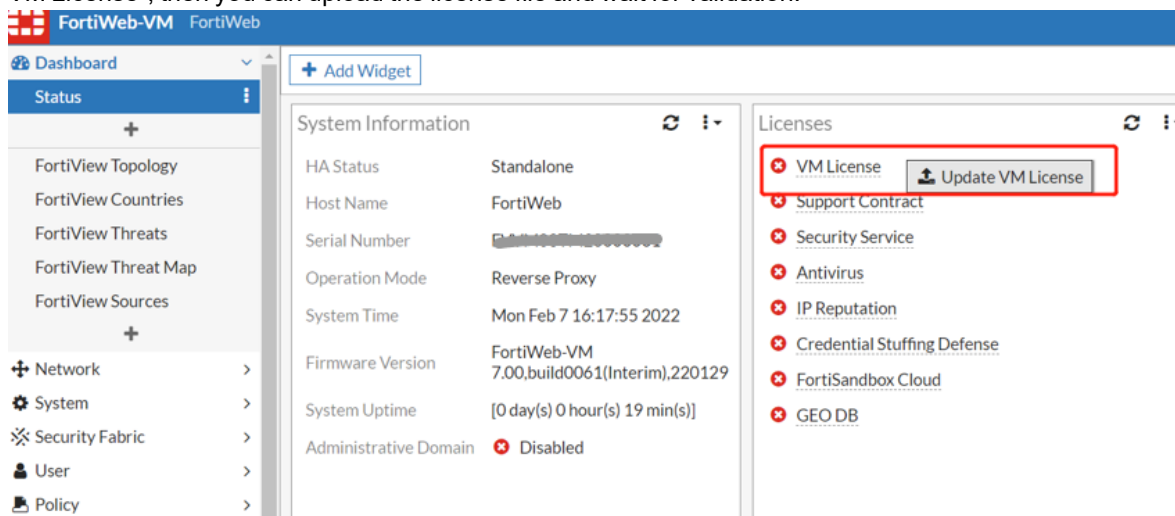
---

For detailed instructions for accessing the web UI and uploading the license, see the FortiWeb-VM Install Guide:

<https://docs.fortinet.com/fortiweb/hardware>

## To upload the license

- Go to the FortiWeb-VM web UI.  
For hypervisor deployments, the URL is the default IP address of `port1` of the virtual appliance, such as `https://192.168.1.99/`.  
For FortiWeb-VM deployed on AWS, the URL is the public DNS address displayed in the instance information for the appliance in your AWS console.
- Log in to the web UI as the `admin` user.  
For hypervisor deployments, by default, the `admin` user does not use a password.  
For AWS deployments, by default, the password is the AWS instance ID.
- Go to **System > Status > License**. When you click the line “VM License”, the system will prompt “Update VM License”, then you can upload the license file and wait for validation.



- Click **Update**.
- Browse to the license file (`.lic`) you downloaded earlier from Fortinet, then click **OK**.  
FortiWeb connects to Fortinet to validate its license. In most cases, the process is complete within a few seconds. A message appears:  

```
License has been uploaded. Please wait for authentication with registration servers.
```
- In the message box, click **Refresh**.  
If you uploaded a valid license, the following message is displayed:  

```
License has been successfully authenticated with registration servers.
```

The web UI logs you out. The login dialog reappears.
- Log in again.
- To verify that the license was uploaded successfully, log in to the web UI again, then view the **FortiGuard Information** widget. The **VM License** row should say **Valid**.  
Also view the **System Information** widget. The **Serial Number** row should have a number that indicates the maximum number of vCPUs that can be allocated according to the FortiWeb-VM software license, such as **FVVM020000003619** (where “VM02” indicates a limit of 2 vCPUs).  
After the VM license is validated successfully, you can check the widget on **Dashboard > Status >**

**Licenses** after license validation. You can also go to **System > Config > FortiGuard** to check the detailed updated license information.

The screenshot shows the FortiWeb-VM dashboard. On the left is a navigation menu with categories like Dashboard, Status, Network, System, Config, and High Availability. The main content area is divided into two panels: 'System Information' and 'Licenses'. The 'System Information' panel lists details such as HA Status (Standalone), Host Name (FortiWeb), Serial Number, Operation Mode (Reverse Proxy), System Time (Wed Aug 3 14:31:48 2022), Firmware Version (7.02,build0091[Interim],220803), System Uptime, Administrative Domain (Disabled), and Threat Analytics (Disabled). The 'Licenses' panel shows a list of licenses with their status: VM License, Support Contract, Security Service, Antivirus, IP Reputation, Credential Stuffing Defense, FortiSandbox, GEO DB, and Threat Analytics (Disabled).

The screenshot shows the FortiGuard Signature Update Management page. The left navigation menu is expanded to 'Config > FortiGuard'. The main content area is titled 'FortiGuard Distribution Network' and contains a 'License Information' table. The table has columns for 'Contract' and 'Status'. Each row represents a different license type with its current status and version information. Action buttons like 'Launch Portal', 'Update', and 'How To Renew' are present for certain licenses.

Contract	Status	Action
Support Contract	Registered	Launch Portal
Security Service	Valid Contract (Expires 2023-06-29) Signature Build Number: 0.00325 Signature Engine Version: 5.0.1	
Antivirus	Valid Contract (Expires 2023-06-29) Regular Virus Database Version: 90.04741 Extended Virus Database Version: 90.04712 Virus Engine Version: 6.00266	
IP Reputation	Valid Contract (Expires 2023-06-29) Signature Build Number: 4.00760	Update How To Renew
Credential Stuffing Defense	Valid Contract (Expires 2023-06-29) Credential Stuffing Defense Database Version: 1.00384	
FortiSandbox	Valid Contract (Expires 2023-06-29) FortiSandbox Database Version: 0.0	
GEO DB	Valid Contract (Expires 2023-06-29) GEO Database Version: 0135	
Threat Analytics	Expired (1969-12-31)	

## Firmware upgrade failures

### How do I reformat the boot device (flash drive) when I restore or upgrade the firmware?

Follow the instructions provided in "Restoring firmware ("clean install")" in FortiWeb Administration Guide.

For Step 11, type `F` to format the boot device (flash drive), and then enter `Y` to confirm your selection.

After a few minutes, the reformatting process is complete. Continue with the instructions for retrieving the firmware image from the TFTP server.

During the system boot, Fortinet highly recommends that you verify the disk integrity. To perform this task, when the prompt `Press [enter] key for disk integrity verification is displayed`, press `Enter`.

After the firmware restore is complete, use the `get system status` CLI command to verify the system version. For additional information on using the CLI, see the *FortiWeb CLI Reference*:

<https://docs.fortinet.com/product/fortiweb/>

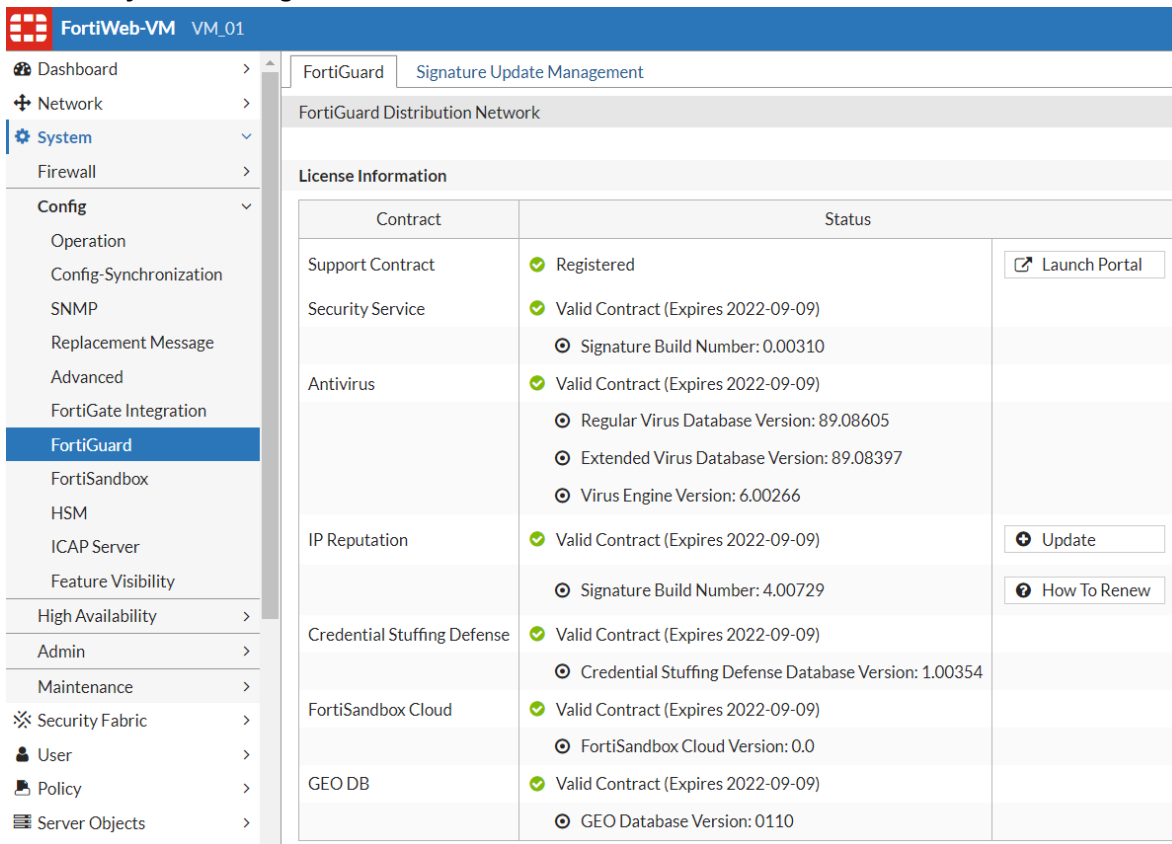
### Troubleshooting firmware upgrade failures

1. If upgrade failed via GUI, check F12 to see which API causes the error;
2. If it's GUI timeout (request timeout), it should be a frontend issue;
3. If it's API timeout, it might be a backend system problem.
4. Check if uploading files to `/var/log/gui_upload` can be successful;
5. Check if upgrade via CLI can be successful;
6. Check if upgrade via a fast-speed link can be successful, especially when GUI warns timeout;
7. Check if hard disk space is enough for uploading image:
  - GUI upgrade: image will be uploaded to `/var/log/cgi_upfile`
  - CLI upgrade: image will be uploaded to `/tmp`

# DB version&update info

## How to check detailed db versions and update information?

### 1. Check in System>Config>FortiGuard:



### 2. Check current db version.

```
FortiWeb # get sys upd-db-version
Regular Virus Database Version: 00089.04670
Extended Virus Database Version: 00089.04220
Virus Engine Version: 00006.00137
Waf Signature Version: 00000.00300
IP Intelligence Signature Version: 00004.00713
Credential Stuffing Defense Database Version: 00001.00339
FortiSandbox Malware Signature Database Version: 0.0
Geo Database Version: Fortiweb-Country-Build0094 2021-09-09
```

### 3. Update db version for a module or all

FortiWeb appliances connect to the FDN by connecting to the FDS nearest to the FortiWeb appliance by its configured time zone.

```
FortiWeb # execute update #update for a specific module
av update antivirus
base update contract, timezone and fds server list
fwdb update fortieweb signature(include geodb)
hcdb update credential stuffing defense
irdb update ip reputation
FortiWeb # execute update-now #update all modules using db
```

#### 4. Check the detailed db version & update information for all modules.

```
FortiWeb # diagnose system update info
FortiWeb signature
-----
Version: 0.00300
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 12:00:18 2021
Next Update Date: Thu Sep 30 14:00:00 2021

Historical versions
-----
0.00326 Aug/31/2022-12:02:55
0.00325 Aug/15/2022-14:02:58
0.00323 Jul/15/2022-14:01:11

FortiWeb GEODB
-----
Version: Fortiweb-Country-Build0094 2021-09-09
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 11:47:07 2021
Next Update Date: Thu Sep 30 14:00:00 2021
Historical versions
-----
Fortiweb-Country-Build0137 2022-08-05 Aug/31/2022-12:02:55
Fortiweb-Country-Build0137 2022-08-05 Aug/31/2022-12:02:55
Fortiweb-Country-Build0135 2022-07-22 Aug/15/2022-14:02:57

Regular Antivirus
-----
Version: 89.04670
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 12:00:20 2021
Next Update Date: Thu Sep 30 14:00:00 2021

Historical versions
-----
90.05561 Aug/31/2022-16:01:41
90.05557 Aug/31/2022-14:00:10
90.05555 Aug/31/2022-12:03:17
89.04650

Extended Antivirus
-----
Version: 89.04220
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 12:00:20 2021
Next Update Date: Thu Sep 30 14:00:00 2021

Historical versions
-----
90.05341 Aug/30/2022-16:00:19
90.05132 Aug/23/2022-16:01:04
90.04922 Aug/16/2022-16:00:53

Antivirus Engine
-----
```

```
Version: 6.00137
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 12:00:20 2021
Next Update Date: Thu Sep 30 14:00:00 2021
```

```
Historical versions
-----
```

```
IP Reputation
-----
```

```
Version: 4.00713
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 12:00:18 2021
Next Update Date: Thu Sep 30 14:00:00 2021
```

```
Historical versions
-----
```

```
4.00762 Aug/25/2022-16:00:08
4.00761 Aug/18/2022-16:00:19
4.00756 Jul/13/2022-16:00:24
```

```
Harvest Credentials
-----
```

```
Version: 1.00339
Expiry Date: Fri Sep 09 2022
Last Update Date: Thu Sep 30 12:00:18 2021
Next Update Date: Thu Sep 30 14:00:00 2021
```

```
Historical versions
-----
```

```
1.00387 Aug/26/2022-12:00:11
1.00386 Aug/19/2022-12:00:33
1.00385 Aug/12/2022-12:00:10
```

```
FortiSandbox Malware Signature Database
-----
```

```
Version: 0.0
Expiry Date: Fri Sep 09 2022
Last Update Date: Wed Dec 31 18:00:00 1969
Next Update Date: Thu Sep 30 14:00:00 2021
```

```
Latest errors
-----
```

```
Mon Sep 27 18:01:19 2021 Failed to receive essential/anti-virus packages from
209.222.136.6:443.
Fri Sep 24 06:01:19 2021 Failed to receive essential/anti-virus packages from
173.243.138.66:443.
Thu Sep 23 21:39:34 2021 update network error:failed to connect servers.
Thu Sep 23 21:39:33 2021 update network error:failed to connect servers.
```

```
Fortisandbox connectivity
-----
```

```
FortiSandbox DOMAIN      : 0.0.0.0
FortiSandbox IP          : 0.0.0.0
FortiSandbox port        : 514
FortiSandbox connect type : Appliance
FortiSandbox connect state: Disconnected
```

```
FortiSandbox connect info : Fail to build FortiSandbox connection.  
FortiSandbox connect ssl :
```

## Why did the FortiGuard service update fail?

If your automatic FortiGuard service update is not successful, complete the following troubleshooting steps:

1. Ensure that your firewall rules allow FortiWeb to access the Internet via TCP port 443.  
This is the port that FortiWeb uses to poll for and download FortiGuard service updates from the FortiGuard Distribution Network (FDN).
2. Ensure FortiWeb can communicate with the DNS server.  
When it performs the initial FortiGuard service update, FortiWeb requires access to the DNS server to resolve the domain name `fds.fortinet.com` to the appropriate host name.
3. Because the size of the virus signature database exceeds 200MB, an unstable network can interrupt the TCP session that downloads the database. If the download fails for this reason, obtain the latest version of the virus signature database from `support.fortinet.com` and perform the update manually. For details, see "Uploading signature & geography-to-IP updates" in FortiWeb Administration Guide. FortiWeb resumes automatic updates of the database at the next scheduled time.
4. If the previous steps do not solve the problem, use the following commands to obtain additional information:

```
diagnose debug enable  
diagnose debug application fds 7
```

If you need to contact Fortinet Technical Support for assistance, provide the output of these diagnose debug commands and a configuration file.

For more information about these commands, see the *FortiWeb CLI Reference*:

<https://docs.fortinet.com/product/fortiweb/>

For additional methods for verifying FortiGuard connectivity, see "Connecting to FortiGuard services" in FortiWeb Administration Guide.

## How to do DB core files integrity check?

Sometimes, FortiWeb system files maybe damaged by some accident or unexpected malicious destruction. In such cases, some abnormal system status will occur. From 7.4.1, new mechanism is added to detect and help locate those issues through GUI or CLI.

- Run `diagnose system waf-signature check-integrity` in ssh console.
- In FortiWeb's GUI, go to **Log&Report > Event**, select action=check-integrity. Here you will find about 30 event logs showing file integrity results, for example `< File integrity of 'name-index' is assured.>`

# Cryptographic Key

## FAQ

### What is the Cryptographic Key?

The cryptographic key is used by some security modules such as Cookie Security, MITB, Site Publish and Captcha for encryption and decryption.

Each FortiWeb appliance will generate such a unique and random key to guarantee its security, and this key will not be changed after system reboots or executed with factory reset.

### Why do we need to backup or restore the cryptographic key?

On 7.0.2 and later builds, you can backup or restore the cryptographic key via **System > Maintenance > Backup & Restore > Cryptographic Key**. As this option is hidden by default, you need to enable it in **System > Config > Feature Visibility > Cryptographic key Backup/Restore**.

In all FortiWeb HA modes including HA Manager mode, this key will be automatically synchronized from the primary node to secondary nodes, so that the same traffic flow can be processed via different appliances in the HA group because it is encrypted and decrypted by the same key. This is crucial for the traffic to be distributed successfully among HA nodes.

For load-balance scenarios in public clouds where multiple FortiWeb appliances are deployed to process traffic flows dispatched by an upstream load-balancer, you need to manually backup the key from one FortiWeb and restore it to all other appliances, because FortiWeb only supports automatic synchronization of the cryptographic key in HA modes.

Please note this key cannot be synchronized via **System > Config > Config-Synchronization** due to some implementation consideration.

## Resetting the configuration

If you will be selling your FortiWeb appliance, or if you are not sure what part of your configuration is causing a problem, you can reset it to its default settings and erase data. If you have not updated the firmware, this is the same as resetting to the factory default settings.



Back up your configuration before beginning this procedure, if possible. Resetting the configuration could include the IP addresses of network interfaces. For details about backups, see "[Backups](#)" on page 1. For details about reconnecting to a FortiWeb appliance whose network interface configuration was reset, see "[Connecting to the web UI or CLI](#)" on page 1.

---

To delete your data from the appliance, connect to the CLI and enter this command:

```
execute formatlogdisk
```

To reset the appliance's configuration, connect to the CLI and enter this command:

```
execute factoryreset
```



Alternatively, you can reset the appliance's configuration to its default values for a specific software version by restoring the firmware during a reboot (a "clean install"). For details, see [Restoring firmware \("clean install"\)](#) on page 66.

---

## Restoring firmware ("clean install")

Restoring (also called re-imaging) the firmware can be useful if:

- You are unable to connect to the FortiWeb appliance using the web UI or the CLI
- You want to install firmware **without** preserving any existing configuration (i.e. a "**clean install**")
- A firmware version that you want to install requires a different size of system partition (see the Release Notes accompanying the firmware)
- A firmware version that you want to install requires that you format the boot device (see the Release Notes accompanying the firmware)

Unlike updating firmware, restoring firmware re-images the boot device, including the signatures that were current at the time that the firmware image file was created. Also, restoring firmware can only be done during a boot interrupt, before network connectivity is available, and therefore **requires a local console connection to the CLI. It cannot be done through an SSH or Telnet connection.**

Alternatively, if you cannot physically access the appliance's local console connection, connect the appliance's local console port to a terminal server to which you have network access. Once you have used a client to connect to the terminal server over the network, you will be able to use the appliance's local console through it. However, be aware that from a remote location, you may not be able to power cycle the appliance if abnormalities occur.

### To restore the firmware



Back up your configuration before beginning this procedure, if possible. Restoring firmware resets the configuration, including the IP addresses of network interfaces. For details about backups, see "[Backups](#)" on page 1. For details about reconnecting to a FortiWeb appliance whose network interface configuration was reset, see "[Connecting to the web UI or CLI](#)" on page 1.

---

1. Download the firmware file from the Fortinet Customer Service & Support website:  
<https://support.fortinet.com/>
2. Connect your management computer to the FortiWeb console port using a RJ-45-to-DB-9 serial cable or a null-modem cable.
3. Initiate a **local console connection** from your management computer to the CLI of the FortiWeb appliance, and log in as the `admin` administrator, or an administrator account whose access profile contains **Read** and **Write** permissions in the **Maintenance** category.  
For details, see "[Connecting to the web UI or CLI](#)" on page 1.

4. Connect port1 of the FortiWeb appliance directly or to the same subnet as a TFTP server.
5. Copy the new firmware image file to the root directory of the TFTP server.
6. If necessary, start your TFTP server. If you do not have one, you can temporarily install and run one such as `tftpd` on your management computer.



Because TFTP is **not** secure, and because it does not support authentication and could allow anyone to have read and write access, you should **only** run it on trusted administrator-only networks, **never** on computers directly connected to the Internet. If possible, immediately turn off `tftpd` when you are done.

7. Verify that the TFTP server is currently running, and that the FortiWeb appliance can reach the TFTP server.

To use the FortiWeb CLI to verify connectivity, enter the following command:

```
execute ping 192.0.2.168
```

where `192.0.2.168` is the IP address of the TFTP server.

8. Enter the following command to restart the FortiWeb appliance:

```
execute reboot
```

9. As the FortiWeb appliances starts, a series of system startup messages appear.

Press any key to display configuration menu.....

10. Immediately press a key to interrupt the system startup.



You have only 3 seconds to press a key. If you do not press a key soon enough, the FortiWeb appliance reboots and you must log in and repeat the `execute reboot` command.

If you successfully interrupt the startup process, the following messages appears:

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[B]: Boot with backup firmware and set as default.
```

```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```

Enter G,F,B,Q, or H:

Please connect TFTP server to Ethernet port "1".

11. If the firmware version requires that you first format the boot device before installing firmware, type `F`. Format the boot disk before continuing.
12. Type `G` to get the firmware image from the TFTP server.  
The following message appears:  
Enter TFTP server address [`192.0.2.168`]:
13. Type the IP address of the TFTP server and press Enter.  
The following message appears:  
Enter local address [`192.0.2.188`]:
14. Type a temporary IP address that can be used by the FortiWeb appliance to connect to the TFTP server.  
The following message appears:  
Enter firmware image file name [`image.out`]:

15. Type the file name of the firmware image and press Enter.  
The FortiWeb appliance downloads the firmware image file from the TFTP server and displays a message similar to the following:

```
MAC:00219B8F0D94
#####
Total 28385179 bytes data downloaded.
Verifying the integrity of the firmware image..
Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?
```



If the download fails after the integrity check with the error message:  
invalid compressed format (err=1)

but the firmware matches the integrity checksum on the Fortinet Technical Support website, try a different TFTP server.

16. Type D.  
The FortiWeb appliance downloads the firmware image file from the TFTP server. The FortiWeb appliance installs the firmware and restarts. The time required varies by the size of the file and the speed of your network connection.  
The FortiWeb appliance reverts the configuration to default values for that version of the firmware.
17. To verify that the firmware was successfully installed, log in to the CLI and type:  
`get system status`  
The firmware version number is displayed.
18. Either reconfigure the FortiWeb appliance or restore the configuration file. For details, see ["How to set up your FortiWeb"](#) on page 1 and ["Restoring a previous configuration"](#) on page 1.  
If you are **downgrading** the firmware to a previous version, and the settings are not fully backwards compatible, the FortiWeb appliance may either remove incompatible settings, or use the feature's default values for that version of the firmware. You may need to reconfigure some settings.
19. Update the attack definitions.  
Installing firmware replaces the current attack definitions with those included with the firmware release that you are installing. After you install the new firmware, make sure that your attack definitions are up-to-date. For details, see ["Uploading signature & geography-to-IP updates"](#) on page 1.

## Checking System Resource Issues

- [Checking CPU information&Issues on page 68](#)
- [Checking memory usage on page 73](#)
- [Diagnosing memory leak issues on page 76](#)
- [Checking disk information & issues on page 81](#)

### Checking CPU information&Issues

1. Check CPU information  
`FortiWeb# diagnose hardware cpu list #show the detail info for all CPU/vCPU`

```
FortiWeb-AWS-M01 # diagnose hardware cpu list
processor      : 0
vendor_id     : GenuineIntel
cpu family    : 6
model         : 79
model name    : Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz
stepping      : 1
microcode     : 0xb000038
cpu MHz       : 2300.049
cache size    : 46080 KB
physical id   : 0
siblings      : 2
core id       : 0
cpu cores     : 2
apicid        : 0
initial apicid : 0
fpu           : yes
fpu_exception : yes
cpuid level   : 13
wp            : yes
...
```

## 2. CPU & processor numbers

```
FortiWeb # fn cat /proc/cpuinfo | grep "cpu cores" #Check physical CPU cores
cpu cores      : 16
/# cat /proc/cpuinfo |grep "processor" | sort -u | wc -l    #Check logical CPU
cores when hyperthread is enabled
32 cat /proc/cpuinfo |grep "processor"
```

## 3. Check which daemon or process consuming the most CPU usage

To determine if high load is frequently a problem, you can display the average load level by using these CLI commands:

```
FortiWeb # get system performance
CPU states:      5% used, 95% idle
Memory states:  29% used
Up:              9 days, 12 hours, 52 minutes.
```

### top

Use the CLI to view the per-CPU/core process load level and a list of the most system-intensive processes. This may show processes that are consuming resources unusually.

While the command is running, you can press Shift + P to sort the five columns of data by CPU usage (the default) or Shift + M to sort by memory usage.

```
FortiWeb# diagnose system top 10
Mem: 4867300K used, 126120392K free, 16536K shrd, 10792K buff, 117620K cached
CPU:  0.1% usr  0.1% sys  0.0% nic 99.6% idle  0.0% io  0.0% irq  0.0% sirq
Load average: 1.71 1.55 1.49 2/953 52110
  PID  PPID  USER      STAT   VSZ  %VSZ  CPU  %CPU  COMMAND
6262   1  root      S      9582m  7.4   31   0.3  /bin/proxyd
 6264   1  root      S      6539m  5.1   29   0.0  /bin/bot_daemon
6273   1  root      S      2498m  1.9   21   0.0  /bin/garbage -o standalone
6316  6238  root      S      2098m  1.6   24   0.0  /bin/mysqld --defaults-file=/data/e
6251   1  root      S       803m  0.6   10   0.0  /bin/monitord
6269   1  root      S       411m  0.3   21   0.0  /bin/sandboxd
6271   1  root      S       400m  0.3   43   0.0  /bin/shibd -F -f -p /var/run/shibd.
6287   1  root      S       256m  0.2   59   0.0  /bin/statusd
```

The above command generates a report of processes every 10 seconds. The report provides the process names, their process ID (pid), status, CPU usage, and memory usage.

The report continues to refresh and display in the CLI until you press q (quit).

### perf top

The perf top command is used for real time system profiling and functions similarly to the top utility. However, where the top utility generally shows you how much CPU time a given process or thread is using, perf top shows you how much CPU time each specific function uses. In its default state, perf top tells you about functions being used across all CPUs in both the user-space and the kernel-space.

```
FortiWeb# diagnose system perf # or "perf top" in backend shell
FortiWeb# diagnose system perf
PerfTop: 69182 irqs/sec kernel:96.4% exact: 100.0% lost: 0/0 drop: 0/0
[4000Hz cycles], (all, 64 CPUs)
```

```
-----
13.50% [kernel] [k] find_busiest_group
3.20% [kernel] [k] idle_cpu
3.15% [kernel] [k] _raw_spin_lock
2.44% [kernel] [k] __schedule
2.42% [kernel] [k] rcu_sched_clock_irq
2.07% [kernel] [k] _raw_spin_trylock
1.95% [kernel] [k] native_irq_return_iret
```

#### 4. Kill processes

Once you locate an offending PID from “diagnose system top”, you may want to terminate it. For example, in a test environment or when you fail to locate the cause when access to a server-policy always fails, you may try to kill proxyd or dnspoxyd.

Under normal conditions, killing a process is not recommended.

```
diagnose system kill 9 <pid>
```

or

```
Fn kill 9 <pid>
```

On some 7.0.x builds, you can execute “fn kill <pid>” on the front-end CLI, or need to login to the back-end shell and then execute kill:

```
/# kill 9 <pid>
```

Please refer to [Run backend-shell commands](#) to learn how to configure shell-access.

#### 5. Check if high CPU usage is caused by heavy traffic load

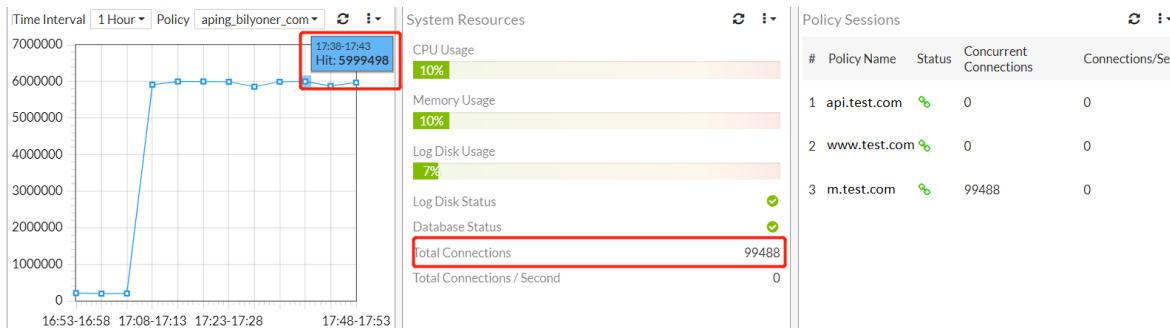
Heavy traffic loads can cause sustained high CPU or RAM usage. If this is unusual, no action may be required, unless you are being subject to a DoS attack. Sustained heavy traffic load may indicate that you need a more powerful model of FortiWeb.

You can check traffic load via GUI or debug logs in several ways:

1) Monitor Total Connection per Second, Total Connections and Total HTTP Transaction, Throughput on the GUI dashboard.

Total Connection per Second, Total Connections (also Concurrent Connection) are displayed directly in the widgets “System Resource” and “Policy Sessions”, whereas the current HTTP transaction per second is not displayed directly on GUI. You need to enable/add a widget named “HTTP Transactions” and calculate the TPS by dividing the total transaction in 5 minutes.

Taking the screenshot below for example, the concurrent connection is 100000 and there are no new connections established per second, whereas there are nearly 6000000 transactions in the past 5 minutes - equal to 20000 transactions per second (TPS), so this might be the main cause why CPU usage reaches 10%.



2) Some of these four real-time performance numbers can be also obtained via CLIs:

- Total Connection per Second: `diagnose policy total-conn-psec list`
- Total Connections: `diagnose policy total-session list`
- Total Throughput in HTTP level: `diagnose policy total-traffic http list`  
This statistics from CLI only includes HTTP payload, does not include L2 & L3 headers
- HTTP Transaction per Second: `diagnose policy total-detail-stats list <server-policy>`  
No total statistics in CLI

3) Check TCP connections in TIME\_WAIT status

TIME\_WAIT connections cannot be displayed in dashboard widgets but also consume system connection/memory resources. You can also check connection in backend shell:

```

/# netstat -nat | awk '{print $6}' | sort | uniq -c | sort -r
199101 ESTABLISHED          #Concurrent connections
 251 LISTEN
   7 TIME_WAIT
   1 established)
   1 Foreign
    
```

4) Examine traffic history in the traffic log. Go to **Logs&Report > Log Access > Traffic**.

If massive traffic logs are generated in a short period, it indicates heavy traffic load.

6. Check if high CPU usage is caused by Attacks

A prolonged denial of service (DoS) or brute-force login attack (to name just a few) can bring your web servers to a standstill, if your FortiWeb appliance is not configured for it.

In the FortiWeb appliance's web UI, you can watch for attacks in two ways:

- 1) Monitor current HTTP traffic on the dashboard. Go to **System > Status > Status** and examine the attack event history graph in the Policy Summary widget.
- 2) Examine attack history in the traffic log. Go to **Logs&Report > Log Access > Attack**.

Before attacks occur, use the FortiWeb appliance's rich feature set to configure attack defenses.

7. 7. Check if high CPU usage is caused by port exhaustion

If there is only one interface IP address and only one back-end server, the CPU tends to be relatively high because too many ports will be occupied for building up connections with the back-end server..

You will see many connections are in the TIME\_WAIT state and being closed after 2 MSL (Maximum Segment life) time. To check the connection in the TIME\_WAIT state, you can run `dia network netstat -nat | grep TIME_WAIT`.

If you run “`diagnose system perf top`”, you can see the following perf top info:

```

PerfTop: 52793 irqs/sec kernel:98.8% exact: 100.0% lost: 0/0 drop: 0/0 [4000Hz cy
-----
17.18% [kernel] [k] _raw_spin_lock
14.75% [kernel] [k] _raw_spin_lock_bh
14.59% [kernel] [k] queued_spin_lock_slowpath
14.48% [kernel] [k] _inet_check_established
4.92% [kernel] [k] _inet_hash_connect
1.74% [kernel] [k] inet_enasnrn
1.68% [kernel] [k] ipt_do_table
1.55% [kernel] [k] _inet_lookup_established
1.50% [kernel] [k] _raw_read_lock_bh
1.31% [kernel] [k] fib_table_lookup

```

you have three options to avoid the port exhaustion.

- set ip-local-port-assign-ex

```

FortiWeb # config system network-option
FortiWeb (network-option) # sh
config system network-option
    set ip-local-port-assign-ex enable
end

```

- Add more IP addresses of the interface to real server and enable the ip-src-balance option.

To add more ip addresses of the interface:

```

config system interface
    edit "port3"
        set type physical
        set ip 40.40.40.1/16
        config secondaryip
            edit 1
                set ip 40.40.40.2/16
            next
        end
        config classless_static_route
            end
        next
    end
end

```

To enable the ip-src-balance option:

```

config system network-option
    set ip-src-balance enable
    set ip6-src-balance enable
end

```

- Applying client real IP in busiest server policy:

```

config server-policy policy
    edit policy_name
        set client-real-ip enable
        ip range: ip-range
    next
end

```

## 8. Check system and debug logs to see CPU resource status:

1) Log&Report > Event > Filter > Action > check-resource

Log example:

```
CPU usage too high,CPU usage is 95, process proxyd
```

## 2) Analyze NMON files with all relevant statistics

NMON files include CPU, Mem, I/O statistics, you can do a comprehensive analysis from these relevant information.

## Checking memory usage

### 1. Use “diagnose debug memory” to check memory usage:

This command will collect memory information via several different kinds of backend commands.

```
FortiWeb# diagnose debug memory
```

```
Tue Oct 26 17:42:56 UTC 2021
```

```
17:42:56 up 5 days, 19:45, load average: 2.09, 1.78, 1.82
```

init	1	shared	1528kB	anonymous	112kB
cmdbsvr	191	shared	17132kB	anonymous	33688kB
syslogd	873	shared	256kB	anonymous	44kB
klogd	874	shared	256kB	anonymous	48kB
hamain	875	shared	10632kB	anonymous	6972kB
hasync	876	shared	9328kB	anonymous	6832kB

```
...
...
```

2. After 6.4 release, the system will generate a regular monitoring file with a backend command “/bin/FortiWeb\_get\_memory\_usage”, which includes the same output of “diagnose debug memory”. The regular output is recorded in /var/log/gui\_upload/debug\_memory.txt and can be downloaded via **System > Maintenance > Backup&Restore**. You can download it manually or use the one-click button to archive and download it.

You can set the interval to record debug memory logs:

```
config system global
```

```
    set debug-memory-interval 5    #default 5 minutes and the range is from 1 to 65535
```

```
end
```

```
/# more /var/log/gui_upload/debug_memory.txt
```

```
Fri May 28 04:30:13 UTC 2021
```

```
04:30:13 up 0 min, load average: 1.07, 0.26, 0.09
```

init	1	shared	1376kB	anonymous	104kB
cmdbsvr	2293	shared	14044kB	anonymous	29032kB
syslogd	3457	shared	280kB	anonymous	48kB

```
...
...
```

### 3. Check current memory usage in backend shell:

Please note that FortiWeb changes the way to login to the backend shell Refer to Part VI: Run backend-shell commands.

#### free

This command gives you a table of the total, used, free, shared, buffer/cache, and available RAM. It also shows the total amount of swap space configured, and how much is used and available. The default unit is KB.

**free= total – used – buff/cache**

```
/# free
```

	buffers	cached	total	used	free	shared
Mem:	130987692	4990340	125997352	16540	23576	129092
-/+ buffers/cache:		4837672	126150020			
Swap:	0	0	0			

**/proc/meminfo**

This is a virtual file that reports the amount of available and used memory. It contains real-time information about the system's memory usage as well as the buffers and shared memory used by the kernel

```

/# cat /proc/meminfo
MemTotal:      28635360 kB
MemFree:       25998836 kB
MemAvailable:  26127368 kB
Buffers:       201340 kB
Cached:        192220 kB
SwapCached:    0 kB
Active:        1730772 kB
Inactive:      164688 kB
Active(anon):  1501972 kB
Inactive(anon): 38064 kB
Active(file):  228800 kB
Inactive(file): 126624 kB
Unevictable:   1164 kB
Mlocked:       1164 kB
SwapTotal:     0 kB
SwapFree:      0 kB
Dirty:         104 kB
Writeback:     0 kB
AnonPages:    1503120 kB
Mapped:        89856 kB
Shmem:         38164 kB
KReclaimable: 22528 kB
Slab:          94268 kB
SReclaimable: 22528 kB
SUnreclaim:   71740 kB
KernelStack:  5536 kB
PageTables:   12048 kB
NFS_Unstable: 0 kB
Bounce:       0 kB
WritebackTmp: 0 kB
CommitLimit:  14317680 kB
Committed_AS: 5405984 kB
VmallocTotal: 34359738367 kB
VmallocUsed:  64024 kB
VmallocChunk: 0 kB
Percpu:       1984 kB
DirectMap4k:  63424 kB
DirectMap2M:  3082240 kB
DirectMap1G:  28311552 kB

```

**/# top**

Some common usage: Press Shift + P to sort the five columns of data by CPU usage (the default) or Shift + M to sort by memory usage; Press "1" (number one) to check status of all logical processors.

```

/# top
Mem: 4919392K used, 126068300K free, 16348K shrd, 45984K buff, 134312K cached
CPU:  0.1% usr  0.0% sys  0.0% nic 99.8% idle  0.0% io  0.0% irq  0.0% sirq
Load average: 1.33 1.40 1.38 2/954 28663

```

```

  PID  PPID  USER      STAT   VSZ  %VSZ  CPU  %CPU  COMMAND
6262   1    root      S      9582m  7.4   55   0.0  /bin/proxyd
6276   1    root      S      224m   0.1   39   0.0  /bin/confd_ha
6264   1    root      S      6539m  5.1   24   0.0  /bin/bot_daemon
6273   1    root      S      2498m  1.9   60   0.0  /bin/garbage -o standalone
6316 6238  root     S      2098m  1.6   7    0.0  /bin/mysqld --defaults-file=/data/etc
6251   1    root     S      803m   0.6  12   0.0  /bin/monitord
6269   1    root     S      411m   0.3  17   0.0  /bin/sandboxd
6271   1    root     S      400m   0.3  41   0.0  /bin/shibd -F -f -p /var/run/shibd.pi
6287   1    root     S      256m   0.2  59   0.0  /bin/statusd
6257   1    root     S      245m   0.1  63   0.0  /bin/wvwsd
6244   1    root     S      219m   0.1  36   0.0  /bin/logd
6272   1    root     S      202m   0.1  26   0.0  /bin/fortiviewd

```

### **#!/# ps -l**

We usually focus on the RSS and VSZ values in ps output, which can be used to check the memory utilization for a specific process.

RSS stands for Resident Set Size and shows how much RAM is utilized at present. It shows the entire stack of physically allocated memory so it is more important.

VSZ is short for Virtual Memory Size. It's the total amount of memory a process may hypothetically access. When a process is started, VSZ memory becomes RSS memory.

If the RSS value increases continuously and does not decrease even if the traffic drops down, it might be a hint of memory leak and require further investigation.

An example as below:

At the beginning without any traffic, the VSZ is 10.3g VSZ, and RSS is 612m.

```

#!/# free
total used free shared buff/cache available
Mem: 130983668 6092968 122149324 78124 2741376 123905312
Swap: 0 0 0
#!/#
#!/# ps -l | grep "/proxyd" | grep -v grep
S 0 23653 1 10.3g 612m 0:0 11:31 00:00:33 /bin/proxyd

```

After traffic is pushed, both RSS and VSZ increase obviously.

```

#!/# free
total used free shared buff/cache available
Mem: 130983668 121216100 567704 78128 9199864 8769384
Swap: 0 0 0
#!/#
#!/# ps -l | grep "/proxyd" | grep -v grep
S 0 23653 1 127g 88.9g 0:0 11:31 02:25:58 /bin/proxyd

```

After traffic is stopped and concurrent connections are released, the RSS value may decrease obviously, but the VSZ often does not decrease.

And, since some memory is still used, generally the RSS memory may not decrease to the initial value. As shown below, RSS is decreased from the peak value 88.9g to 1982m, but not the initial value 612m. It is normal and does not indicate a memory leak.

```

#!/# free
total used free shared buff/cache available
Mem: 130983668 9952592 119414496 77964 1616580 120133272
Swap: 0 0 0
#!/#
#!/# ps -l | grep "/proxyd" | grep -v grep

```

```
S 0 23653 1 127g 1982m 0:0 11:31 02:39:38 /bin/proxyd
```

## Diagnosing memory leak issues

When you find the memory usage is very high and increases very fast in a short time period, it might be a memory leak issue, and you can analyze by the following steps.

Please note memory increase does not always mean a memory leak. A memory leak issue usually has these phenomena:

- Very fast and abnormal memory increase (usually with common or low traffic level)
- Continuous memory increase without deallocated
- Used memory are not deallocated even after traffic drops or stopped

The most important thing for troubleshooting a memory leak issue is to locate which module, process or function causes the memory increase.

1. Check history logs to see memory resource status:

**Log&Report > Event > Filter > Action > check-resource**

```
failure msg="mem usage raise too high,mem(67)
```

2. Check if there are some memory related print outputs in the console.
3. Check connection amounts to see if memory increase is possibly caused by too many concurrent connections.

```
#!/# netstat -nat | awk '{print $6}' | sort | uniq -c | sort -r
319800 ESTABLISHED
330 FIN_WAIT2
251 LISTEN
7 TIME_WAIT
1 established)
1 SYN_SENT
1 Foreign
```

If there are too many TIME\_WAIT or FIN\_WAIT2 connections, it may be abnormal because connections are not closed normally.

If memory usage still does not decrease when TIME\_WAIT or FIN\_WAIT2 are released, it may mean memory leak.

4. Execute “diagnose debug memory” several times, then compare the diff of the output to find which part/module/process has the most increase.  
According to the memory increment speed, you may adjust the interval to execute the command and collect the output.
5. Use `diagnose debug jemalloc-heap` & `diagnose system jeprof` to trace and analyze memory occupation and cause of memory usage over a period of time.
  - If the jemalloc profile is activated and the memory usage exceeds the configured threshold, the heap file will be generated in directory `/var/log/gui_upload`.
  - You can use `jemalloc-heap` to show or clear the heap files. At most 10 heap files are kept on the device.
  - You can use `jeprof` to parse the heap file via `jeprof` tool
  - The `jemalloc` commands don't give us useful information when the memory doesn't increase.
    - 1) Enable jemalloc profile

```
FortiWeb# diagnose debug jemalloc-conf proxyd enable
```
    - 2) if memory increases quickly, execute below command to generate dump files.

E.g., you can wait the memory usage to increase 10% and execute below commands; and it's better to repeat this commands for several times when memory increases every 10%:

```
FortiWeb# diagnose debug jemalloc proxyd dump
```

### 3) Check the dump heap file generated:

```
FortiWeb # diagnose debug jemalloc-heap show
  jeprof.out.28279.1641342474.heap
  jeprof.out.4973.1641276249.heap
```

### 4) After getting a few heap file, execute below command to parse the heap file

```
FortiWeb # diagnose system jeprof proxyd
Using local file /bin/proxyd
Using local file /var/log/gui_upload/jeprof.out.28279.1641342474.heap
Total: 124422365 B
34403589  27.7%  27.7% 34403589  27.7% ssl3_setup_write_buffer
34262011  27.5%  55.2% 34262011  27.5% ssl3_setup_read_buffer
18062121  14.5%  69.7% 18062121  14.5% CRYPTO_zalloc
17011023  13.7%  83.4% 17011023  13.7% _HTTP_init
9905760   8.0%  91.3% 9905760   8.0% BUF_MEM_grow
3195135   2.6%  93.9% 3195135   2.6% buffer_new
1583640   1.3%  95.2% 18857320  15.2% HTTP_substream_process_ctx_create
...
Using local file /bin/proxyd
Using local file /var/log/gui_upload/jeprof.out.4973.1641276249.heap
Total: 576387295 B
175840569 30.5%  30.5% 175840569 30.5% ssl3_setup_write_buffer
175415833 30.4%  60.9% 175415833 30.4% ssl3_setup_read_buffer
81823328  14.2%  75.1% 81823328  14.2% CRYPTO_zalloc
72087699  12.5%  87.6% 72612307  12.6% _HTTP_init
8578052   1.5%  89.1% 84473564  14.7% HTTP_substream_process_ctx_create
7654262   1.3%  90.5% 7654262   1.3% asnl_enc_save
7311586   1.3%  91.7% 7311586   1.3% HTTP_get_modify_value_by_name
6855757   1.2%  92.9% 6855757   1.2% pt_stream_create_svrinfo
5851046   1.0%  93.9% 5851046   1.0% _hlp_parse_cookie
5136808   0.9%  94.8% 5136808   0.9% HTTP_process_ctx_create
```

### 5) Use graph tool to analyze the function call relationship from .heap files

This tool is for internal R&D investigation only. Just for reference.

- Generate a .dot file on FortiWeb backend shell:

```
jeprof --dot /bin/proxyd jeprof.out.4973.1641276249.heap > 1641276249.dot
```

Or add an option --base with a previous .heap file to get the difference between two heaps:

```
jeprof --base= jeprof.out.4973.1642276345.heap --dot /bin/proxyd
jeprof.out.4973.1641276249.heap > diff.dot
```

- Copy 1601044510.dot to ubuntu;

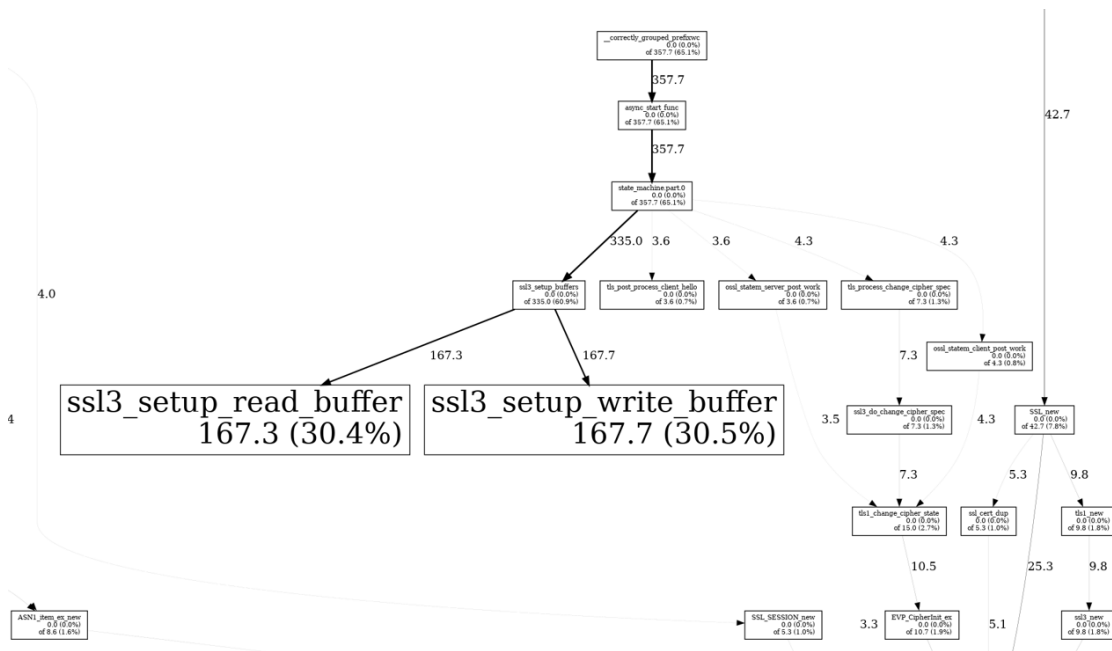
- Install graphviz on Ubuntu:

```
apt install graphviz
```

- Generate a png picture:

```
dot -Tpng 1641276249.dot -o 1641276249.png
```

A png image will be generated as below, indicating the top memory usage functions, and function call relationship. Taking the case below for example, one can check if HTTPS traffic load increased or related configuration is changed.



6) You can also download the jeprof.out files and provide them to support team for further investigation:

```

/var/log/gui_upload# ls jeprof.out* -l
-rw-r--r--  1 root    0          109251 Sep 27 18:30
      jeprof.out.11164.1632789019.heap
-rw-r--r--  1 root    0          111975 Dec 22 12:22
      jeprof.out.3777.1640200954.heap
    
```

**Note:** In `jeprof.out.3777.1640200954.heap`:

3777 is the PID of proxyd

1640200954 is the UNIX timestamp; one can use online tools to convert it to a human-readable date so as to just pay attention to recent dump files. This is useful to confirm the recent & current coredump files if there are many files.

E.g.:

[Epoch Converter - Unix Timestamp Converter](#)



## Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is **1640979152**

### Convert epoch to human-readable date and vice versa

 [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

**GMT** : Wednesday, December 22, 2021 7:22:34 PM

**Your time zone** : Wednesday, December 22, 2021 11:22:34 AM GMT-08:00

**Relative** : 9 days ago

- Besides jemalloc dump files, you can also generate proxyd pdump logs with the following command. These logs named as "proxyd-objpool-\*.txt" include memory statistics information for key data structures. You can find these logs in the same directory, but manually download them via **System > Maintenance > Backup & Restore**, because these logs are not included in the one-click download debug log "console\_log.tar.gz".

```
FWB# diagnose debug jemalloc proxyd dump
/var/log/gui_upload# ls -l proxyd*
--ws--Sr-x 1 root 0 1417 Aug 3 10:38 proxyd-objpool-32741-1659548316.txt
--ws--Sr-x 1 root 0 1417 Aug 3 10:38 proxyd-objpool-32741-1659548336.txt
```

- As stated in point 2, after 6.4.0 GA release, a regular monitoring file is generated as /var/log/gui\_upload/debug\_memory.txt. One can set a memory boundary for it: if the memory usage reaches the boundary and proxyd or ml\_daemon is the top 10 high memory usage, it will enable their jemalloc debug function automatically.

```
FortiWeb # show full system global
config system global
    set debug-memory-boundary 70    #memory usage percentage, 1%-100%
End
```

## Diagnosing kernel memory leak issues

Sometimes, despite minimal or very low traffic, the memory utilization of the FortiWeb remains relatively high, for example, reaching around 80%. This situation could indicate the presence of a potential kernel memory leak. Run `cat /proc/meminfo` in Shell. Check if the slab (memory consumed by the kernel) is exceptionally high (reaching values of 1 GB or even 10 GB).

The following is an example of the output of `cat /proc/meminfo`.

```
MemTotal: 16186144 kB
MemFree: 481784 kB
MemAvailable: 13119360 kB
Buffers: 1106296 kB
Cached: 1378200 kB
SwapCached: 0 kB
Active: 3015388 kB
Inactive: 1157396 kB
Active(anon): 1693084 kB
Inactive(anon): 71832 kB
Active(file): 1322304 kB
Inactive(file): 1085564 kB
Unevictable: 47960 kB
Mlocked: 47960 kB
SwapTotal: 0 kB
SwapFree: 0 kB
Dirty: 128 kB
Writeback: 0 kB
AnonPages: 1735972 kB
Mapped: 170672 kB
Shmem: 81160 kB
KReclaimable: 10399120 kB
Slab: 10623512 kB
SReclaimable: 10399120 kB
SUnreclaim: 224392 kB
KernelStack: 6496 kB
PageTables: 13568 kB
NFS_Unstable: 0 kB
Bounce: 0 kB
WritebackTmp: 0 kB
CommitLimit: 8093072 kB
Committed_AS: 5777048 kB
VmallocTotal: 34359738367 kB
VmallocUsed: 11028 kB
VmallocChunk: 0 kB
Percpu: 1984 kB
HugePages_Total: 0
HugePages_Free: 0
HugePages_Rsvd: 0
HugePages_Surp: 0
Hugepagesize: 2048 kB
Hugetlb: 0 kB
DirectMap4k: 88204 kB
DirectMap2M: 4022272 kB
DirectMap1G: 12582912 kB
```

In this case, it's recommended to run the following command to release cache every 45 minutes.

```
config system settings
  set enable-cache-flush enable
end
```

- By default, `enable-cache-flush` is enabled on FortiWeb-VM and disabled on FortiWeb appliance.
- The system only logs the operations when the feature is enabled or disabled. No event log is recorded for each cache flush that occurs every 45 minutes.

- Even if the memory usage is not high, when `enable-cache-flush` is enabled, the cache is flushed every 45 minutes as per the configuration.

## Checking disk information & issues

### 1. Check hard disk & raid info:

```
FortiWeb# diagnose hardware harddisk list
name      size(M)
sda       959656.76
sdb       8012.39
```

```
FortiWeb # diagnose system mount list
Filesystem      1M-blocks      Used Available Use% Mounted on
/dev/ram0        473            310      162    65% /
none            1164           31       1132    2% /tmp
none            3880           3        3877    0% /dev/shm
/dev/sdb1        362            254      89     74% /data
/dev/sdb3        91             0        86     0% /home
/dev/sda1        449651         7771    418971  1% /var/log
```

```
FortiWeb# diagnose hardware logdisk info
disk number: 1
disk[0] size: 937.16GB
raid level: raid1
partition number: 1
mount status: read-write
```

### 2. Check RAID information:

```
FortiWeb# diagnose hardware raid list
level  size(M)  disk-number
raid1  899811   0 (OK), 1 (OK)
```

```
FortiWeb# diagnose hardware raid-card info
FW Package Build: 50.5.0-1121
```

## MegaCli

Usually we need to pay attention to fields like below when checking the output:

- Slot number and device ID
- Firmware status (a failed disk will show Failed)

### 3. Initialize RAID:

Use the this command to initialize the RAID

Currently, only RAID level 1 is supported, and only on FortiWeb 1000B/C/D/E, 2000E, 3000C/CFsx, 3000E, and 4000E shipped with FortiWeb 4.0 MR1 or later.

```
FortiWeb# execute create-raid level raid1
```

### 4. Rebuild RAID:

Use this command to rebuild the RAID.

Currently, only RAID level 1 is supported, and only on FortiWeb-1000B, 1000C, 3000C/CFsx, 3000E, and 4000E shipped with FortiWeb 4.0 MR1 or later.

```
FortiWeb# execute create-raid rebuild
This operation will clear all data on disk :0!
Do you want to continue? (y/n)
```

## Retrieving system&debug logs

To troubleshoot system level issues, we often need to analyze system logs. Some of these logs are generated by daemons while some others are generated by scripts, which run periodically in the background to record system resource changes, statistics, etc.

Please collect such logs for further investigation.

### Retrieving system logs in backend system

#### 1. dmesg

Dmesg is used to examine or control the kernel ring buffer. It includes all important kernel information such as hardware loading and call trace information. Kernel level traffic debug logs will be also included in dmesg.

One can check such logs with “# dmesg” or “#dmesg | grep xxx” directly;

For further troubleshooting, you can archive all logs under the directory /var/log/dmesg/:

```
tar czf /var/log/gui_upload/dmesg.tar.gz /var/log/dmesg/
```

#### Notes:

By default, dmesg uses a time stamp notation of seconds and nanoseconds since the local kernel started, and it's not in a human-friendly format. If you need to check the accurate time, please check the "/var/log/dmesg/kern.log".

kern.log contains the latest dmesg information, and other logs started with kern.log are backup logs.

#### 2. Apache error logs

If one failed to do some GUI related operation, please collect this logs for analysis:

```
/var/log# ls apache_logs/
error_log
```

#### 3. CMDB logs

For configuration deployment issues, please collect cmdb logs for analysis:

```
# ls /var/log/cmdb/cmdb.log.*
cmdb/cmdb.log.0      cmdb/cmdb.log.155  cmdb/cmdb.log.211  cmdb/cmdb.log.44
#ls /var/log/dbg_cli/
```

#### 4. /var/log/debug/

Some real-time logs will be generated and stored at /var/log/debug/:

```
/# ls /var/log/debug/
collect_tcpdump_para.txt  daemon_log_flag  proxyd_dbg
coredump_log_flag        dbsync_log       sample
crash.log                kernel.log       system-startup.log
crash_log_flag           kernel_log_flag  tmp
```

```
crl_updated_dbg          netstat_log_flag      daemon.log             nstd
```

### 5. /var/log/gui\_upload/

1) Core, coredump and some real-time logs will be generated and stored at /var/log/gui\_upload/:

```
/# ls /var/log/gui_upload/
core-proxyd-2141-1630609770    dlog_logd             ha_event_log
core-proxyd-7794-1630610047    ints.txt              debug_disk.txtirq
jeprof.out.51146.1630448785.heap  perf.data            kern.log
debug_out_d_cond_cpu.sh.txt     debug_out_d_mem.sh.txt  debug_out_d_
    net.sh.txt
debug_out_d_proc.sh.txt
```

2) Some logs named as “debug\_<function name>.txt” (or with the prefix “debug\_out\_d\_” in some intermediate builds) are generated after 6.4.1.

- Scripts in /var/log/debug/sample/ are samples to run in /var/log/outgoing;
- Scripts in /var/log/outgoing/ are scripts actually run in /var/log/outgoing;
- Currently these system information are collected:

```
/# ls /var/log/debug/sample/          #script samples
README          d_cond_cpu.sh  d_mem.sh      d_net.sh      d_proc.sh      first_
flag
/# ls /var/log/outgoing/              #scripts actually run
d_cond_cpu.sh  d_mem.sh      d_net.sh      d_proc.sh
/# ls -l /var/log/gui_upload/debug_out_d_*  (in new builds files are debug_
    <function name>.txt)
-rw-r--r--    1 root    0                65018 Sep 28 18:03 /var/log/gui_
    upload/debug_out_d_cond_cpu.sh.txt
-rw-r--r--    1 root    0                119859 Sep 28 18:03 /var/log/gui_
    upload/debug_out_d_mem.sh.txt
-rw-r--r--    1 root    0                66371 Sep 28 18:03 /var/log/gui_
    upload/debug_out_d_net.sh.txt
-rw-r--r--    1 root    0                126484 Sep 28 18:03
/var/log/gui_upload/debug_out_d_proc.sh.txt
```

- The information collected by these scripts mainly include:

d\_cond\_cpu.sh: If the CPU usage more than 90% - date, top 10 daemons of CPU usage, perf top for 10 seconds

d\_mem.sh: date, free, /proc/meminfo, etc.

d\_net.sh: date, netstat -natpu, route -n

d\_proc.sh: date, top -b -n1, ps

- The running interval for these scripts can be set with CLI:

```
FortiWeb # show full system global
config system global
    set debug-monitor-interval 5    #minutes
End
```

If the script is blocked for 30 sec, the system will kill it and call it in the next debug-monitor-interval.

- If necessary, one can add scripts (shell or python) to this directory to collect system information; (NOT Recommended, because too many these manually-added tasks may impact system running & stability)
- The size of “debug\_<function name>.txt” is limited to 25MB. If the size gets greater, it will be moved to an .old file. And there are only two files rotated.

3) **NMON** logs are generated after 6.4.0.

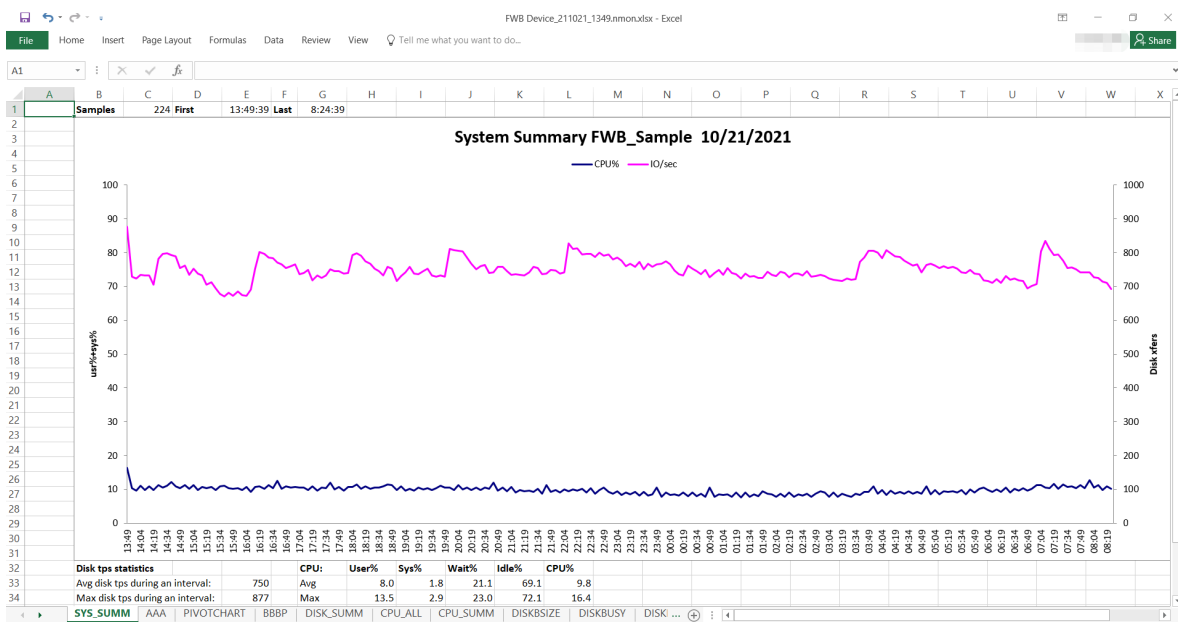
NMON (shorthand for Nigel's Monitor) is a system monitor tool that can collect system performance statistics including CPU, Mem, Disk, Net, etc.

- NMON log files (with a suffix .nmon) are generated automatically and stored at /var/log/debug/tmp, and will be archived and can be downloaded via the method described in below section 10.2. The maximum number of .nmon files stored is 180.
- A .nmon file is generated with a sampling interval of 5 minutes, and each time when system boots up, a new .nmon file will be generated. So generally only one .nmon file named “FortiWeb\_220107\_1734.nmon” (may be different on some previous builds) will be generated each day. Multiple .nmon files generated in one day indicate that system rebooted or crashed.

G:\Downloads\console\_log.tar.gz\console\_log.tar\var\log\debug\http\_download\_log\

Name	Size	Packed Size	Modified	Mode	User	Group
core-proxyd-19284-1623682574.gz	38 557 990	38 558 208	2021-10-22 01:26	-rw-----	root	0
core-proxyd-20764-1620056130.gz	67 661 931	67 662 336	2021-10-22 01:26	-rw-----	root	0
core-proxyd-24022-1623588026.gz	62 206 015	62 206 464	2021-10-22 01:27	-rw-----	root	0
coredump	477	512	2021-10-22 01:26	-rw-r--r--	root	0
crash	0	0	2021-10-22 01:26	-rw-r--r--	root	0
daemon	6 690 503	6 690 816	2021-10-22 01:26	-rw-r--r--	root	0
debug_disk.txt	8 888 693	8 888 832	2021-10-22 01:26	-rw-r--r--	root	0
jeprof.out.3271.1629878388.heap	134 308	134 656	2021-10-22 01:26	-rw-r--r--	root	0
kernel	0	0	2021-10-22 01:26	-rw-r--r--	root	0
netstat	0	0	2021-10-22 01:26	-rw-r--r--	root	0
sn.txt	96	512	2021-10-22 01:27	-rw-r--r--	root	0
WAF_WPA_PIO_210927_1122.nmon	81 069	81 408	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_210927_1348.nmon	538 481	538 624	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_210928_1348.nmon	563 665	563 712	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_210929_1348.nmon	576 816	577 024	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_210930_1348.nmon	576 568	577 024	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_211001_1348.nmon	574 588	574 976	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_211002_1348.nmon	574 603	574 976	2021-10-22 01:26	-rw-r--r--	root	0
WAF_WPA_PIO_211003_1348.nmon	575 016	575 488	2021-10-22 01:26	-rw-r--r--	root	0

- After processed by an nmon analyzer:



4) Jemalloc dump logs for proxyd & ml\_daemon.

Please refer to [Diagnosing memory leak issues](#).

Jemalloc dump logs named as “jeprof.out.\*.\*.heap” can be generated manually by executing `diagnose debug jemalloc proxyd dump`, or produced automatically when the total system memory usage reaches the boundary value (70% by default).

Jeprof information is very useful when debugging memory issues for proxyd & machine learning.

5) Jemalloc pdump logs for proxyd.

Please refer to [Diagnosing memory leak issues](#).

Jemalloc pdump logs named as “proxyd-objpool-\*.\*.txt” can be generated manually by executing `diagnose debug jemalloc proxyd pdump`.

Such logs include memory statistics information for key data structures, and only proxyd supports generating these logs. When analyzing proxyd issues, you can also collect both dump and pdump logs at the same time.

6) Proxyd watchdog logs generated from 7.0.1.

Proxyd watchdogs logs are useful when analyzing proxyd thread lock issues.

If a proxyd thread is stuck for 5 or 60 seconds, FortiWeb will write a debug message like “proxyd worker thread [1] stuck for 5 (or 60) seconds” into the `/var/log/debug/daemon.log` and generate a log file named like “watchdog-proxyd-3991-1658580435.bt” under the `/var/log/gui_upload/`.

Watchdog logs mainly include “pstack <proxyd>” information. And `/var/log/debug/daemon.log` is included in the one-click downloaded debug file “console\_log.tar.gz”.

From 7.0.1 to 7.0.3, the default stuck time period is 5, while on 7.0.4 and newer builds, the time is changed to 60 seconds.

7) Console output log (COMlog) generated from 7.0.2

COMlog refers to system outputs that are printed out to console terminal automatically when system reboots or encounters unexpected problems, and the logs displayed on console when you configure directly on the console terminal.

```
/# ls -l /var/log/gui_upload/ | grep console
-rw-r--r-- 1 root 0 8261 Aug 8 13:45 console.log
```

This information can be used for troubleshooting if unexpected behavior starts to occur, or when you need to collect console prints while lacking SSH permission for security purposes.

COMlog can record up to 4 MB of console output to the kernel ring buffer, and also supports reading the content and writing it to a log file “`/var/log/gui_upload/console.log`”.

- To enable/disable the COMlog:

```
diagnose debug comlog enable/disable #dump & read will only take effect after comlog is enabled
```

COMlog is enabled by default. To change the default behavior and save it to configuration file, run:

```
config system global
  set console-log enable/disable
end
```

**Notes:** when console-log is enabled, `diagnose debug comlog` will also be enabled.

- To view the COMlog status, including speed, file size, and log start and end:

```
FWB # dia debug comlog info
ttyname: /dev/pts/1 com_speed = 9600
control = Logging enabled #COMlog is enabled
```

```
log_space = 4186042/4194304
log_start = 0
log_end = 8261
log_size = 8261
```

- To dump the COMlog from the kernel ring buffer:  
diagnose debug comlog dump
- To read the COMlog from ring buffer and write to /var/log/gui\_upload/console.log:  
FWB # diagnose debug comlog read  
Dump log to /var/log/gui\_upload/console.log done.
- To clear the COMlog in the kernel ring buffer:  
diagnose debug comlog clear

**Notes:**

- COMlog will be written into the "console.log" only after you execute `diagnose deb comlog read`;
- Every time after executing `diagnose deb comlog read`, the content of "console.log" will be overwritten, so if you execute it after system reboots, the logs saved before rebooting will be lost.

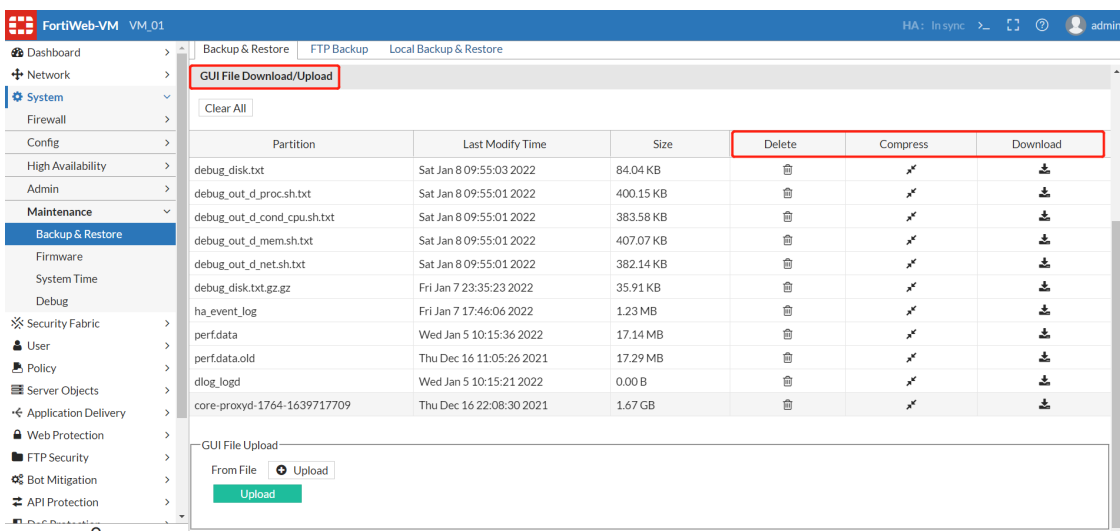
Due to the two limitations above, console output for kernel coredump or other issues that cause system reboot cannot be recorded in "console.log". FortiWeb will enhance this limitation in future builds.

## Customizing and downloading debug logs

There are several ways to collect or customize debug logs.

1. Many debug logs are stored at /var/log/gui\_upload and can be downloaded via GUI:
  - a. Enable upload/download option in CLI first, then you'll see the section GUI File Download/Upload in **System > Maintenance > Backup & Restore**:  

```
config system settings
  set enable-file-upload enable
end
```



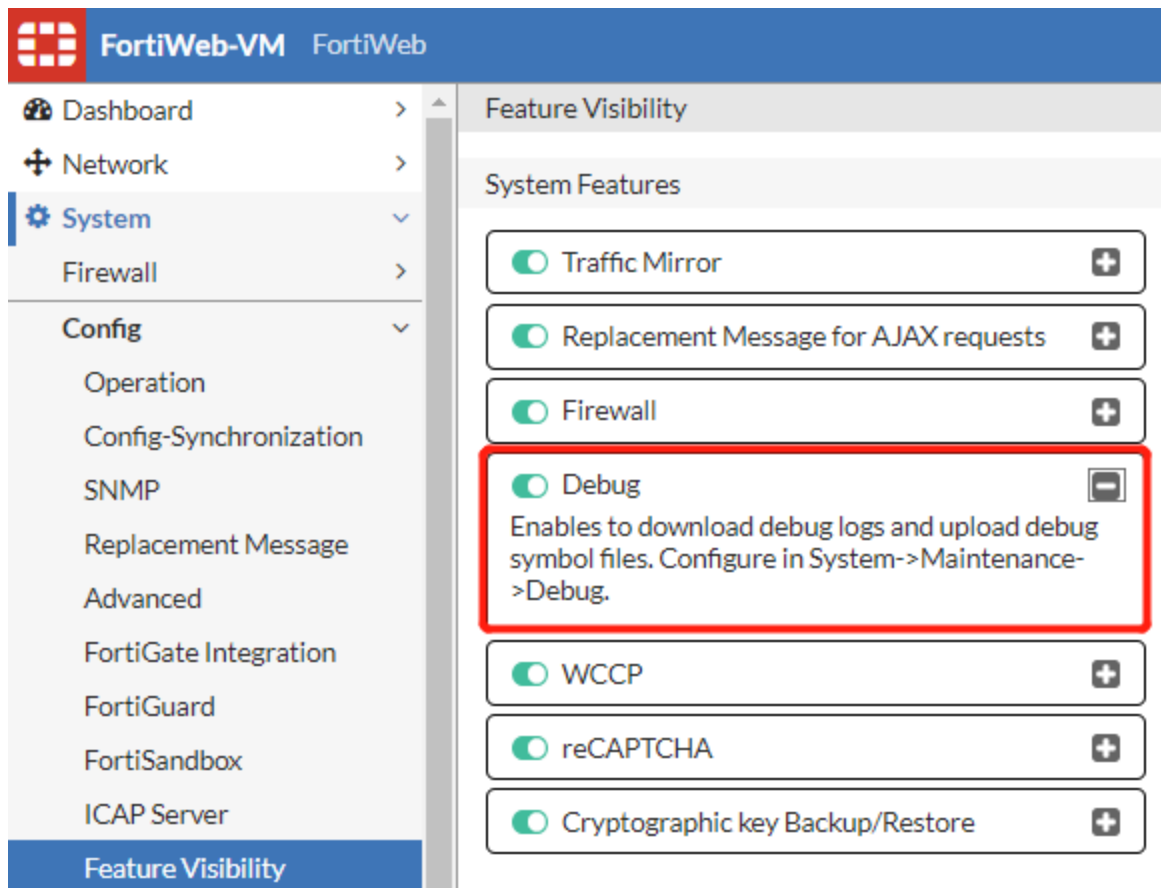
- b. Select, compress and download debug logs or core/coredump files that you need.
- c. You can also login the backend shell, move or copy logs files from other directories to /var/log/gui\_upload, and download them here.

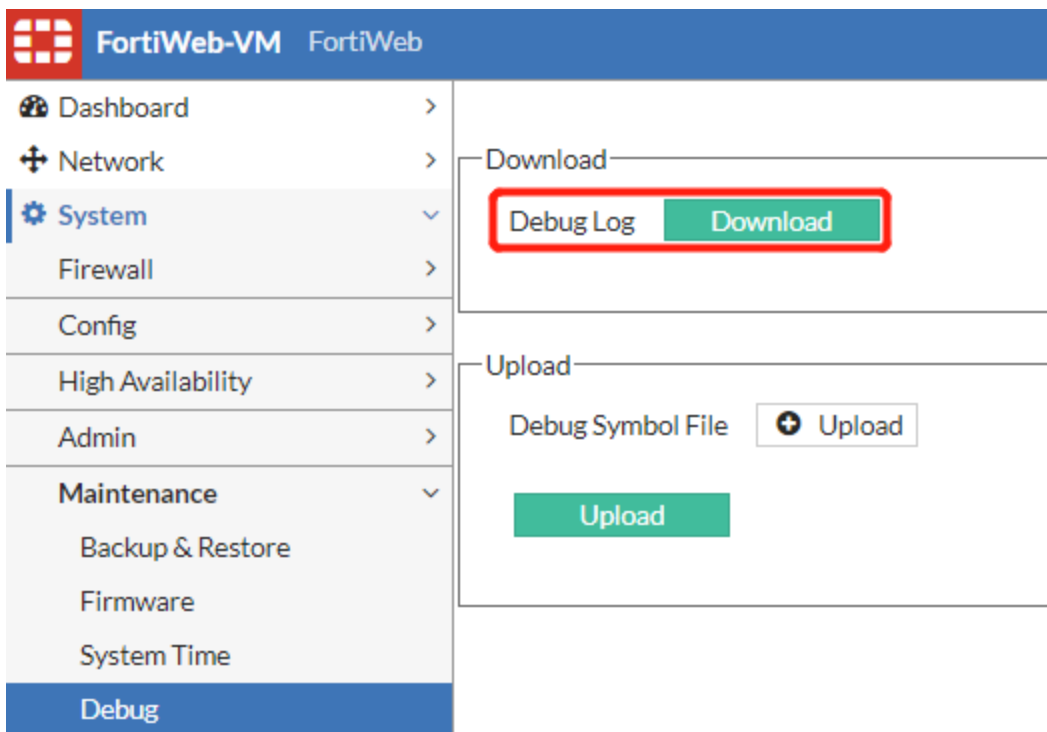
2. One-click to archive and download most important logs (Recommended Way)

FortiWeb GUI provides an easier way to collect such debug logs. Most logs under /var/log/debug/ and /var/log/gui\_upload will be archived after you click the “Download” button on **System > Maintenance > Debug > Download** section.

Before you can begin downloading the debug log, you have to enable it first via **System > Config > Feature Visibility > Debug**.

Please note that some logs and core/coredump files may not be included in this archive file, so you may need to download them manually with the first method.





As more features or debug logs are added on 7.0.1, 7.0.2, and later builds, more logs will be included in this debug log, and different types of logs are classified into sub-directories:

G:\Downloads\console\_log (5).tar.gz\console\_log (5).tar\var\log\debug\http\_download\_log\

Name	Size	Packed Size	Modified	Mode	User
sn.txt	100	512	2021-09-28...	-rw-r--r--	root
netstat	0	0	2021-09-28...	-rw-r--r--	root
kernel	1 728 095	1 728 512	2021-09-28...	-rw-r--r--	root
jeprof.out.11164.1632789019.heap	109 251	109 568	2021-09-28...	-rw-r--r--	root
FortiWeb_210928_1728.nmon	30 714	30 720	2021-09-28...	-rw-r--r--	root
FortiWeb_210927_1728.nmon	428 994	429 056	2021-09-28...	-rw-r--r--	root
FortiWeb_210926_1728.nmon	428 362	428 544	2021-09-28...	-rw-r--r--	root
FortiWeb_210925_1727.nmon	428 371	428 544	2021-09-28...	-rw-r--r--	root
debug_memory.txt	2 109 009	2 109 440	2021-09-28...	-rw-r--r--	root
debug_disk.txt	16 703 984	16 704 000	2021-09-28...	-rw-r--r--	root
daemon	1 840 584	1 840 640	2021-09-28...	-rw-r--r--	root
crash	0	0	2021-09-28...	-rw-r--r--	root
coredump-2021-08-29-05_51.gz	281 774 239	281 774 592	2021-09-28...	-rw-----	root
coredump-2021-01-08-05_55.gz	289 008 348	289 008 640	2021-09-28...	-rw-----	root
coredump	0	0	2021-09-28...	-rw-r--r--	root
core-2021-01-08-05_55.gz	14 164	14 336	2021-09-28...	-rw-r--r--	root

3. You can run diagnose debug commands to customize logs included in the archive debug file.  
 For example, you can capture the flow from the client 216.232.182.247 and activate the debug flow from it as below. Then you'll find that the following files will be included in the downloaded debug file console\_log.tar.gz:

- sn.txt: SN & current build
- entire configuration file
- crash logs
- daemon logs: the debug flow trace logs is included in this file
- kernel logs
- netstat logs
- coredump logs
- perf logs
- top logs
- nmon logs: regular record
- jeprof.out.\*.\*.heap: need to enable jemalloc-conf and trigger jemalloc dump first
- debug\_net/disk/mem/process.txt or debug\_out\_d\_mem/net/proc/cond.sh.txt: regular record
- collect\_xxx: captured pcap file (diagnose CLI filtered output) and other debug information
- other logs

```
FortiWeb # diagnose debug trace tcpdump filter "host 216.232.182.247 and port 443"
FortiWeb # diagnose debug flow filter client-ip "216.232.182.247"
FortiWeb # diagnose debug flow filter flow-detail 7
FortiWeb # diagnose debug trace report
FortiWeb # diagnose debug trace report start
Then wait to collect traffic...
FortiWeb # diagnose debug trace report stop
Then you can click the "Download" button on System > Maintenance > Debug > Download to download the archive file:
```

G:\Downloads\console\_log (10).tar.gz\console\_log (10).tar\var\log\debug\http\_download\_log\

Name	Size	Packed Size	Modified	Mode	User	Grot
FWB-AWS-M01_210823_2202.nmon	479 609	479 744	2021-10-04...	-rw-r--r--	root	0
FWB-AWS-M01_210822_2202.nmon	480 777	481 280	2021-10-04...	-rw-r--r--	root	0
FWB-AWS-M01_210821_2202.nmon	478 627	478 720	2021-10-04...	-rw-r--r--	root	0
FWB-AWS-M01_210820_2202.nmon	479 665	479 744	2021-10-04...	-rw-r--r--	root	0
FWB-AWS-M01_210820_0055.nmon	447 644	448 000	2021-10-04...	-rw-r--r--	root	0
debug_out_d_proc.sh.txt	73 627	73 728	2021-10-04...	-rw-r--r--	root	0
debug_out_d_net.sh.txt	58 722	58 880	2021-10-04...	-rw-r--r--	root	0
debug_out_d_mem.sh.txt	83 481	83 968	2021-10-04...	-rw-r--r--	root	0
debug_out_d_cond_cpu.sh.txt	58 464	58 880	2021-10-04...	-rw-r--r--	root	0
debug_memory.txt	118 772	118 784	2021-10-04...	-rw-r--r--	root	0
debug_disk.txt	6 194 083	6 194 176	2021-10-04...	-rw-r--r--	root	0
daemon	912 499	912 896	2021-10-04...	-rw-r--r--	root	0
crash	0	0	2021-10-04...	-rw-r--r--	root	0
coredump	0	0	2021-10-04...	-rw-r--r--	root	0
collect_top	6 159	6 656	2021-10-04...	-rw-r--r--	root	0
collect_tcpdump.pcap	7 001	7 168	2021-10-04...	-rw-r--r--	root	0
collect_perf	8 192	8 192	2021-10-04...	-rw-r--r--	root	0
collect_other	4 224	4 608	2021-10-04...	-rw-r--r--	root	0
collect_fw_b_system.conf.zip	7 634 830	7 634 944	2021-10-04...	-rw-r--r--	root	0

**Note:** To access this part of the web UI, your administrator’s account must have the prof\_admin permission. For details, see "Permissions" in FortiWeb Administration Guide.

## Diagnose Crash & Coredump issues

- [Common troubleshooting steps on page 90](#)
- [Checking core files and basic coredump information on page 90](#)
- [Collecting core/coredump files and logs on page 93](#)
- [What to do when coredump files are truncated or damaged on page 97](#)

### Common troubleshooting steps

When you find an unexpected system reboot or intermittent connection interrupt, the system may encounter a daemon or kernel crash. At this time the most important thing is to collect core/coredump files and system logs, then provide them to R&D for further analysis immediately.

Common checking & analyzing steps:

- Check if daemon or kernel coredump files are generated
- Check the basic coredump information
- Download core & coredump files
- Collect & download system logs (Listed in [Customizing and downloading debug logs on page 86](#), including dmesg & other debugs logs)
- Possible temporary workaround/solution:
  - Restore the latest configuration or remove newly-added configuration
  - Move away newly migrated traffic if there is
- Submit bugs and provide information collected for further analysis

### Checking core files and basic coredump information

When you suspect that a system or daemon crash happened, one can use diagnose commands to confirm and check the basic information.

1. Confirm that `enable-debug-log` is enabled, so that FortiWeb will record crash, daemon, kernel, netstat, and core dump logs.

```
FortiWeb# show full-configuration sys settings
config system settings
    set enable-debug-log enable    #enabled by default
end
```

2. Check if `enable-core-file` is enabled or not.

```
FortiWeb# show full-configuration system settings
config system settings
    set enable-core-file enable #disabled by default on 7.0.4 and later builds
end
```

1) On 7.0.3 and previous builds including 6.3.x, this option is enabled by default. That means if daemon coredump happens, a coredump file which includes the snapshot of the current memory will be generated. However, generating a coredump file usually takes from several seconds to several minutes, especially on a device with large memory size. During this period, the program stops providing service.

2) On 7.0.4 and later builds, `enable-core-file` is set as disable by default. FortiWeb also optimizes the coredump mechanism thus more useful information can be recorded even if without a coredump file. You

need to use “diagnose debug crashlog show” as below to collect stack information for the crashed daemon.

3. Use “diagnose debug crashlog show” to check if any core dump files are generated or collect the stack information.

1) On 7.0.1 and previous builds including 6.3.x:

Only daemon (proxyd, ml, etc.) core dump files can be listed, so it is better to double check via GUI to see if kernel core dump occurred.

The files are named with a Unix timestamp, so you need to convert it into a human-readable date and time format to see if it’s a newly generated one. (Refer to the below section Notes for details)

```
FWB# diagnose debug crashlog show
core-proxyd-2141-1630609770
core-proxyd-60152-16306095792)
```

2) On 7.0.2 and later builds:

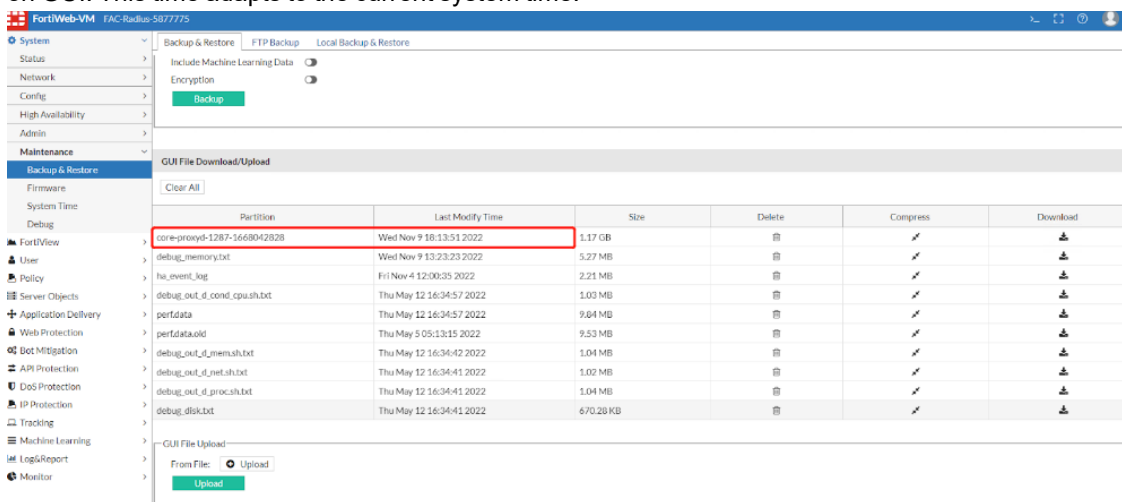
- Both daemon and kernel core dump files will be shown by this command.
- The files are named with a readable timestamp. Just note the timestamp for kernel core & core dump files are adjusted to fit the system time & timezone, while the daemon core dump filename is using the UTC time.

```
FWB# diagnose debug crashlog show
core-2022-11-09-16_40-7.0.2-B0090
coredump-2022-11-09-16_40-7.0.2-B0090
core-proxyd-10984-1668037208-UTC-2022-11-09-23_40-7.0.2-B0090
```

- If enable-core-file is disabled, the function stack information will be shown instead of the core dump files. Please collect these information for developer analysis.

```
FWB# diagnose debug crashlog show
2022-11-09 15:59:20 <10359> application proxyd
2022-11-09 15:59:20 <10359> *** signal 6 received ***
2022-11-09 15:59:20 <10359> __poll[0x7fcb81055580 + 0x4f]
2022-11-09 15:59:20 <10359> dbg_writedisk_unlock_func[0x8ab4b0 + 0x20f2]
2022-11-09 15:59:20 <10359> main[0x4df5a0 + 0x154]
2022-11-09 15:59:20 <10359> __libc_start_main[0x7fcb80f8cc20 + 0xeb]
2022-11-09 15:59:20 <10359> _start[0x4e0f20 + 0x2a]
```

On all builds, an easier way to judge if core or core dump files are new is checking the Last Modify Time on GUI. This time adapts to the current system time.



4. Use “diagnose debug coredumplog show” to show daemon core dump. Only daemon core dump information can be shown here.

```
FortiWeb# diagnose debug coredumplog show
```

```

===== coredump about /var/log/gui_upload/core-proxyd-4830-1639993541 =====
(gdb) 0 0x0000563f7b340e24 in pth_comm_add_pb_adom_entry ()
1 0x0000563f7b48584c in session_management_get_weight ()
0000002 0x0000563f7b4b23b2 in ip_intelligence_session_init_do_action ()
3 0x0000563f7b4b262d in ip_intelligence_session_init ()
4 0x0000563f7b3343ff in pth_init_modinfo ()
5 0x0000563f7b310797 in pt_service_HTTP_init ()
6 0x0000563f7b30959c in pt_service_init ()
7 0x0000563f7b3837bb in pt_stream_create_service ()
8 0x0000563f7b3842f1 in pt_stream_create ()
9 0x0000563f7b38a3d4 in session_accept ()
10 0x0000563f7b350cba in fd_epoll_poll ()
11 0x0000563f7b39622d in _worker_loop ()
0000012 0x0000563f7b3965f8 in worker_run ()
13 0x00007fa62d314f27 in start_thread () from /fwdev2//lib/libpthread.so.0
14 0x00007fa6269ff1df in clone () from /fwdev2//lib/libc.so.6
(gdb)

```

From above information from bug #770008 (already fixed on 6.3.18), it seems the coredump is related to client management configuration, so one workaround applied at that time was disable the block settings in client management

**Note:**

Notes: On 7.0.1 and previous builds, the format of core files are defined by:

```

/# more /proc/sys/kernel/core_pattern
/var/log/gui_upload/core-%e-%p-%t

```

%e: daemon/process name

%p: PID of the process

%t: UNIX timestamp; one can use online tools to convert it to a human-readable date. This is useful to confirm the recent & current coredump files if there are many files. (Of course, you can also check the file created time from “Last Modified Time” via **System > Maintenance > Backup & Restore > GUI File Download/Upload**)

E.g.:

[Epoch Converter - Unix Timestamp Converter](#)



## Epoch & Unix Timestamp Conversion Tools

The current Unix epoch time is **1637782895**

### Convert epoch to human-readable date and vice versa

Timestamp to Human date [\[batch convert\]](#)

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:

**GMT** : Thursday, September 2, 2021 7:09:30 PM  
**Your time zone** : Thursday, September 2, 2021 12:09:30 PM GMT-07:00 DST  
**Relative** : 3 months ago

Actually you have another way to simply check the file generation date from GUI; just check the section below to find "Download core/coredump files".

### Collecting core/coredump files and logs

As stated in above section, core/coredump files formatted as core-\* and coredump-\* can be downloaded from **System > Maintenance > Backup & Restore > GUI File Download/Upload**.

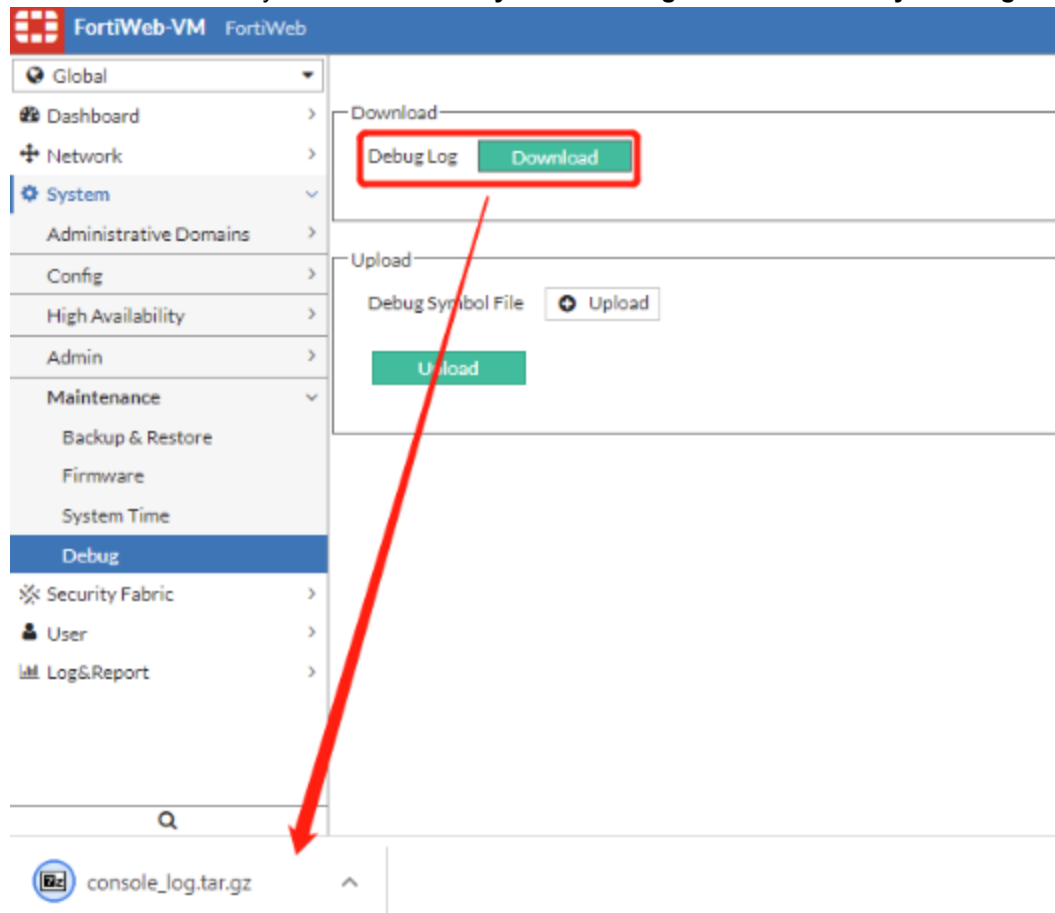
It's also necessary to collect some other logs that can help to analyze the coredump causes.

Please collect these logs:

1. Download the archived debug log with one-click button (**System > Maintenance > Debug > Download**). The archive file includes most logs under /var/log/debug/, /var/log/gui\_upload and some other system directories.

Please refer to [Customizing and downloading debug logs](#).

Please remember that you have to enable **System > Config > Feature Visibility > Debug** at first.



2. Download core/coredump files and other logs that are not archived in the debug log. Core and coredump files are usually very big, so they are not included in the one-click debug log file. Some other bugs such as complete dmesg logs and ha\_event\_log are not included at earlier builds especially when they're added by new features, so it's better for you to check the one-click downloaded debug file and see which logs are not included. For these logs, you can download via **System > Maintenance > Backup & Restore > GUI File Download/Upload**:

The screenshot shows the FortiWeb GUI's 'Backup & Restore' section. The 'Backup' button is highlighted. Below, the 'GUI File Download/Upload' section shows a table of files. Two files are highlighted with red boxes: 'ha\_event\_log' and three 'core-proxyd' files.

Partition	Last Modify Time	Size
debug_disk.txt	Fri Apr 29 14:27:01 2022	17.60 MB
debug_out_d_memsh.txt	Fri Apr 29 14:26:47 2022	8.93 MB
debug_out_d_netsh.txt	Fri Apr 29 14:26:47 2022	2.35 MB
debug_out_d_procsh.txt	Fri Apr 29 14:26:47 2022	1.15 MB
debug_out_d_cond_cpu.sh.txt	Fri Apr 29 14:26:47 2022	707.80 KB
debug_out_d_procsh.txt.old	Fri Apr 29 08:26:46 2022	25.01 MB
debug_out_d_memsh.txt.old	Thu Apr 28 08:41:42 2022	25.01 MB
ha_event_log	Wed Apr 27 17:00:07 2022	94.88 KB
perfdata	Fri Apr 8 14:48:49 2022	18.03 MB
perfdata.old	Thu Apr 7 14:50:06 2022	20.82 MB
dlog_logd	Fri Apr 8 14:48:31 2022	0.00 B
debug_memory.txt	Fri Feb 4 10:19:29 2022	1.62 MB
core-proxyd-22687-1642662345	Wed Jan 19 23:05:46 2022	1.45 GB
core-proxyd-16273-1642661121	Wed Jan 19 22:45:21 2022	1.45 GB
core-proxyd-3292-1642659896	Wed Jan 19 22:24:56 2022	1.48 GB

Accordingly, these logs are stored at the following directories. Sometimes the support team may also require you to copy other log files to `/var/log/gui_upload`, then you can download them from GUI.

```
/var/log/gui_upload/core-*
/var/log/gui_upload/coredump-*
/var/log/dmesg/ : #You can archive this directory first by executing "tar czf /var/log/gui_
upload/dmesg.tar.gz /var/log/dmesg/"
```

ha\_event\_log: including very detailed HA init, switch, config-sync, heartbeat logs

**Note:** After 7.0.1 release, `/var/log/dmesg/*` & `ha_event_log` are already included in the archived debug log, so you do not need to download them separately.

3. Download core/coredump files (named as `core-*` and `coredump-*`), detailed dmesg logs, and other logs (not archived in the debug log, but can be seen directly in GUI File Download/Upload).

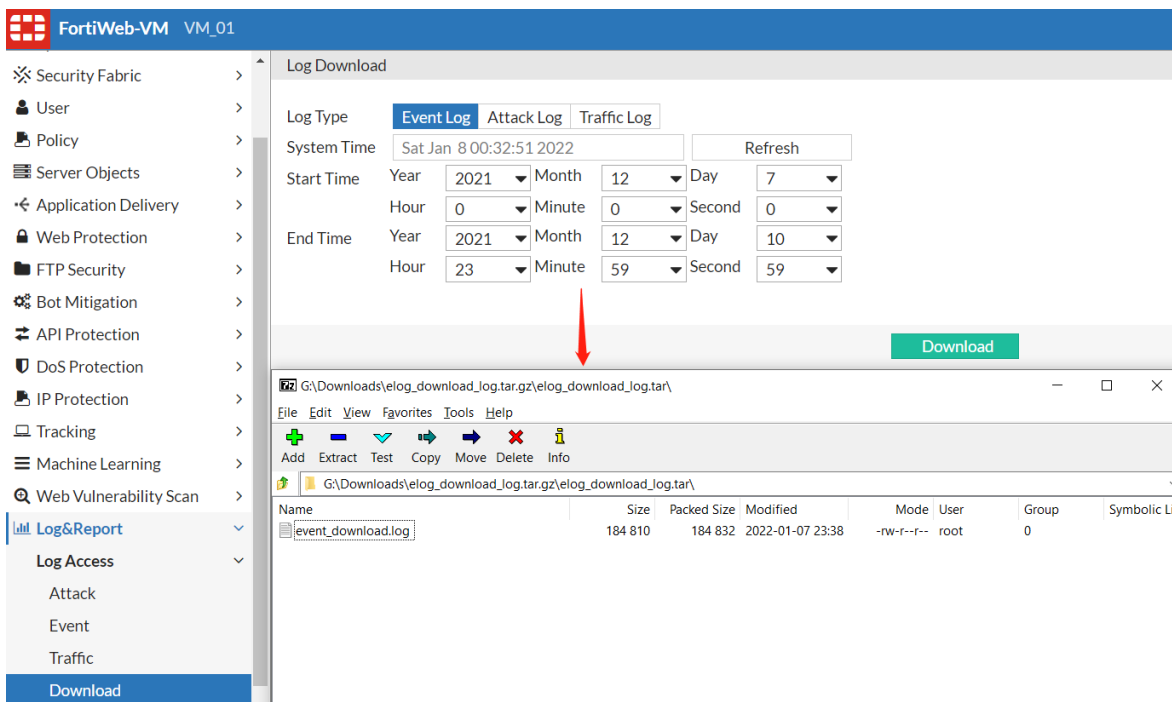
It's better to check the files in the one-click downloaded debug file to see which logs are not included, then just download them to avoid duplicate download.

```
/var/log/gui_upload/core-*
/var/log/gui_upload/coredump-*
```

```
/var/log/dmesg/: #You can archive this directory first by executing "tar czf
/var/log/gui_upload/dmesg.tar.gz /var/log/dmesg/"
```

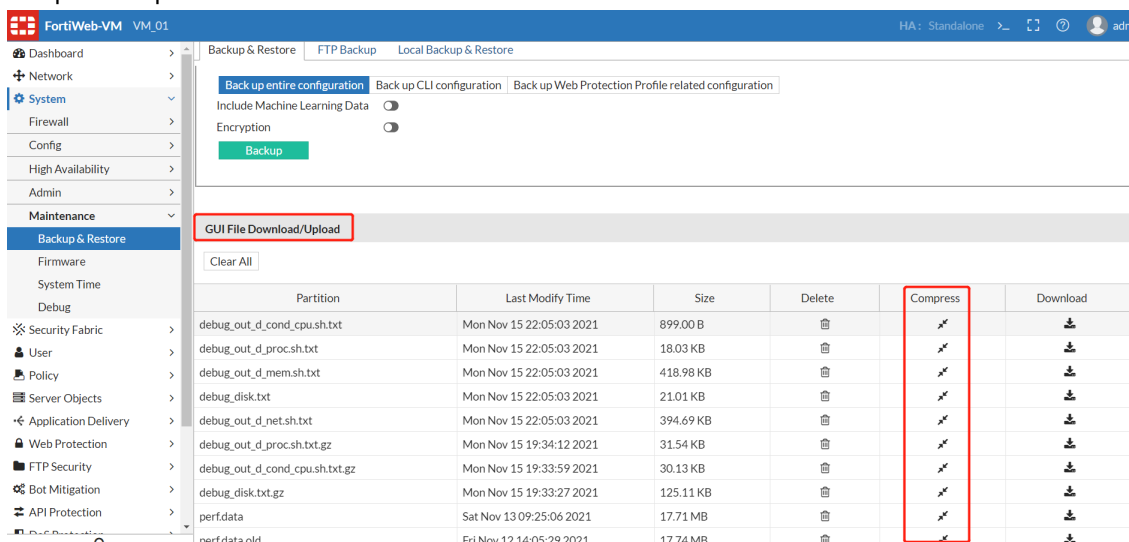
ha\_event\_log: including very detailed HA init, switch, config-sync, heartbeat logs

4. Download Event logs from **Log&Report > Log Access > Download**, selecting the corresponding time period;



**Note:**

- a. In 6.4.0, core and coredump files will be achieved and put a copy into /var/log/debug/tmp when one clicks to download the debug log (**System > Maintenance > Debug > Download Log**),
- b. In 6.4.1, 7.0.0 and later releases, all kernel core and coredump files will not be achieved and can be only downloaded from /var/log/gui\_upload. Please refer to the screenshot below, one can also compress a specific file before download it:



**5. Provide core/coredump files, dmesg and other necessary logs to the support team for further investigation.**

Usually you only needs to collect core/coredump, dmesg and other logs and provide them to support team for further analysis.

## What to do when coredump files are truncated or damaged

Sometimes you may find the size of a coredump file is 0, or obvious truncated stack information from the coredump file. It might mean the coredump file is truncated or damaged. To provide enough information to locate the root cause of a system/daemon crash, it's necessary to resolve the problem and generate a complete coredump file.

1. Check if disk space (especially /var/log) is enough for generating/storing a coredump file:

```
/# df -h
Filesystem      Size      Used Available Use% Mounted on
/dev/root       472.5M    335.7M   136.8M   71% /
none            1.1G     116.0K    1.1G    0% /tmp
none            3.8G      2.5M     3.8G    0% /dev/shm
/dev/sdb1       362.4M    213.7M   129.1M   62% /data
/dev/sdb3        90.6M     56.0K    85.6M    0% /home
/dev/sda1       439.1G     7.5G   409.3G    2% /var/log
```

2. Check if the size of coredump file generated is very large - in older versions there is a limit of 50G for proxyd core files.

3. Check if there is any file system issue:

```
FortiWeb# execute fscklogdisk
This operation will fsck logdisk !
Do you want to continue? (y/n)y
```

```
fsck logdisk...
FortiWeb#
```

4. Set `enable-core-file` to generate a complete coredump:

As mentioned in [Checking core files and basic coredump information](#), this option is enabled on 7.0.3 and previous builds including 6.3.x, while disabled by default on 7.0.4 and later builds. If necessary coredump information cannot be collected in the stack information without a coredump file, it might be useful to enable this option to generate coredump files for further investigation.

By default, if the coredump file is very large (usually with a FortiWeb box with large memory size), the time used to generate the core file and write to disk might be very long (several minutes to more than 10 minutes). The negative impact is that a reboot will be triggered if the dump cannot be completed in 120s, and the daemon will not respond to new requests during this period.

On FortiWeb 6.3.15 and later releases, a new option `enable-best-effort` for `set enable-core-file` is added. When this option is set, "hung task timeout" will not take effect. That is to say, we can always expect the system to generate a complete coredump file. This option is useful to analyze a tough issue, though it may cause the service to stop responding for a long time. Also, in 6.3.15 and later releases, the 50G core size limit has been removed.

```
FortiWeb# config server-policy setting
FortiWeb(setting) # set enable-core-file          #only works for proxyd
  disable          Disable coredump for proxyd.
  enable          Enable coredump action for proxyd, stop if coredump cannot finish in
                  hung task timeout seconds.
  enable-best-effort  Enable coredump action for proxyd, stop until the entire core
                  file is generated.
```

5. Other related configuration:

There are several other options related to coredump settings:

- **set core-file-count**

You can set the maximum daemon coredump files that can be stored to disk. If more core files are generated, the eldest one will be removed.

```
FortiWeb (setting) # set core-file-count
3 3
5 5
```

Please Note:

- This command only works for daemon coredump file. For kernel core and core dump files, the limitation is fixed as: only 1 coredump files; up to 5 core files.
  - This limitation works separately for different daemons. For example, if the count is set as 3, then up to 3 corefiles for the daemon proxyd or ml\_daemon is allowed. That is to say, a total of 6 coredump files can be allowed at the same time.
- **set corefile-ha-failover enable/disable for proxyd**

This option is introduced from 7.0.4 and applies to HA scenarios. In the previous implementation, if a proxyd coredump occurs on the primary device in a HA group, HA failover will not happen because the heartbeat still works and all link status and priority do not change. However the current service will be interrupted until the crashed daemon restarts successfully.

With this option enabled, once the system has detected a proxyd coredump file generating process being started, HA failover will be triggered immediately, thus the service will be recovered much faster. In this situation the previous primary device can take more time to generate the coredump file without impacting the application traffic.

To enable `corefile-ha-failover`, `enable-core-file` needs to be set as `enable` or `enable-best-effort` in advance:

```
FortiWeb # show server-policy setting
config server-policy setting
    set enable-core-file enable #or enable-best-effort
    set corefile-ha-failover enable
end
```

Please note:

- “set enable-core-file” and “set corefile-ha-failover” attributes will NOT be synchronized to other devices in the same HA group, so one needs to configure these configurations on each device if needed.
- Currently only one daemon - proxyd coredump can trigger the corefile-ha-failover. Corefile-ha-failover will not be triggered by other daemons.
- This function works in AP, AAS and AAHV modes, but is not suggested to be enabled in HA Manager modes in public clouds, because usually the load balancers in front of FortiWeb devices will do health checks and can guarantee that traffic is dispatched to the healthy nodes.
- It is recommended just to enable this option on one FortiWeb, usually the primary device only. Otherwise a proxyd coredump that can happen on both devices may lead to HA failover back and forth between two devices.

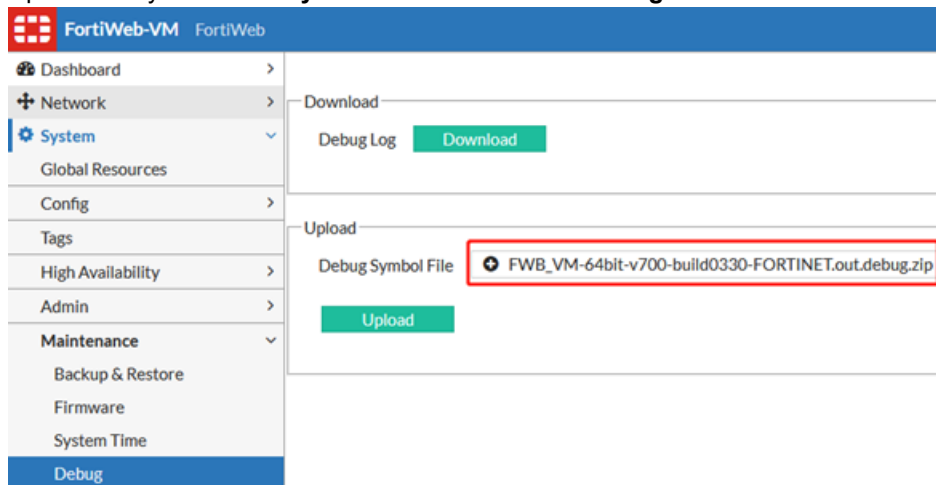
Please refer to "How is FortiWeb appliance elected to be the primary node?" in [FAQ](#) for more detailed description of this feature.

## Diagnose memory violation issues

From 7.2.0, you can use `diagnose debug asan` to collect memory violation events.

The following steps should be performed:

1. Please contact Fortinet Technical Support to get the Symbol file.
2. Enable **Debug** in **System > Config > Feature Visibility**.
3. Upload the symbol file in **System > Maintenance > Debug**.

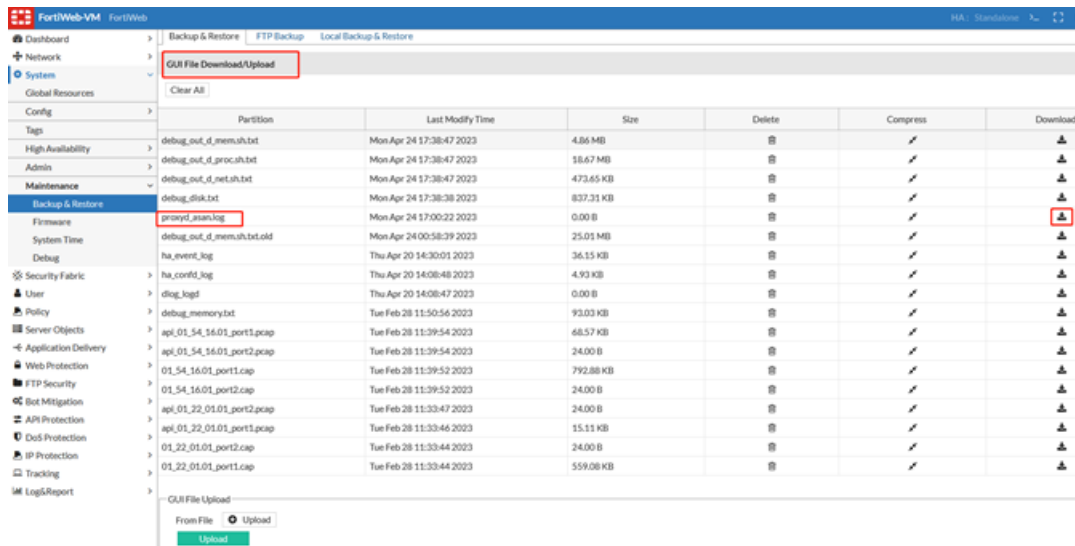


After the symbol file is uploaded, you should see the following directories created on FortiWeb:

```
/var/log/debug/symbol# ls -lh
drwxr-xr-x 3 root 0 4.0K Apr 24 16:58 asan
drwxr-xr-x 2 root 0 4.0K Apr 24 16:59 bin
drwxr-xr-x 2 root 0 12.0K Apr 24 16:58 lib
drwxr-xr-x 2 root 0 4.0K Apr 24 16:58 modules
-rwxr-xr-x 1 root 0 170.9M Apr 24 16:58 vmlinux
/var/log/debug/symbol#
```

4. Enable `proxyd asan` to collect memory violation events. Please note this consumes a large amount of memory thus may interfere traffic processing. Highly recommend to perform this step with the help of a Fortinet Support staff.  
Please be aware that enabling ASAN will respawn the `proxyd` daemon.  
`diagnose debug asan proxyd enable`
5. Wait for the system to collect memory violation events, and then check if the `proxyd_asan.log` file under `/var/log/gui_upload` is logged.
6. To download the `proxyd_asan.log` file in GUI, first enable the upload/download option in CLI:  
`config system settings`  
`set enable-file-upload enable`  
`end`

You will see the `proxyd_asan.log` in the **Backup & Restore** tab in **System > Maintenance > Backup & Restore**. Click the **Download** icon to download it.



7. Disable proxyd asan as soon as the root cause is located, so that the memory consumed by asan proxyd can be released.  
Please be aware that disabling ASAN will respawn the proxyd daemon.  
diagnose debug asan proxyd disable

# Diagnose software function issues

---

<b>Server policy</b> .....	<b>101</b>
<b>SSL/TLS</b> .....	<b>108</b>
<b>Application Delivery - URL Rewriting</b> .....	<b>123</b>
<b>Application Delivery - Site Publish</b> .....	<b>129</b>
<b>Application Delivery - Caching</b> .....	<b>145</b>
<b>Application Delivery - Lua Script</b> .....	<b>149</b>
<b>Application Delivery - Waiting Room</b> .....	<b>150</b>
<b>Web Protection - General Issues</b> .....	<b>152</b>
<b>Web Protection - Known Attack</b> .....	<b>158</b>
<b>Web Protection - Advanced Protection</b> .....	<b>162</b>
<b>Web Protection - Input Validation</b> .....	<b>168</b>
<b>Web Protection - Bot Mitigation</b> .....	<b>169</b>
<b>Web Protection - API Protection</b> .....	<b>170</b>
<b>Web Protection - IP Protection</b> .....	<b>171</b>
<b>Machine Learning - Anomaly Detection</b> .....	<b>172</b>
<b>ZTNA troubleshooting and debugging</b> .....	<b>180</b>
<b>HA issues</b> .....	<b>195</b>
<b>Log&amp;Report issues</b> .....	<b>216</b>
<b>Replacement message</b> .....	<b>226</b>

## Server policy

- [Why don't my back-end servers receive the virtual server IP address as the source IP?](#)
- [Does an FTP server policy handle FTP, FTPS and SFTP traffic?](#)
- [Why does blocking by XFF not work when private IP in XFF?](#)

## FAQ

### Why don't my back-end servers receive the virtual server IP address as the source IP?

When the operation mode is Reverse Proxy, the server pool members receive the IP address of the FortiWeb interface the connection uses. If the back-end servers need to know the IP address of the client where the request originated, configure a X-Forwarded-For rule for the appropriate profile. For details, see "Defining your proxies, clients, & X-headers" in FortiWeb Administration Guide.

### Does an FTP server policy handle FTP, FTPS and SFTP traffic?

Until you configure an FTP server policy, FortiWeb will deny all FTP traffic.

You can configure an FTP server policy to handle FTP and FTPS traffic, but SFTP is not supported.

FTPS (also named as FTP-over-SSL) is based on SSL/TLS and actually requires a backend FTP server for the communication. SFTP (SSH File Transfer Protocol) is just a part of SSH. It's more like a file transfer client instead of a server service.

### Why does blocking by XFF not work when private IP in XFF?

By default, XFF parsing will ignore private IP. If you do not want to ignore it, please set as follows:

```
FortiWeb # config waf x-forwarded-for
FortiWeb (x-forwarded-for) # edit test
FortiWeb (test) # set skip-private-original-ip disable
FortiWeb (test) # end
```

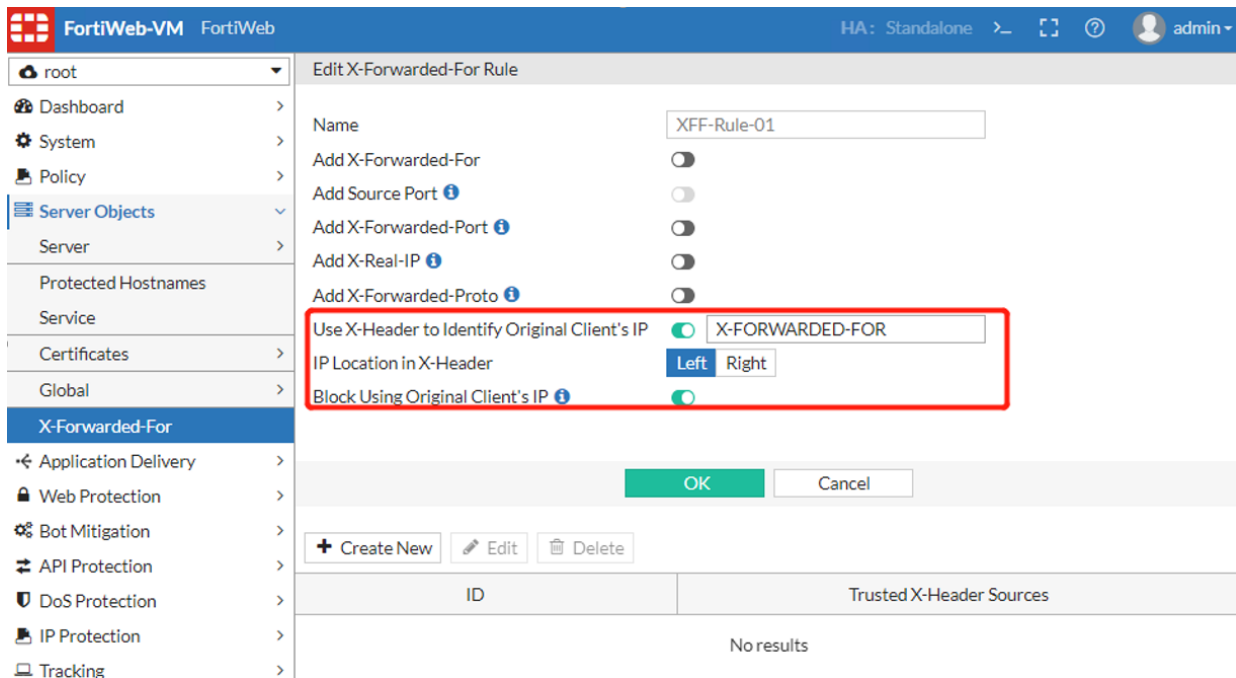
### Will all IP addresses listed in the XFF (X-Forwarded-For) header be handled by WAF modules?

The general format of the field is:

```
X-Forwarded-For: client, proxy1, proxy2
```

In 7.0.1 and previous builds, only the left-most or the right-most IP address can be scanned and processed by WAF modules including IP Protection features and other features. You can select the option "IP Location in X-Header" accordingly as below.

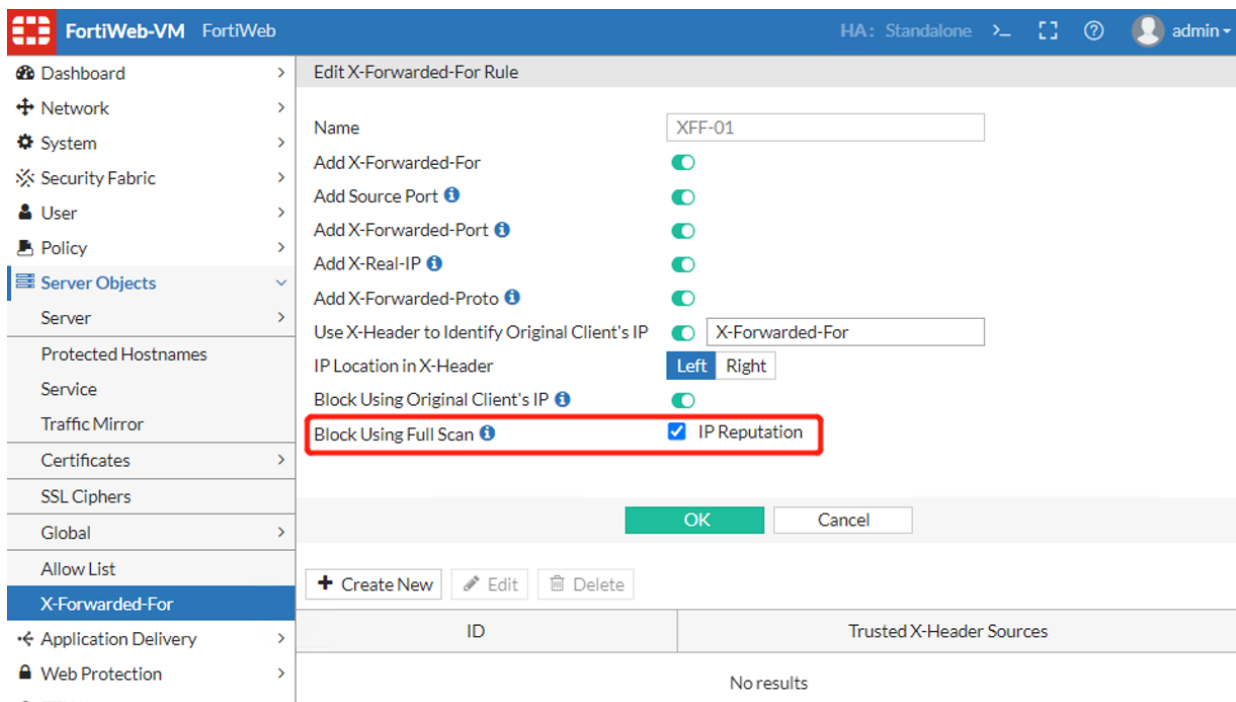
That means, a request including header "X-Forwarded-FOR: A.A.A.A, B.B.B.B, C.C.C.C" will NOT be blocked if only B.B.B.B is added into a IP block list.



From 7.0.2, an option **Block Using Full Scan** is added thus WAF modules can scan and process the IP addresses in the middle of the XFF header. Currently only IP Reputation is supported, while more features will be added and listed here in future release.

When this option is enabled, IP Reputation will scan all IP addresses listed in the X-Forwarded-For header to match with the IPs in the categories.

Both IP Reputation policy and X-Forwarded-For rule should be linked to the Protection Profile for a Server Policy. Also, **Use X-Header to Identify Original Client's IP** and **Block Using Original Client's IP** should be enabled in the X-Forwarded-For rule.



For troubleshooting purpose, the following diagnose commands can be used:

```
# diagnose debug flow filter module-detail x-forward-for 7
# diagnose debug enable

> GET / HTTP/1.1
> Host: 10.33.33.1:81
> User-Agent: curl/7.83.1
> Accept: */*
> X-Forwarded-For: 1.2.3.4, 192.168.0.2, 10.33.33.3
[x forward for][INFO](x_forward_for_process-949): inside x_forward_for process
[x forward for][INFO](http_parse_x_forwarded_for-850): inside x_forward_for http
  parse
[x forward for][INFO](http_parse_orig_ip-673): inside x_forward_for parse original ip
[x forward for][DEBUG](http_parse_orig_ip-693): Skip = 0, location = 1, Value =
  [1.2.3.4,192.168.0.2,10.33.33.3], Unparsed value[1.2.3.4, 192.168.0.2,
  10.33.33.3]
[x forward for][INFO](http_parse_orig_ip-732): Original ip = 10.33.33.3
[x forward for][INFO](http_parse_fullscan_ip-755): inside http_parse_fullscan_ip
[x forward for][DEBUG](http_parse_fullscan_ip-792): Skip = 0, location = 1, Value =
  [1.2.3.4,192.168.0.2,10.33.33.3,]
[x forward for][DEBUG](http_parse_fullscan_ip-817): ips from value cur: 1.2.3.4
[x forward for][DEBUG](http_parse_fullscan_ip-819): parse original: this ip list has
  : 1.2.3.4
[x forward for][DEBUG](http_parse_fullscan_ip-817): ips from value cur: 192.168.0.2
[x forward for][DEBUG](http_parse_fullscan_ip-819): parse original: this ip list has
  : 192.168.0.2
[x forward for][DEBUG](http_parse_fullscan_ip-817): ips from value cur: 10.33.33.3
[x forward for][DEBUG](http_parse_fullscan_ip-819): parse original: this ip list has
  : 10.33.33.3
[x forward for][INFO](x_forward_for_process-990): xff: after parse ip str: 10.33.33.3
[x forward for][INFO](set_original_ip-428): xff: set original ip str: 10.33.33.3
[x forward for][INFO](set_original_ip-435): during set_original_ip: original IP
  address = 10.33.33.3
[x forward for][INFO](set_original_ip-452): set_original_ip: Full Scan IP address =
  1.2.3.4
[x forward for][INFO](set_original_ip-452): set_original_ip: Full Scan IP address =
  192.168.0.2
[x forward for][INFO](set_original_ip-452): set_original_ip: Full Scan IP address =
  10.33.33.3
```

## Why doesn't Protected Hostnames work as expected?

Protected Hostnames are used in a server policy to restrict requests to specific hostnames. FortiWeb 7.0.1 and previous builds support setting the exact hostname or using wildcards such as \*.example.com to match the field `Host:` in HTTP header. Please note that only one wildcard is supported. If you enter multiple wildcards, matching of hostname will be unexpected.

From 7.0.2, Protected Hostname supports `Ignore Port` and `Include Sub-Domain`, and wildcard is still supported. Sub-Domain will be ignored if the `Host:` field in a request is an IPv4 or IPv6 address.

Below are examples to show whether a request will match the configured hostname.

Protected Hostname	Enable Ignore Port	Enable Include Sub-Domain	Request Host	Result
abc.example.com	No	No	abc.example.com:8080	Not match
abc.example.com	Yes	No	abc.example.com:8080	Match
abc.example.com	Yes	Yes	xyz.abc.example.com:8080	Match
*example.com	No	No	abc.example.com	Match
example.com*	No	No	example.com:8080	Match
example.com*	Yes	No	example.com:8080	Match
*example.com*	No	No	abc.example.com:8080	Not match
example.com:8080	No	No	example.com:8080	Match
example.com:8080	Yes	No	example.com:8080	Not match

The reason of the Not match cases is either of the following:

- Only one wildcard is supported;
- When **Ignore Port** is enabled, the port in the `Host :` field of the incoming request will be removed, so it does not match the protected hostname configured.

If you encounter other mismatching issues, you can either check the attack log or run diagnose logs as below:

```
diagnose debug flow filter module-detail allow-hosts 7
diagnose debug enable

[Protected Hostnames][INFO](allow_host_process-742): protected hostname validation
begin
[Protected Hostnames][INFO](http_host_check-495): Enter Function : http_host_check
[Protected Hostnames][INFO](http_host_check-520): Request Host value :
    try.fwbtestgslb.com:8333
[Protected Hostnames][INFO](http_host_check-521): Request Host len : 24
[Protected Hostnames][INFO](host_parse_ignore_port-440): Inside host_parse_ignore_
port
[Protected Hostnames][INFO](host_parse_ignore_port-441): Request Host value :
    try.fwbtestgslb.com:8333
[Protected Hostnames][INFO](host_parse_ignore_port-482): ipv4 or domain host removed
port: try.fwbtestgslb.com
[Protected Hostnames][INFO](http_host_check-557): Ignore port enabled
[Protected Hostnames][INFO](http_host_check-560): hoststr after ignore port trim:
    try.fwbtestgslb.com
[Protected Hostnames][INFO](http_host_check-561): hoststr len after ignore port trim:
    19
[Protected Hostnames][INFO](http_host_check-568): Include subdomains enabled
[Protected Hostnames][INFO](host_parse_include_subdomains-298): Inside host_parse_
include_subdomains
[Protected Hostnames][INFO](host_parse_include_subdomains-299): hoststr recieved:
    try.fwbtestgslb.com
[Protected Hostnames][INFO](host_parse_include_subdomains-313): single request host
subdom: try
[Protected Hostnames][INFO](host_parse_include_subdomains-313): single request host
subdom: fwbtestgslb
```

```
[Protected Hostnames][INFO](host_parse_include_subdomains-313): single request host
subdom: com
[Protected Hostnames][INFO](host_parse_include_subdomains-319): longest section is :
11
[Protected Hostnames][INFO](host_parse_include_subdomains-326): single fwb host
subdom: *
[Protected Hostnames][INFO](host_parse_include_subdomains-326): single fwb host
subdom: fwbtestgslb
[Protected Hostnames][INFO](host_parse_include_subdomains-326): single fwb host
subdom: com*
[Protected Hostnames][INFO](host_parse_include_subdomains-331): section count of
request host: 3, section count of fwb host: 3
[Protected Hostnames][INFO](http_host_check-570): hoststr after subdomains trim:
try.fwbtestgslb.com
[Protected Hostnames][INFO](http_host_check-571): hoststr len after subdomains trim:
19
[Protected Hostnames][INFO](http_host_check-579): Protected Hostname host :
*.fwbtestgslb.com*
[Protected Hostnames][INFO](http_host_check-584): url case disabled
[Protected Hostnames][INFO](http_host_check-586): found '*' at the beginning of
Protected Hostname host
[Protected Hostnames][INFO](http_host_check-588): Request host after manipulation:
y.fwbtestgslb.com
[Protected Hostnames][INFO](http_host_check-703): Request host did not matched a
Protected Hostname, perform default action
```

### Which WAF modules will be skipped if the Allow List is matched?

When enabled, allow-listed items will skip the subsequent scans after the Global Object allow list. Please check the scan sequence of the Global Object Allow List in "Sequence of scans" in FortiWeb Administration Guide, or "What's the sequence of WAF module scans in 7.0.0" in [FAQ on page 152](#).

When the Allow List is matched, the following modules will be affected:

Allow Name	Check Position	Affected Modules
Allow URL	Global white list	URL Access Rule will be checked; Modules after URL Access will be skipped
Allow Parameter	<ul style="list-style-type: none"> <li>Parameter Validation</li> <li>Signature</li> <li>Syntax based detection</li> <li>ML-based Anomaly Detection</li> </ul>	When these four modules check parameters, parameters in Allow Parameter list will be skipped.
Allow Cookie	<ul style="list-style-type: none"> <li>Signature</li> <li>Syntax based detection</li> <li>Cookie security</li> </ul>	When these three modules check or process cookies, cookies in Allow Cookie list will be skipped
Allow Header	<ul style="list-style-type: none"> <li>Global white list</li> <li>Syntax based</li> </ul>	URL Access Rule will be checked; When Syntax based detection checks headers, headers in Allow Cookie list

Allow Name	Check Position	Affected Modules
	detection	will be skipped

The scan sequence of the modules mentioned above is:

Global White List -> URL Access -> Parameter Validation -> Signature -> Syntax Based Detection -> Cookie Security -> ML-based Anomaly Detection

The following parameters or cookies are by default included in Allow List if their corresponding modules are enabled. For example, the request with cookiesession1 will match the Allow list and be exempted from the subsequent scans only when Client Management is enabled.

Name	Type	Owner Module
cookiesession1	cookie	Client management
cookiesession3	cookie	Site Publish
cookiesession6	cookie	Robot Check
cookiesession8341	parameter	RBE(bot_reco_process is used by 5 modules)
redirect491	parameter	Custom page
rewrite491	parameter	Custom page/Url Rewrite
reason747sha	parameter	Custom page

## How do Global Allow List and Policy Based Allow List work?

On 7.0.1 and previous builds, only Global Allow List is supported, while on 7.0.2 and newer builds, FortiWeb also supports Policy Based Allow List.

Predefined Global or Predefined Policy Based Allow List have the same items updated from FortiGuard FortiWeb Security Service. The difference is that Predefined Global Allow List can be enabled or disabled, while Predefined Policy Based List cannot be disabled.

You can either enable or disable some Predefined Global Allow List that updated from FortiGuard FortiWeb Security Service, or create custom list to allow your own URLs, header field, cookies and parameters on the Custom Global Allow List tab in **Server Objects > Global > Global Allow List**. Global allow list applies to all server policies in all ADOMs.

As for Policy based Allow List, you can reference the predefined list or customized list (via Server Objects > Global > Global Allow List > Policy Based Allow List) in a server policy. When the traffic arrives at this server policy, it will be screened only according to the server policy based allow list instead of the global one.

By default, Global Allow List takes effect. When Allow List is set for a server-policy, the policy-based Allow List will take effect instead of the Global Allow List.

## Why is the cookiesession1 generated by Client Management persistent cookie?

In inline deployment mode, when a client accesses a web application for the first time, FortiWeb inserts a cookie named "cookiesession1" into the client's browser. If the client carries the inserted cookie in subsequent access,

FortiWeb tracks the client by this cookie; otherwise, FortiWeb tracks the client by the client's source IP.

To do user tracking more accurately, "cookiesession1" is set as a persistent cookie with one year validity by default. FortiWeb will identify it as the same user even if the client browser is closed and opened again.

On 7.0.2, FortiWeb provides an option to set "cookiesession1" as a session cookie. If you think that a persistent cookie introduces a threat to your application, they can enable this option, or disable this cookie altogether by disabling **Client Management** in the web protection profile.

```
config waf web-protection-profile inline-protection
  edit <web-protection-profile name>
    set http-session-cookie enable
  next
end
```

you can enable `diagnose debug flow filter module-detail client-management 7` to double check which type of cookie is applied in the web-protection-profile.

When http-session-cookie is disabled:

```
[client-manage][INFO](insert_wafsid:1419): [Note] it's persistent cookiesession1
```

When http-session-cookie is enabled:

```
[client-manage][INFO](insert_wafsid:1417): [Note] it's session level cookiesession1
```

## SSL/TLS

- [FAQ on page 108](#)
- [Diagnosing SSL/TLS handshake failures on page 113](#)
- [Decrypting SSL packets to analyze traffic issues on page 116](#)

## FAQ

### How do I detect which cipher suite is used for HTTPS connections?

Use sniffing (packet capture) to capture SSL/ TLS traffic and view the "Server hello" message, which includes cipher suite information.

For more HTTPS troubleshooting information, see "Supported cipher suites & protocol versions" and "Checking the SSL/TLS handshake & encryption" in FortiWeb Administration Guide

### How can I strengthen my SSL configuration?

The following configuration changes can make SSL more effective in preventing attacks and can improve your website's score for third-party testing tools (for example, the SSL server test provided by [Qualys SSL Labs](#)).

Which configuration changes you make depends on your environment. For example, some older clients do not support SHA256.

- For your website certificate, do the following:
  - If it uses the SHA1 hashtag function, replace it with one that uses SHA256.
  - Ensure that its key size is 2048-bit.

- For the server policy (Reverse Proxy mode) or server pool member configuration (True Transparent Proxy mode), specify the following values in the advanced SSL settings:
  - Select Add HSTS Header, and then for Max. Age, enter 15552000.
  - For Supported SSL Protocols, disable SSL 3.0.
  - For SSL/TLS Encryption Level, select High.
  - For Enable Perfect Forward Secrecy, select Yes.
  - Select Disable Client-Initiated SSL Renegotiation.

For details, see Configuring a server policy on in FortiWeb Administration Guide.

Use the following CLI command to set the Diffie-Hellman key exchange parameters to 2048 or greater:

```
config system global
  set dh-params 2048
```

The command is available in FortiWeb 5.3.6 and higher releases. For additional information on using CLI commands, see the FortiWeb CLI Reference:

<https://docs.fortinet.com/product/fortiweb/>

### Does FortiWeb support partial-chain verification?

On 7.0.1 and previous builds, FortiWeb needs the full certificate chain (RootCA + SubCA) in the CA-group to validate the client certificate. If only intermediate CA is included in the CA Group, client verification will fail.

7.0.2 supports partial-chain verification by enabling below options via CLI:

- set trust-anchor to "enable" for a CA group
- set partial-chain to "enable" in the certificate verify rule

```
FortiWeb # show system certificate ca-group
config system certificate ca-group
  edit "CA_GP_01"
    config members
      edit 1
        set name subCA_Group_01
        set trust-anchor enable
      next
    end
  next
end
FortiWeb # show system certificate verify
config system certificate verify
  edit "Client_Cert_Verify_01"
    set ca subCA_Group_01
    set partial-chain enable
  next
end
```

### How to troubleshoot a LetsEncrypt certificate obtaining failure?

If Letsencrypt is configured for a server policy, but system fails to obtain a certificate, you can follow these steps for troubleshooting:

1. Check prerequisites for Letsencrypt:

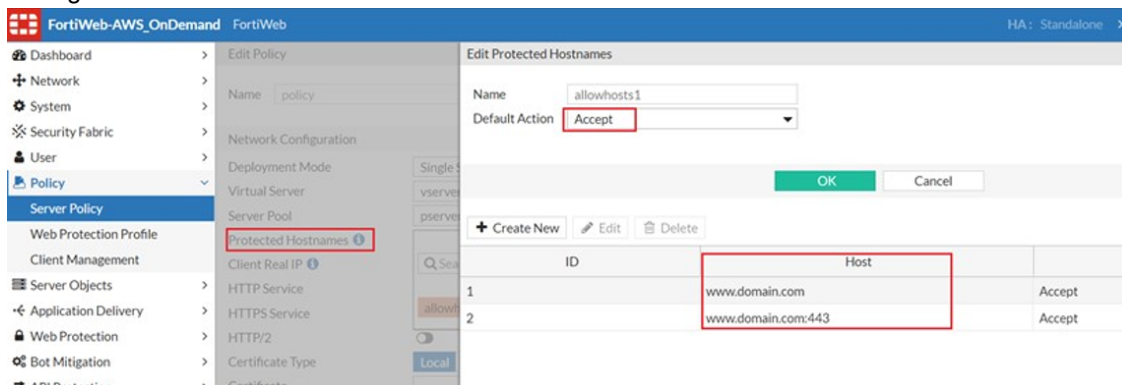
- The DNS entry has been mapped to your domain name with FortiWeb's VIP address.
- If multiple SANs (Subject Alternative Name) are added, make sure that all domains are mapped to the same public IP address (also FortiWeb's VIP).

From 7.0.2, FortiWeb supports requesting a LetsEncrypt certificate with multiple SAN (Subject Alternative Name). You can add SAN via **Server Objects > Certificates > Letsencrypt > Create New**.

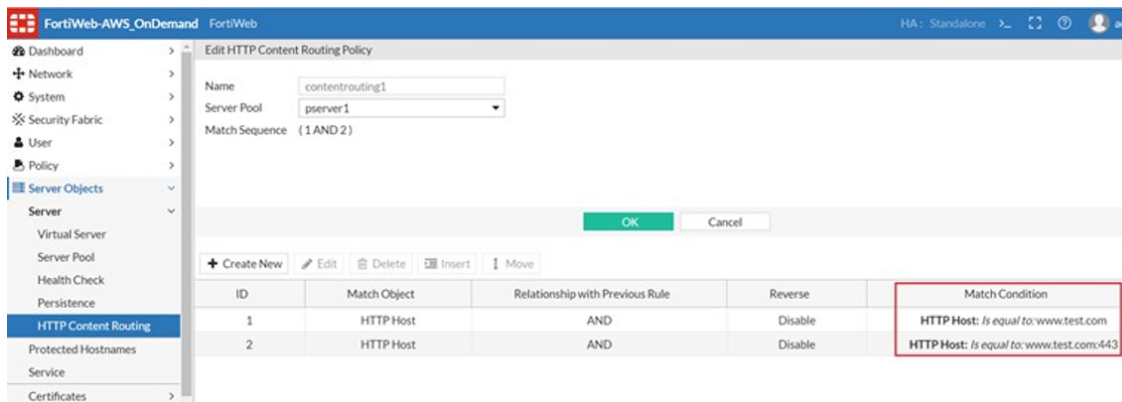
- Do not block requests from United States in **IP Protection > Geo IP Block**, otherwise FortiWeb can't retrieve certificates from Let's Encrypt.

2. Check Letsencrypt related configuration on FortiWeb:

- Make sure that port 80 is enabled, because Let's Encrypt sends HTTP requests to FortiWeb in order to validate the ownership of the domain name:
  - In RP mode, make sure to select HTTP service when configuring server policy.
  - In TTP mode, the back-end server which uses Letsencrypt certificate should have port 80 enabled.
- If you select the Letsencrypt certificate and also enable **Redirect HTTP to HTTPS**, make sure that both domain.com and domain.com:443 are added as the accepted hosts in **Protected Hostnames** settings.



- If a server policy enables HTTP Content Routing, make sure the match conditions match both domain.com and domain.com:443.

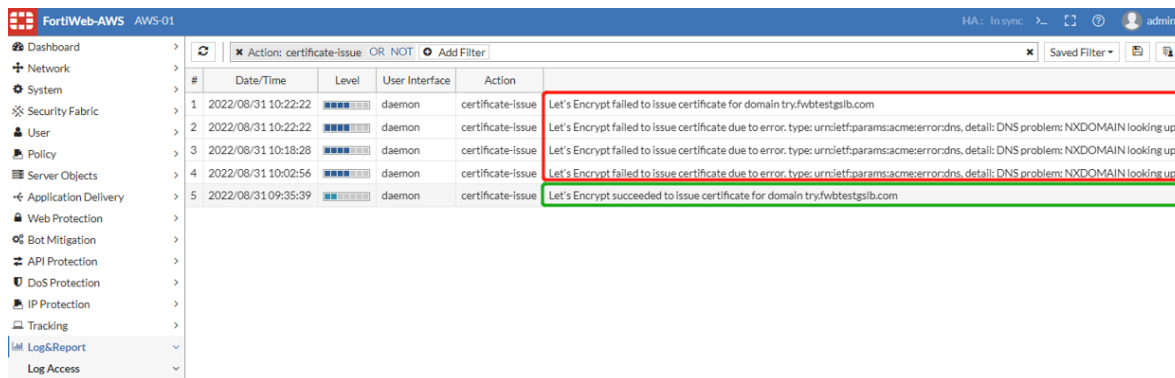


**Notes:** Before 7.2.0, we only the HTTP-01 validation method. For 7.2.0, support of DNS-01 and TLS-ALPN-01 are added to address the above limitation.

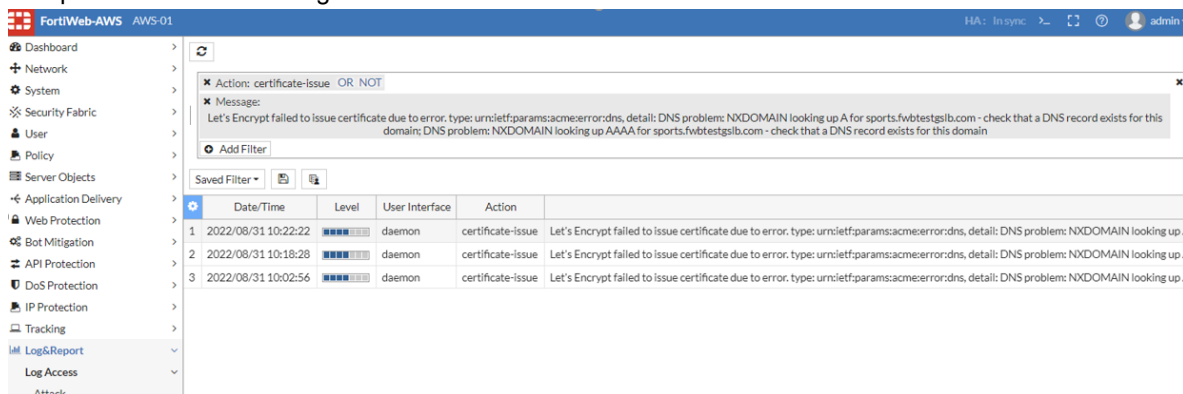
3. Check event logs for success or failure events.

Both successful and failed issue processes will generate at least one event log. You can right click the log to check detailed information.

Certificate renewal will also generate event logs.



Sample for detailed event log info:



4. Check more details in diagnose logs:

For 7.0.2 and previous builds, you just need to enable below commands for diagnose logs:

```
diagnose debug application acmed 7
diagnose debug enable
```

Sample for a certificate issuing failure due to DNS search failed:

```
(acme_log_err_event_process_inner_json : 583)acme_log_err_event_process_inner_
json: type = urn:ietf:params:acme:error:dns, detail = DNS problem: NXDOMAIN
looking up A for sports.fwbtestgslb.com - check that a DNS record exists for
this domain; DNS problem: NXDOMAIN looking up AAAA for
sports.fwbtestgslb.com - check that a DNS record exists for this domain
(acme_post : 742)acme_post: return code 200, json=
(authorize : 1025)challenge https://acme-v02.api.letsencrypt.org/acme/chall-
v3/148263779557/UU140g failed with status invalid
(acme_error : 276)the server reported the following error:
(authorize : 1039)running /etc/acme/acme.sh failed http-01 sports.fwbtestgslb.com
xBEJLu4bsEHTIf_3LVvY1_VwWLTdovJmHMicWx51PNE xBEJLu4bsEHTIf_3LVvY1_
VwWLTdovJmHMicWx51PNE.i9Tp-bb8fw4CsxC7QJfuRYMDQv-251EzsYgn3o3DQ6s
(cert_issue : 1328)failed to authorize order at https://acme-
v02.api.letsencrypt.org/acme/order/643342336/121299792817
(acme_cert_valid_and_issue : 1669)/etc/acme/try.fwbtestgslb.com cert issue failed
(cert_load : 1282)/etc/acme/try.fwbtestgslb.com/cert.pem does not exist
```

```
(acme_update_cert : 1127)acme_update_cert:1127: update CMDB entry
try.fwbtestgslb.com status to 7
```


**Sample for a certificate issuing failure due to reaching the max retry limitation:**

```
(acme_log_err_event_process_inner_json : 583)acme_log_err_event_process_inner_
json: type = urn:ietf:params:acme:error:rateLimited, detail = Error creating
new order :: too many failed authorizations recently: see
https://letsencrypt.org/docs/failed-validation-limit/
(acme_post : 742)acme_post: return code 429, json=
(cert_issue : 1303)failed to create new order at https://acme-
v02.api.letsencrypt.org/acme/new-order
(acme_error : 268)the server reported the following error:
(acme_cert_valid_and_issue : 1669)/etc/acme/try.fwbtestgslb.com cert issue failed
(cert_load : 1282)/etc/acme/try.fwbtestgslb.com/cert.pem does not exist
(acme_update_cert : 1127)acme_update_cert:1127: update CMDB entry
try.fwbtestgslb.com status to 7
```

- 5. Let's Encrypt only allows 5 times of certificate obtaining failure per hour for each host name and account. Please check if the number of retries reaches this limitation.

If FortiWeb fails to obtain the certificate, it will try again every 2 hours until the certificate is successfully obtained.

You can also manually obtain the certificate by clicking the **Issue** button. FortiWeb will obtain the certificate immediately.

#	Name	Domain	Status	Operation
1	1	www.fortinet.com	certificate status failed	

If the following error message displays, it means you have retrieved the certificate too frequently. You will see below information in the event log or diagnose output:

```
Let's Encrypt failed to issue certificate due to error. type:
urn:ietf:params:acme:error:rateLimited, detail: Error creating new order ::
too many failed authorizations recently: see
https://letsencrypt.org/docs/failed-validation-limit/
```

**How will LetsEncrypt certificate be renewed?**

On 7.0.1 and previous builds, Letsencrypt certificates will be renewed automatically every 90 days. 5 days before your letsencrypt certificate expires, FortiWeb renews it for another 90 days, so it never expires.

From 7.0.2, FortiWeb supports setting **Renew Period**, that is the number of days to renew a certificate before it expires. The default value is 30 days.

**Why can't a browser connect securely to my back-end server?**

If a browser cannot communicate with a back-end server using SSL or TLS, use the following troubleshooting steps to resolve the problem:

1. Without connecting via FortiWeb, ensure that you can access the server using HTTPS.
2. Ensure that your browser supports HTTP Strict Transport Security (HSTS). For example, following web page provides compatibility tables for various web browser versions:

<http://caniuse.com/stricttransportsecurity>

3. Ensure that the FortiWeb response includes the strict transport security header.

To add this header, select Add HSTS Header in the server policy or server pool configuration. For details, see "Configuring a server policy" or "Creating a server pool" in FortiWeb Administration Guide.

4. Use the following to ensure that the server certificate is trusted:

- If the certificate is signed by intermediate certificate authority (CA), the intermediate CA is signed by a root CA.
- The root CA is listed in your browser's store of trusted certificates.
- The domain name or IP address is consistent with the certificate subject.

For details, see "Uploading a server certificate" in FortiWeb Administration Guide.

### How to backup & restore private keys

- Refer to Admin Guide > How to set up your FortiWeb > Secure connections > How to export/backup certificates & private keys.
- Local certificates are stored at: /data/etc/cert/local/root

```
/data/etc/cert/local/root# ls
FortiWeb_CA.cer  server_2048.cer  server_4096.cer
FortiWeb_CA.key  server_2048.key  server_4096.key
```

Keys are encrypted. During the encryption process, we will convert the key file into a matrix system and perform matrix conversion and hashing algorithms to protect each key file.

## Diagnosing SSL/TLS handshake failures

If the client is attempting to make an HTTPS connection, but the attempt fails after the TCP connection has been initiated, during negotiation, the problem may be with SSL/TLS.

### 1. Check the errors displayed on SSL/TLS client/browser.

A SSL/TLS client or browser usually displays the SSL error code it encountered. Once can check and try to resolve them based on the specific error message.

Common symptoms may include error messages such as:

- `ssl_error_no_cypher_overlap` (Mozilla Firefox 9.0.1)
- Error 113 (`net::ERROR_SSL_VERSION_OR_CIPHER_MISMATCH`): Unknown error (Google Chrome 16.0.912.75 m)

You can search on Internet to find solutions for those common error messages and check if any problem is caused by client sides:

[How to Fix SSL Error on Firefox Browser? - A Complete List \(comparecheapssl.com\)](http://comparecheapssl.com)

However, we can often check SSL error codes on FortiWeb attack logs as below.

### 2. Check detailed SSL errors in attack logs.

SSL errors will be displayed in attack logs once "Ignore SSL Erros" is disabled by either method as below:

- Disable Ignore SSL Errors in **Log&Report > Log Config > Other Log Settings**

The screenshot shows the FortiWeb-AWS FWB-AWS-M01 configuration interface. On the left is a navigation menu with categories like Security Fabric, FortiView, User, Policy, Server Objects, Application Delivery, Web Protection, FTP Security, Bot Mitigation, API Protection, DoS Protection, IP Protection, Tracking, Machine Learning, Web Vulnerability Scan, Log&Report, and Log Config. The 'Log Config' category is expanded to show 'Other Log Settings'. The main content area displays a list of log settings, each with a toggle switch. 'Ignore SSL Errors' is currently turned off. Below this is a section titled 'Retain Packet Payload For' with a list of events and their corresponding toggle switches.

Setting	Status
Enable Attack Log	On
Enable Traffic Log	On
Enable Traffic Packet Log	On
Enable Event Log	On
Ignore SSL Errors	Off
<b>Retain Packet Payload For</b>	
Parameter Rule Violation	On
Hidden Fields Violation	On
HTTP Protocol Constraints	On
Signature Detection	On
Custom Signature Detection	On
Anti Virus Detection	Off
Custom Access Violation	On
CORS Protection	On
IP Reputation Violation	On
Illegal File Type	On
Cookie Security	On
Padding Oracle Attack	On
FortiSandbox Detection	On
JSON Protection	On
Illegal File Size	On
Web Shell Detection	On

- Check detailed SSL errors in attack logs through:

```
conf log attack-log
    set no-ssl-error disable
end
```

For instance, a log is like below:

"SSL Error(394) - dh key too small".

This error means the length of dh pukkey in the ssl "server key exchange" is short, that is to say, it's too weak and insecure, and the higher version will consider closing it.

Please check the error code/message listed:

[SSL/TLS error messages \(fortinet.com\)](https://www.fortinet.com/ssl/tls-error-messages)

[https://mantis.fortinet.com/file\\_download.php?file\\_id=666300&type=bug](https://mantis.fortinet.com/file_download.php?file_id=666300&type=bug)

**3. If SSL error is related to protocol or cipher suite, you can use OpenSSL to confirm which protocol & ciphers are supported:**

- Check whether the backend server or FortiWeb supports strong (HIGH) encryption:

```
openssl s_client -connect example.com:443 -cipher HIGH
```

- Check whether the backend server or FortiWeb supports old versions such as SSL 1.1:

```
openssl s_client -tls1.1 -connect example.com:443
```

If you have checked the errors but are not sure about the cause, please collect diagnose logs and also capture packets at the same time, then send to developers for further investigation:

**4. Diagnose debug flow can output error during SSL handshake:**

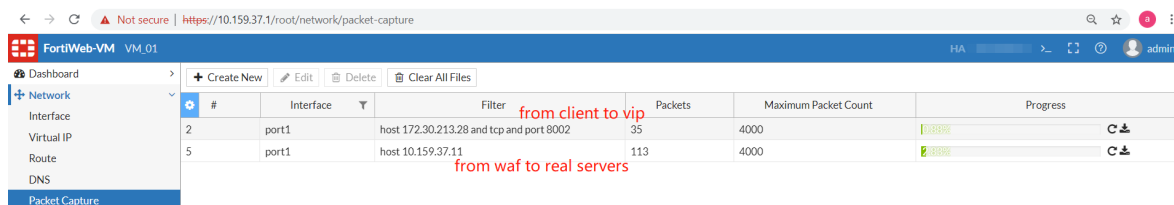
```
diagnose debug reset
diagnose debug enable
diagnose debug timestamp enable
diagnose debug flow filter flow-detail 7
diagnose debug flow filter server-ip 192.168.12.12 #The VIP in RP mode or the
    real server IP in TP/TI mode
diagnose debug flow filter client-ip 192.168.12.1
diagnose debug flow trace start
diagnose debug flow trace stop
```

```
FortiWeb # <04:05:24>[work 0][flow] policy SP_01 create service:0x7fae5d14ce28
<04:05:24>[work 0][flow] ssn 1120 policy SP_01 strm 0 dir 0 subclient 0 create
    HTTP substream:0x7fae5d195328
<04:05:24>[work 0][flow] ssn 1120 policy SP_01 strm 0 dir 0 subclient 0 create
    stream:0x7fae5e05d908
<04:05:24>[work 0][flow] ssn 1120 policy SP_01 strm 0 dir 0 subclient 0 session
    accept(104.40.29.86:46226->10.0.0.108:443), fd:27, clissl 0x7fae8568bf88,
    session count 1 session:0x7fae5e036a98
<04:05:24>[work 0][flow] ssn 1120 policy SP_01 strm 0 dir 0 subclient 0 client 27
    [ST-ssl-handshake], conn st 0x00000004
<04:05:24>[conn lib]ssl handshake failed
<04:05:24>[work 0][flow] ssn 1120 policy SP_01 strm 0 dir 0 subclient 0 ssl
    handshake failed for client 27
<04:05:24>[work 0][flow] ssn 1120 policy SP_01 strm 0 dir 0 subclient 0 client 27
    conn st 0x00000004, conn set err, err msg:err_ssl_handshake
```

For real-time debugging, besides logging the diagnose outputs, it's better to also capture application traffic packets at the same time like below.

**5. Capture packets and check the handshake.**

Usually one can create two filter tasks in **Network > Packet Capture** to capture packets from a specific client and to a specific backend server in server-pool simultaneously.



After the pcap files are downloaded, one can open them with Wireshark to check the TCP and SSL negotiation details. You can check statistics conversations, follow a TCP/TLS stream, or add filters such as “ip.addr==172.30.213.28 && tcp.port==23222 && ip.addr==10.159.37.1 && tcp.port==8002” to narrow down traffic flow to a specific stream.

6. If you find that SSL negotiation fails only when traffic load is heavy, you may also consider if the system reaches a certain performance bottleneck, such as TCP ports used-up, SSL performance limitation, etc. Please refer to [Server policy intermittently inaccessible](#) for troubleshooting methods.

## Decrypting SSL packets to analyze traffic issues

If SSL/TLS handshakes are successful but there are still server-policy access failures, sometimes we may need to decrypt the SSL packets and check more details in HTTP packets.

In brief, we need to capture packets on FortiWeb and enable diagnose debug flow at the same time; after retrieving the SSL keys from diagnose output, use it in Wireshark to decrypt the SSL traffic, then you'll be able to see the encrypted HTTP communication. As the keys used for TLS1.3 are different with TLS1.2 and before, we describe them separately as below.

### Enabling diagnose debug flow to retrieve TLS Pre-master secrets

SSL pre-master secrets, also stated as “SSL keys” in below sections, which are necessary to decrypt SSL packets, can be retrieved from diagnose debug flow trace logs.

To decrypt SSL packets, you need to capture SSL packets and enable diagnose debug flow at the same time. After pre-master secrets are retrieved from diagnose logs, one can save them in a file and import it into Wireshark to decrypt the captured SSL packets, then you'll be able to see the encrypted HTTP flows.

Use below diagnose commands to print `diagnose debug flow trace` in which SSL pre-master secrets will be included:

```
# diagnose debug flow filter flow-detail 4 #4 is the lowest level to print SSL
  secrets
# diagnose debug flow trace start
FWB# diagnose debug enable
```

To scale down diagnose flow output, you can add IP filters in flow trace logs:

```
# diagnose debug flow filter client-ip <A.A.A.A> #Client IP address
# diagnose debug flow filter server-ip <B.B.B.B> #The VIP in RP mode or the real
  server IP in TP/TI mode
# diagnose debug flow filter pserver-ip <C.C.C.C> #The real server IP in RP mode; TTP
  or other operation modes do not support this filter
```

Please note:

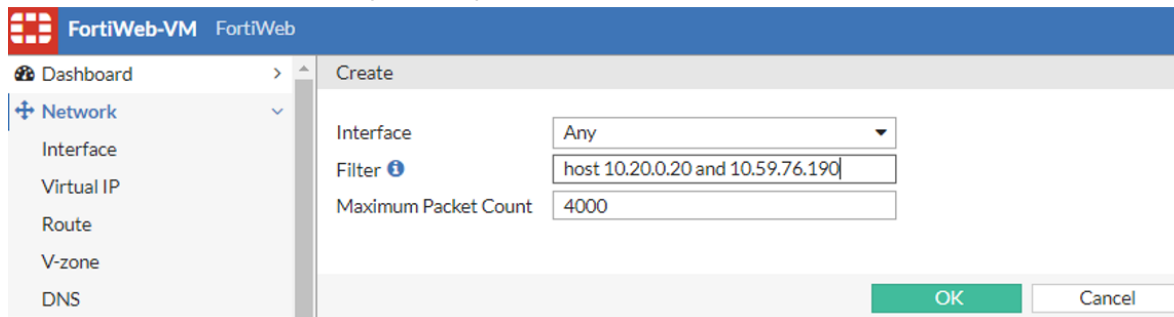
- Client-ip & server-ip are supported on all 6.3.x and 7.0.x builds; pserver-ip is supported on 6.3.21, 7.0.3 and later builds.
- On 6.3.20, 7.0.1 and earlier builds:
  - If no IP filters are added, both front-end and back-end TLS 1.2 & 1.3 pre-master secrets can be printed out in diagnose logs;
  - If client-ip or/and server-ip are added, only flows matched will be printed out in diagnose logs; pre-master secrets for TLS 1.2 and lower protocols on both the front-end and back-end-side will be printed in diagnose logs;

- A known limitation is that when TLS 1.3 is deployed on the back-end side (between FortiWeb and the real back-end servers) and IP flow filters are added, pre-master secrets cannot be printed out. You need to remove all IP filters to retrieve the TLS 1.3 secrets.
- On 6.3.21, 7.0.3 and newer builds:
  - If no IP filters are added, both front-end and back-end side TLS 1.2 & 1.3 pre-master secrets can be printed out in diagnose logs;
  - If only the front-end IP filters (client-ip or/and server-ip) or the back-end IP filter pserver-ip is added, only flows matched the filters will be printed out in diagnose logs, which include the pre-master secrets;
  - If both the front-end IP filters (client-ip or/and server-ip) and the back-end IP filter pserver-ip are added at the same time, the relationship between the front-end filters and the back-end filter is OR. That is to say the flows either matching the front-end or back-end IP filters will be printed.
  - The back-end IP filter pserver-ip is necessary for retrieving the back-end pre-master secrets either when TLS 1.2 or TLS 1.3 is deployed between FortiWeb and the real back-end servers.

Please refer to [Debugging traffic flow at user level with diagnose commands on page 31](#) for usage of related commands.

## Decrypting TLS 1.2/1.1/1.0 Traffic

1. Capture packets on FortiWeb, and enable diagnose debug flow at the same time as follows. For example, capturing packets from client IP 10.20.0.20 to FortiWeb VIP 10.59.76.190 on FortiWeb GUI as below. If the IP used on FortiWeb to connect pservers is also 10.59.76.190, then the traffic flow on both the frontend and backend sides will be captured; otherwise you may need to specify the pserver as another host filter instead of the VIP to capture the packets on the backend side.



2. The client random and "pre master key" will be in the diagnose debug output as follows. You can find the client random and "pre master key" in two sections in diagnose output. Either of them can be retrieved and used as keys to encrypt SSL traffic in Wireshark.

### Section I:

```

tls1.3 ssl key (server):
CLIENT_RANDOM 61e7b3d0b841a4abd371199cd32e23b6ee89f405c7aabc2a28997964ed01a677
e392e420f25bfb69cfae878c05c098dcea21020de21e1852c44701edfb25a28677a4b3677c3a
a054352643bcad171a70
tls1.3 ssl key (client):
CLIENT_RANDOM bcac18831f2c2b63d8ea784ba5df74bc8e0e1618f3c7bb927bcda5bbc4ba322a
cebb2af2b4bb2fed087214da294dbd8ffbbdbd162466f76aaab9c822aa73bfec991b6b7cefb9
c98c3434300afcb32ac0
  
```

### Section II: (client random&keys are as same as that in section I)

```

[work 1][flow] ssn 1 policy SP_01 strm 0 dir 0 subclient 0 client 32 ssl handshake
(172.30.212.177:1074->10.159.37.1:7002) session data: client random
  
```

```
61e7b3d0b841a4abd371199cd32e23b6ee89f405c7aabc2a28997964ed01a677, master key
e392e420f25bfb69cfae878c05c098dcea21020de21e1852c44701edfb25a28677a4b3677c3a
a054352643bcad171a70
```

```
[work 1][flow] ssn 1 policy SP_01 strm 0 dir 1 subclient 0 server 34 ssl handshake
(10.159.37.1:13536->10.159.37.11:443) session data: client random
bcac18831f2c2b63d8ea784ba5df74bc8e0e1618f3c7bb927bcda5bbc4ba322a, master key
cebb2af2b4bb2fed087214da294dbd8ffbbdbd162466f76aaab9c822aa73bfec991b6b7cefb9
c98c3434300afcb32ac0
```

3. Create a wireshark key file. The key file format is as follows with content retrieved from the diagnose output.

```
CLIENT_RANDOM 61e7b3d0b841a4abd371199cd32e23b6ee89f405c7aabc2a28997964ed01a677
e392e420f25bfb69cfae878c05c098dcea21020de21e1852c44701edfb25a28677a4b3677c3a
a054352643bcad171a70
CLIENT_RANDOM bcac18831f2c2b63d8ea784ba5df74bc8e0e1618f3c7bb927bcda5bbc4ba322a
cebb2af2b4bb2fed087214da294dbd8ffbbdbd162466f76aaab9c822aa73bfec991b6b7cefb9
c98c3434300afcb32ac0
```

The first section is for client to FortiWeb and the second is for FortiWeb to back-end server.

You can manually copy and save the client random and "pre master key" to a file, or use a Linux command to retrieve them as follows:

For releases earlier than 6.3:

```
awk '{gsub(/\,/, " ")} /session data: client random/{print "CLIENT_RANDOM " $19 " "
$22}' tls12_debug.log > tls12key.file
```

For 6.3 and later:

```
awk '{gsub(/\,/, " ")} /session data: client random/{print "CLIENT_RANDOM " $21 " "
$24}' tls12_debug.log > tls12key.file
```

You can save the diagnose output in `tls12_debug.log` as above and run the command in the FortiWeb backend shell or a Linux machine.

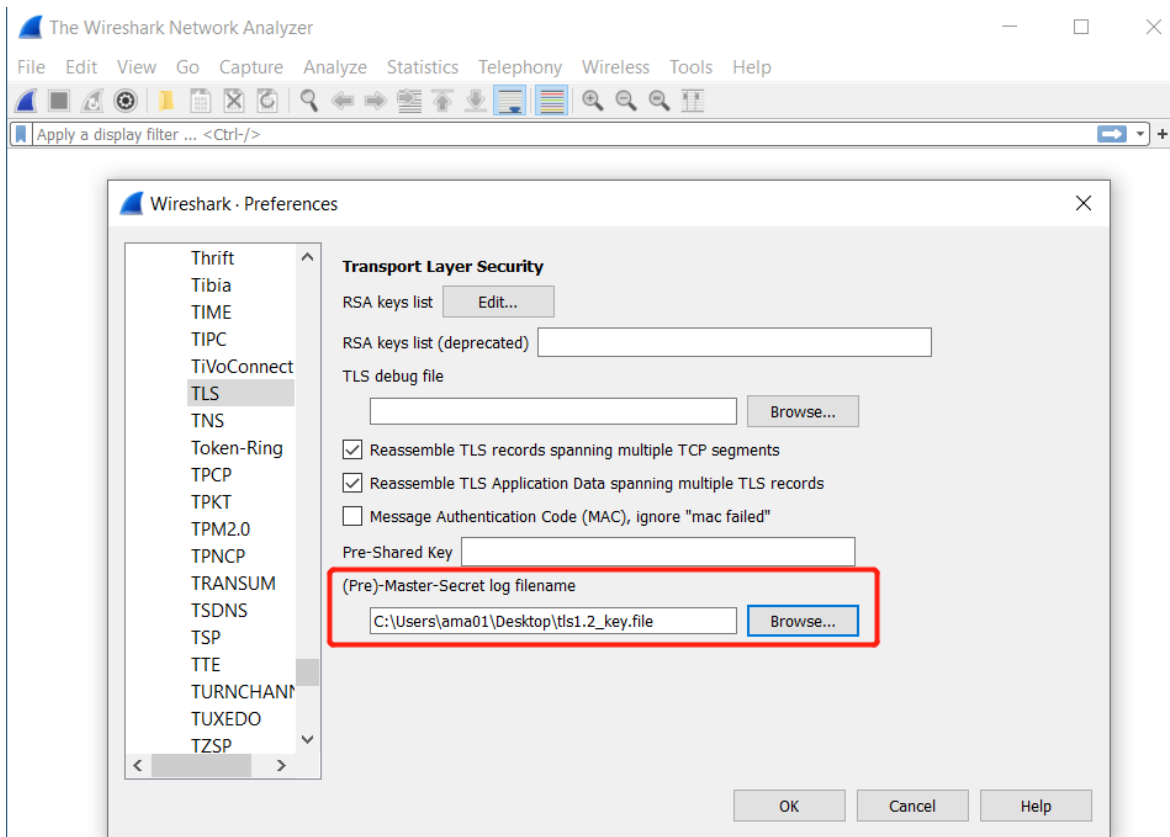
Sometimes running the command may run into an error:

```
root@ut:/home/test# awk '{gsub(/\,/, " ")} /session data: client random/{print
"CLIENT_RANDOM " $21 " " $24}' tls1.2_flow.log > tls1.2_key.log
awk: cmd. line:1: warning: regexp escape sequence `\', ' is not a known regexp
operator
```

Use below command instead:

```
awk '{gsub(/,/, " ")} /session data: client random/{print "CLIENT_RANDOM " $21 " "
$24}' "tls1.2_flow.log" > tls1.2_key.file
```

4. Set wireshark: edit > preference > protocols > TLS: choose the key file "tls1.2\_key.file" from "(Pre)-Master-Secret log filename". Then you'll be able to see that decrypted HTTP traffic.



## Decrypting TLS 1.3 Traffic

1. Capture packets on FortiWeb, and enable diagnose debug flow at the same time as follows.

```
FortiWeb# diagnose debug flow filter flow-detail 4
FortiWeb# diagnose debug flow trace start
FortiWeb# diagnose debug enable
```

Please note:

- Add filters when capturing packets on FortiWeb;
- Do not add filters in diagnose commands as below if the back-end server provides SSL/TLS service, otherwise SSL keys cannot be displayed in diagnose output. It's a known limitation while we'll enhance it in future builds.
- If you only want to decrypt SSL traffic from clients to FortiWeb, below filters can be added
 

```
diagnose debug flow filter client-ip 172.30.214.11
diagnose debug flow filter server-ip 10.159.37.33
```

2. The keys can be also found in the diagnose debug output as follows. It's a little different from that of TLS1.2 and before.

```
[work 0][f] ssn 5 policy SP_01 strm 0 dir 0 subclient 0 client 32 ssl handshake
(172.30.212.177:1039->10.159.37.1:7002),ssl event:2
[work 0][f] ssn 5 policy SP_01 strm 0 dir 0 subclient 0 client 32 [ST-ssl-
handshake], conn st 0x00000004
tls1.3 ssl key (server):
SERVER_HANDSHAKE_TRAFFIC_SECRET
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
```

```

a52744e732f1b328650b40653ea0d9845fa8726f79b19a6b6dbdf08ff24c735efc907e948a53
709c0cf5ef2c7038c8af
tls1.3 ssl key (server):
CLIENT_HANDSHAKE_TRAFFIC_SECRET
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
e14368e33bd50ba4dd106d0a5018e8e145e112b9cdac6fd3e0455b2479399bbf8bc54ab0f522
512f93170c754d32a9ad
tls1.3 ssl key (server):
EXPORTER_SECRET 72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
31ccb2227090eea6653d334f5fd9a08667292ac0a220e25f139270fde716a5a14f3b426ba06
11b012b985e04028c178
tls1.3 ssl key (server):
SERVER_TRAFFIC_SECRET_0
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
0faae977ef5ba35accdac2b189eedefea4ccf7363fc78f6933569f42659f27ece1bdae43dff8
8a7da18b950e5d021505
[conn lib]ssl handshake, state:1

[work 0][flow] ssn 5 policy SP_01 strm 0 dir 0 subclient 0 client 32 ssl handshake
(172.30.212.177:1039->10.159.37.1:7002),ssl event:2
[work 0][flow] ssn 5 policy SP_01 strm 0 dir 0 subclient 0 client 32 [ST-ssl-
handshake], conn st 0x00000004
tls1.3 ssl key (server):
CLIENT_TRAFFIC_SECRET_0
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
c06b9cb7332bd05f1761d6ba6621345aa73a018f5f5db2ddfeb160b3aec755f8a9a40fd30041
232a3d37bfb93aff24bd
[conn lib]ssl handshake, state:2

```

The first column is tls1.3 secret label as below:

```

CLIENT_EARLY_TRAFFIC_SECRET:    client early traffic secret
CLIENT_HANDSHAKE_TRAFFIC_SECRET:client handshake secret
SERVER_HANDSHAKE_TRAFFIC_SECRET:server handshake secret
CLIENT_TRAFFIC_SECRET_0:        client application data secret
SERVER_TRAFFIC_SECRET_0:        server application data secret

```

3. Create a wireshark key file. The key file format is as follows with content retrieved from the diagnose output.

```

root@ut:/home/test/keys# cat tls1.3_key.file
SERVER_HANDSHAKE_TRAFFIC_SECRET
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
a52744e732f1b328650b40653ea0d9845fa8726f7
9b19a6b6dbdf08ff24c735efc907e948a53709c0cf5ef2c7038c8af
CLIENT_HANDSHAKE_TRAFFIC_SECRET
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
e14368e33bd50ba4dd106d0a5018e8e145e112b9c
dac6fd3e0455b2479399bbf8bc54ab0f522512f93170c754d32a9ad
EXPORTER_SECRET 72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
31ccb2227090eea6653d334f5fd9a08667292ac0a220e25f139270fd
e716a5a14f3b426ba0611b012b985e04028c178
SERVER_TRAFFIC_SECRET_0
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
0faae977ef5ba35accdac2b189eedefea4ccf7363fc78f693
3569f42659f27ece1bdae43dff88a7da18b950e5d021505
CLIENT_TRAFFIC_SECRET_0
72e61efe2594465bf79935093e9d73254e1cd2e67f0acee06379166af25be863
c06b9cb7332bd05f1761d6ba6621345aa73a018f5f5db2ddf
eb160b3aec755f8a9a40fd30041232a3d37bfb93aff24bd
SERVER_HANDSHAKE_TRAFFIC_SECRET
49e35b0c4ddf3e521e07d2fc660a271cff2b2b64317bd48f343a69eb57ce70b6

```

```

fe1eb5cef9ca293fbd4899612d89339e0d76a5426
55ccb08c249d32e330bc8232a8572d9bdcea7bbfd002764df227458
EXPORTER_SECRET 49e35b0c4ddf3e521e07d2fc660a271cff2b2b64317bd48f343a69eb57ce70b6
5549b723b72fb18c30cc25a8ce86f8b5afe1bcfaled9bb6c3b9584408
ef6fdac0c6286083c4046c99433e0424724351c
SERVER_TRAFFIC_SECRET_0
49e35b0c4ddf3e521e07d2fc660a271cff2b2b64317bd48f343a69eb57ce70b6
ba1bb94d8740f7609919b18ab0c09201ade62ed6f6d8687ad
892bdcf00e3bbc2f6ee253e26cf005acdabc6e80d2a29c2
CLIENT_HANDSHAKE_TRAFFIC_SECRET
49e35b0c4ddf3e521e07d2fc660a271cff2b2b64317bd48f343a69eb57ce70b6
6fc9d895b73d8e8f33461b043ab0239b757d734b8
f1dde1a664d519792cddd82aed2f81cc892f4e01865f68785851cc3
CLIENT_TRAFFIC_SECRET_0
49e35b0c4ddf3e521e07d2fc660a271cff2b2b64317bd48f343a69eb57ce70b6
d4f3118b685428e8d53f7bbd63c15baa8b9828a8af062d984
1619fa2d6b076d27bb3735df598f06204f13918a7993218

```

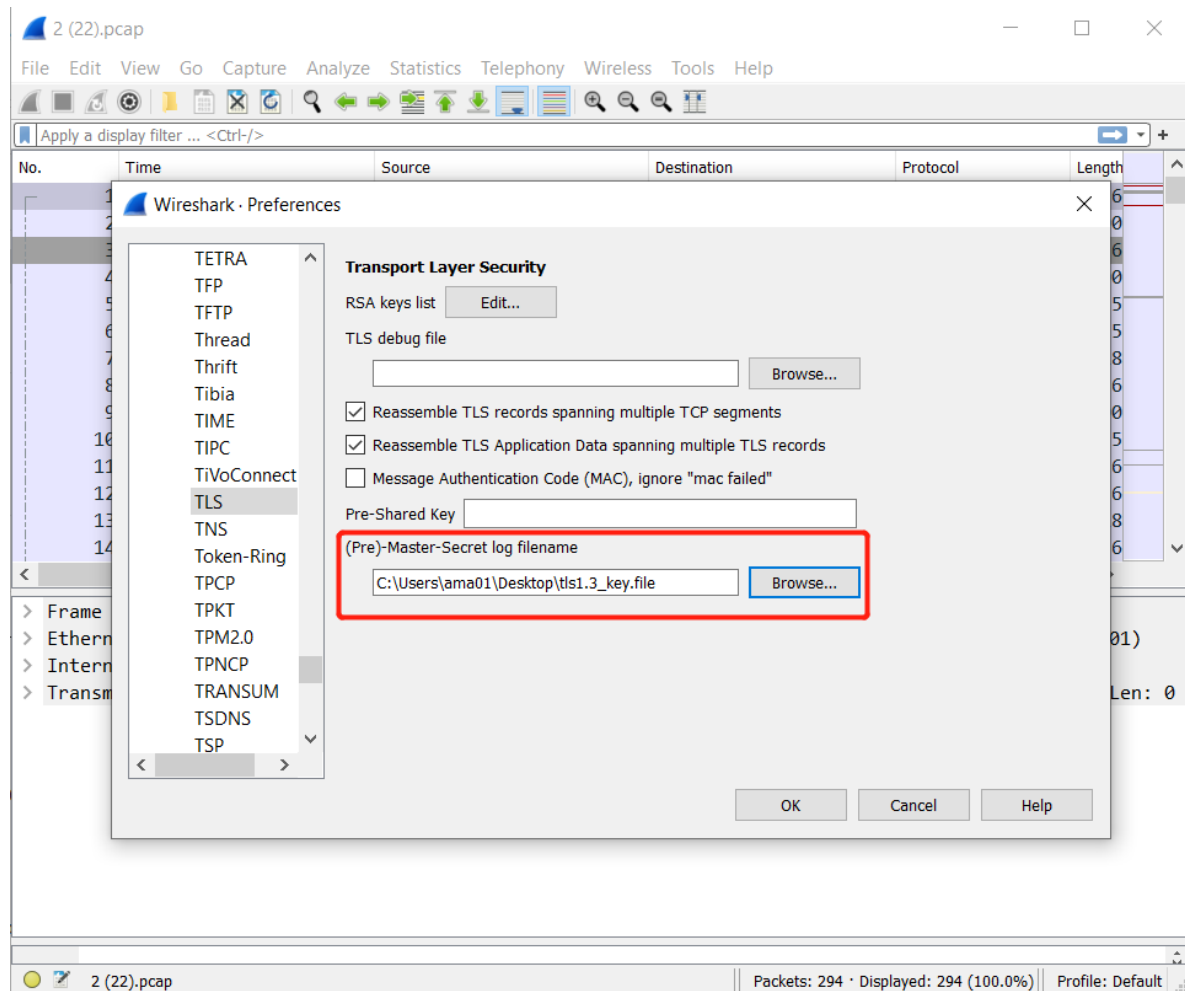
You can manually copy & save the these sections to a file, or use a Linux command to retrieve them in the FortiWeb backend shell or a Linux machine as follows:

```

root@utma:/home/test# awk '/EXPORTER_SECRET|SERVER_HANDSHAKE_TRAFFIC_
SECRET|SERVER_TRAFFIC_SECRET_0|CLIENT_HANDSHAKE_TRAFFIC_SECRET|CLIENT_
TRAFFIC_SECRET_0/{print $1" "$2" "$3}' tls1.3_flow.log > tls1.3_key.file

```

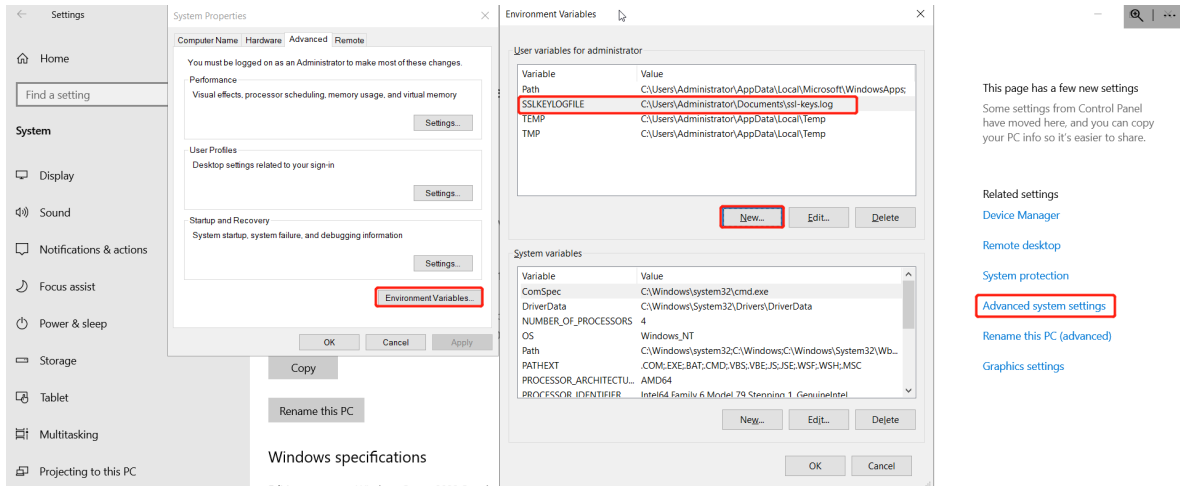
4. Set wireshark: edit > preference > protocols > TLS: choose the key file "tls1.3\_key.file" from "(Pre)-Master-Secret log filename". Then you'll be able to see that decrypted HTTP traffic.



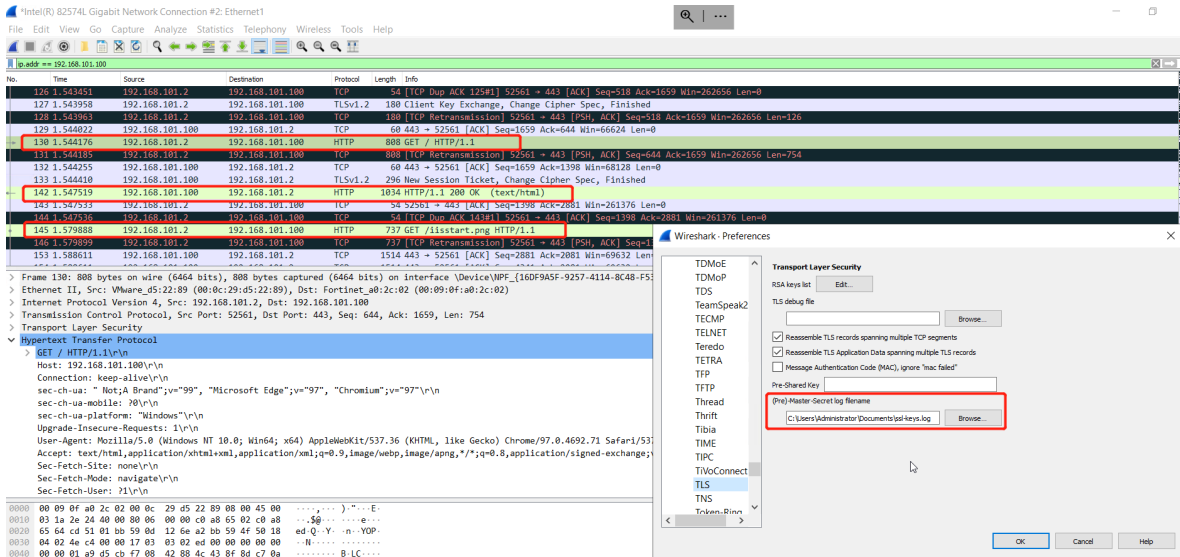
## An alternative way to decrypt TLS traffic on Windows PC

If you're using a Windows client and want to decrypt SSL/TLS traffic from the client to FortiWeb, there is a simpler way to get the SSL keys instead of retrieving them from FortiWeb diagnose output.

1. Set a Windows environment variable.  
E.g. Create a new environment variable under User variables and select a file named "ssl-keys.log" to store SSL keys.



2. Set wireshark: edit > preference > protocols > TLS: choose the key file "ssl-keys.log" from "(Pre)-Master-Secret log filename". Then you'll be able to see that decrypted HTTP traffic.



**Please Note:**

This method cannot capture and analyze packets from FortiWeb to the backend server.

## Application Delivery - URL Rewriting

### Why does URL rewriting not work?

If FortiWeb is not rewriting URLs as expected, complete the following troubleshooting steps:

1. Ensure the value of Action Type is correct.  
Request Action rewrites HTTP requests from clients, and Response Action rewrites responses to clients from the web server.
2. Ensure that you have added items to the URL Rewriting Condition Table.

3. If one of your conditions uses a regular expression, ensure that the expression is valid.
  - Click the **>> (double arrow)** button beside the **Regular Expression** field to test the value.
  - For an online guide for regular expressions, go to:  
<http://www.regular-expressions.info/reference.html>
  - For an online library of regular expressions, go to:  
<http://regexlib.com>
  - If the page is compressed, ensure that you have configured a decompression policy.
4. Check if the webpage size is larger than the **Maximum Body Cache Size**.  
URL body rewriting does not work when the page is larger than the cache buffer size. The default size is 64KB.

Go to **System > Config > Advanced** and adjust the value of **Maximum Body Cache Size**.

To adjust the buffer using the CLI, use a command like the following example:

```
config global
  config sys advanced
    set max-cache-size 1024
  end
end
```

5. For a Response rewrite rule and the action is “Rewrite HTTP Body”, ensure there is a “Content-Type” header in the response from the backend server, and the Content-Type (also called Internet or MIME file types) must be supported by FortiWeb.

FortiWeb supports the following Content-Type values only:

- text/html
- text/plain
- text/javascript
- application/xml
- text/xml
- application/javascript
- application/soap+xml
- application/x-javascript
- application/json
- application/rss+xml

“Content-Type” is not a must for other types of rewrite rules including Request rewrite rules and Rewrite HTTP Header rules.

6. Specifically, if the option **Content Type Filter** is enabled in the match condition, only the types selected in **Content Type Set** will be matched and rewritten. Webpages with other unselected types will match the rewrite rule.

7. Enable diagnose logs for further analysis:

```
FWB # diagnose debug flow filter module-detail url-rewrite 7
FWB # diagnose debug flow filter flow-detail 0 # available since 7.4.1
FWB # diagnose debug flow trace start # available since 7.4.1
FWB # diagnose debug enable
```

Diagnose logs will show HTTP request & response details, url-rewrite rule & policy matching conditions (match or not), etc.

Example: url-rewrite-policy “redirect\_policy\_01” contains two rules.

“redirect\_rule\_01” is a request redirect action that aims to remove the port 8443

“url-rewrite-rule-ResponseAction-RewriteBody” is a response rewrite body action that targets to replace “It works!” with “Hey, It works now!!”

For request direction, all conditions are matched so redirect 301 is responded to the client.

URL Rewriting Policy
URL Rewriting Rule

Edit URL Rewriting Rule

Name

Action Type Request Action Response Action

Request Action Redirect (301 Permanently)

OK
Cancel

URL Rewriting Condition Table

+ Create New
✎ Edit
🗑 Delete

ID	Object	Regular Expression	Protocol Filter	Protocol
1	HTTP Host	portal.testdomain.com:8443	Disable	-
2	HTTP URL	/index.html	Disable	-

Replacement Location

Location

```
[url rewrite][INFO] (./waf_module/url_rewrite.c:2543): CLIENT -> SERVER.
[url rewrite][INFO] (./waf_module/url_rewrite.c:2483): Request host:
    [portal.testdomain.com:8443].
[url rewrite][INFO] (./waf_module/url_rewrite.c:2487): Request url: [/index.html].
[url rewrite][INFO] (./waf_module/url_rewrite.c:1619): url rewrite policy name:
    [redirect_policy_01].
[url rewrite][INFO] (./waf_module/url_rewrite.c:515): url rewrite rule name:
    [redirect_rule_01] ,check rule conds.
[url rewrite][INFO] (./waf_module/url_rewrite.c:523): the matching host
    :portal.testdomain.com:8443
[url rewrite][INFO] (./waf_module/url_rewrite.c:528): the matching url :/index.html
[url rewrite][INFO] (./waf_module/url_rewrite.c:651): all conditons matched!
[url rewrite][INFO] (./waf_module/url_rewrite.c:1658): matched...
[url rewrite][INFO] (./waf_module/url_rewrite.c:1660): the pcre capture $0 is :
... ..
[url rewrite][INFO] (./waf_module/url_rewrite.c:1572): the action is :8
[url rewrite][INFO] (./waf_module/url_rewrite.c:1342): make redirect response.
[url rewrite][INFO] (./waf_module/url_rewrite.c:1351): the new location is :
    http://portal.testdomain.com
[url rewrite][INFO] (./waf_module/url_rewrite.c:2565): The response custom redirect
    301.
[url rewrite][INFO] (./waf_module/url_rewrite.c:2543): CLIENT -> SERVER.
[url rewrite][INFO] (./waf_module/url_rewrite.c:2483): Request host:
    [portal.testdomain.com].
[url rewrite][INFO] (./waf_module/url_rewrite.c:2487): Request url: [/].
[url rewrite][INFO] (./waf_module/url_rewrite.c:1619): url rewrite policy name:
    [redirect_policy_01].
[url rewrite][INFO] (./waf_module/url_rewrite.c:515): url rewrite rule name:
    [redirect_rule_01] ,check rule conds.
```

```
[url rewrite][INFO] (./waf_module/url_rewrite.c:523): the matching host
:portal.testdomain.com
[url rewrite][INFO] (./waf_module/url_rewrite.c:643): not matched,and no invert,not
matched.
```

For response direction, all condition is also matched so body-rewrite is also performed.

URL Rewriting Policy
URL Rewriting Rule

**Edit URL Rewriting Rule**

Name

Action Type

Response Action

**URL Rewriting Condition Table**

ID	Object	Regular Expression	Protocol Filter	Protocol
1	HTTP Body	(*)(it)(*)(works)	Disable	-

Replacement Strings in Body

Replacement	<input type="text" value="Hey, \$0\$1\$2\$3 now!"/>
-------------	---

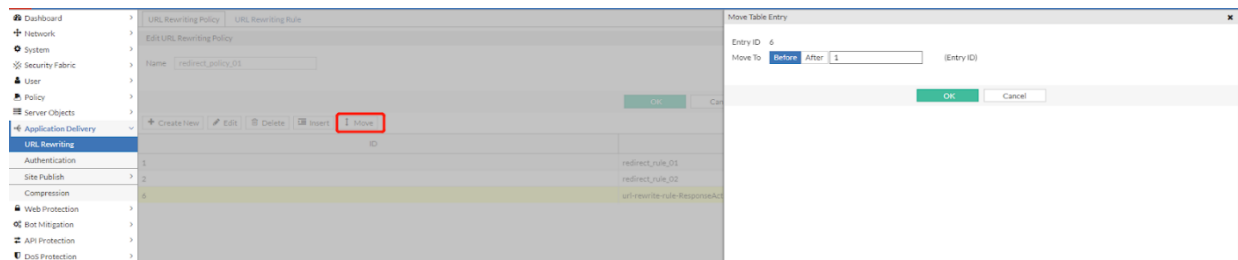
```
[url rewrite][INFO] (./waf_module/url_rewrite.c:2607): SERVER -> CLIENT.
[url rewrite][INFO] (./waf_module/url_rewrite.c:1920): response rewrite check.
[url rewrite][INFO] (./waf_module/url_rewrite.c:1924): url rewrite policy name:
[redirect_policy_01].
[url rewrite][INFO] (./waf_module/url_rewrite.c:1763): HTTP body cache (3477) finish.
[url rewrite][DEG] (./waf_module/url_rewrite.c:1814): response raw body: [HTTP/1.1 200
OK
Date: Thu, 26 May 2022 21:03:08 GMT
Server: Apache/2.4.41 (Ubuntu)
Last-Modified: Thu, 07 Oct 2021 17:55:36 GMT
ETag: "2aa6-5cdc6f84d8056-gzip"
Accept-Ranges: bytes
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 3138
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html
... ..
[url rewrite][INFO] (./waf_module/url_rewrite.c:846): _body_rewrite_check_rule_
conds...
[url rewrite][INFO] (./waf_module/url_rewrite.c:912): content_type is 1
[url rewrite][INFO] (./waf_module/url_rewrite.c:913): content_type_set is 65535
[url rewrite][INFO] (./waf_module/url_rewrite.c:962): match ovector[0]; 385 ovector
[1]: 433
[url rewrite][INFO] (./waf_module/url_rewrite.c:1006): all body-rewrite conditons
matched!
```

## How will multiple rules in one rewrite policy be matched?

If multiple rules are configured in one URL rewrite policy, then these rules will be matched in order. That is to say, when the traffic matches the first rule and is processed, the following rules will be skipped and not take effect any more.

This is also one of the reasons that a rewrite rule does not take effect.

You can move a rewrite rule to adjust the order of entries via CLI or GUI as below:



## How will multiple match-conditions in one rewrite rule be matched?

The relationship between multiple match-conditions are AND. So only if all conditions are matched, the request or response will be rewritten.

## How will FortiWeb handle duplicate headers that are matched by rewrite rules?

From HTTP RFC7230, multiple headers with the same name (e.g. Set-Cookie, www-authenticate) are acceptable and may be received by FortiWeb.

FortiWeb will handle such situations as below:

- If a **Field Name** configured in **HTTP Header Removal** matches multiple headers:
  - If **Remove Duplicate Headers** is enabled, all these headers will be removed;
  - If **Remove Duplicate Headers** is disabled, only the first matched header will be removed.
- For **Replacement URL, Referrer and Location**, in theory only the first header will be replaced. However, in practice duplicate these header fields can be hardly duplicated appearing in the same HTTP packet.

## Why sometimes URL rewriting rules cause Loop in browser visiting?

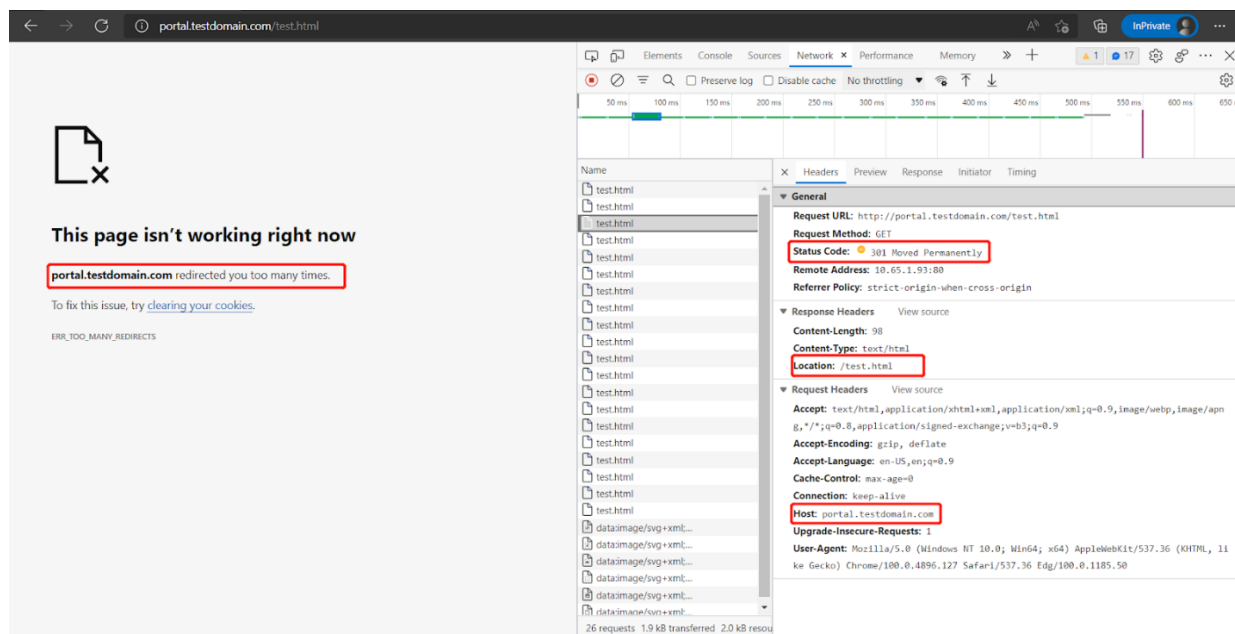
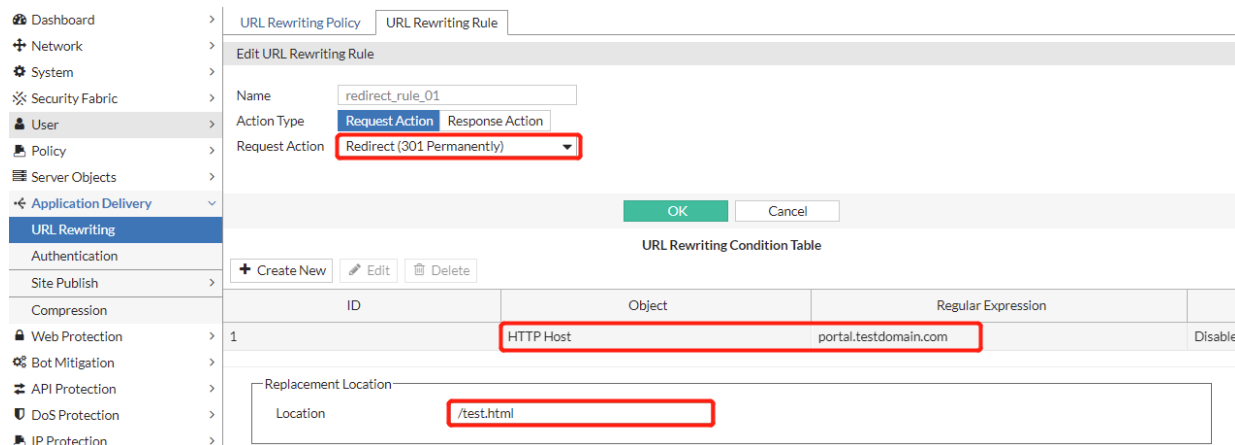
It's a typical issue that sometimes after rewriting rules are added, you may observe loop failures when visiting a server-policy on browsers. However, these issues are usually caused by configuration mistakes.

Below is an example of such misconfiguration failures:

**The request action is Redirect 301. The match condition object is "HTTP Host" with portal.testdomain.com, and the replacement Location is configured as "/test.html".**

The user intended to redirect the visit to the default webpage of portal.testdomain.com to portal.testdomain.com/test.html, but with this configuration, the browser will visit

“http://portal.testdomain.com/test.html” after receiving the 301 response, because the Location header is just “/test.html” rather than a full URI. However this new request will match the rewrite rule again and trigger another 301, thus causing an unexpected loop failure.



To resolve this issue, you can add an extra condition rule as below, then the visits to “http://portal.testdomain.com/index.html” will be successfully redirected to “http://portal.testdomain.com/test.html”, and no loop occurs again.

The screenshot shows the 'Edit URL Rewriting Rule' configuration page. The 'Name' field is 'redirect\_rule\_01'. The 'Action Type' is 'Request Action' and the 'Request Action' is 'Redirect (301 Permanently)'. Below the configuration is a table for 'URL Rewriting Condition Table' with columns for ID, Object, and Regular Expression. The table contains two entries: ID 1 for HTTP Host 'portal.testdomain.com' and ID 2 for HTTP URL '/index.html'. At the bottom, the 'Replacement Location' is set to '/test.html'.

ID	Object	Regular Expression
1	HTTP Host	portal.testdomain.com
2	HTTP URL	/index.html

The tip here is that Location needs to be a full URI, otherwise the browser will reuse the original Host with the relative URI specified by Location.

For example, if you want to redirect a URL to <https://www.google.com>, then you need to configure the Location as “<https://www.google.com>”, not just “[www.google.com](http://www.google.com)”, otherwise the browser will visit “<http://portal.testdomain.com/www.google.com>” after it received 301 redirect.

## Application Delivery - Site Publish

### FAQ

#### What’s the difference between HTTP/User authentication and Site-Publish? Which solution is recommended?

You can treat Site-Publish as a substitute and better solution to replace HTTP authentication.

Most HTTP/User authentication functions can be implemented by Site-Publish, and FortiWeb recommends using Site-Publish policies instead of HTTP/User authentication policies for better future up-to-date technical support.

#### How will authentication server pool members be used to authenticate clients if multiple remote servers are contained in one pool for Site-Publish rule?

When you configure a site publishing rule that offloads authentication for a web application to FortiWeb, you use an authentication server pool to specify the method and server that FortiWeb uses to authenticate clients.

The pool can contain one or more servers that use either LDAP or RADIUS to authenticate clients. FortiWeb attempts to authenticate clients using the server at the top of the list of pool members, and then continues to the

next member down in the list if the authentication is unsuccessful, and so on. You can use the list options to adjust the position of each item in the list.

### Does Site Publish support changing password (CPW)?

FortiWeb supports a user to change password (CPW) after a successful login. This function works in two scenarios:

- A user must change password at next logon.
- A user must change password when it is expired.

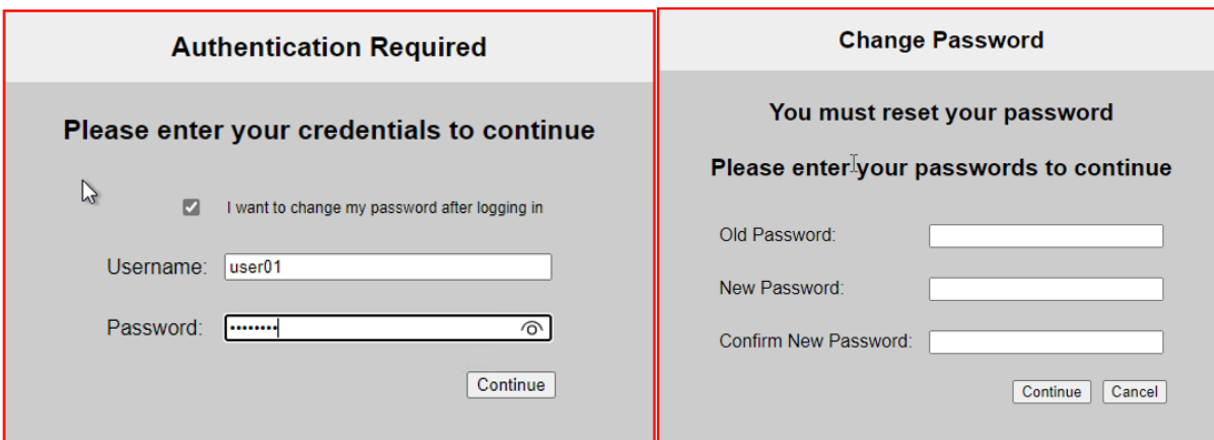
LDAP CPW is supported on 7.0.x and 6.3.x, and Radius CPW is supported from 7.0.2. CPW support does not need extra configuration on FortiWeb, but it requires that CPW is enabled on LDAP or Radius servers.

Some configuration tips on FortiWeb:

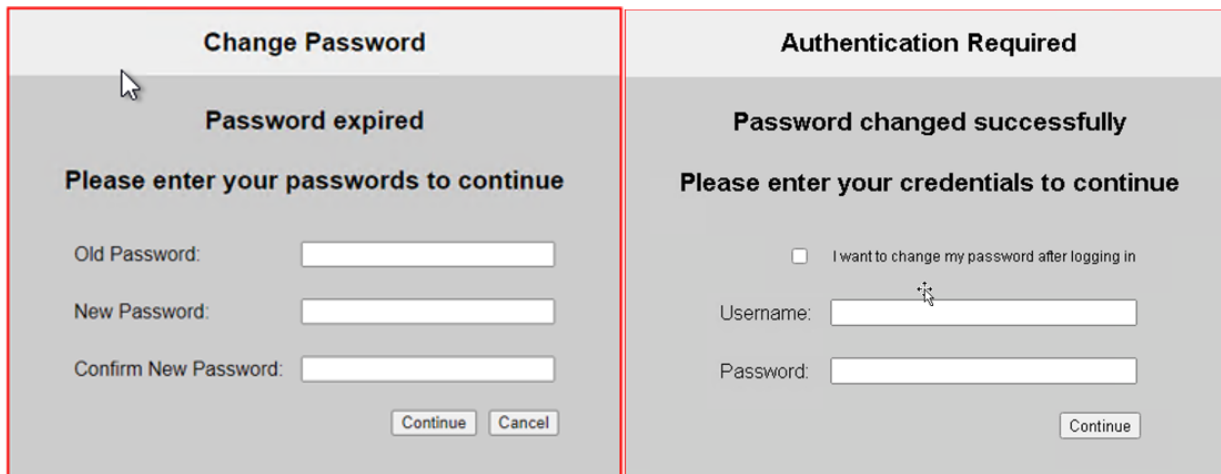
- The **Client Authentication Method** in Site Publish rule should be set as **HTML Form Authentication**;
- LDAP: **Bind Type** in LDAP Server should be **Regular**;
- Radius: **Authentication Scheme** in Radius Server should be **MS-CHAP-V2**;

You can actively check **I want to change my password after logging in** to change the password, or passively be required to change the password by the LDAP or Radius server.

Change password at next login:

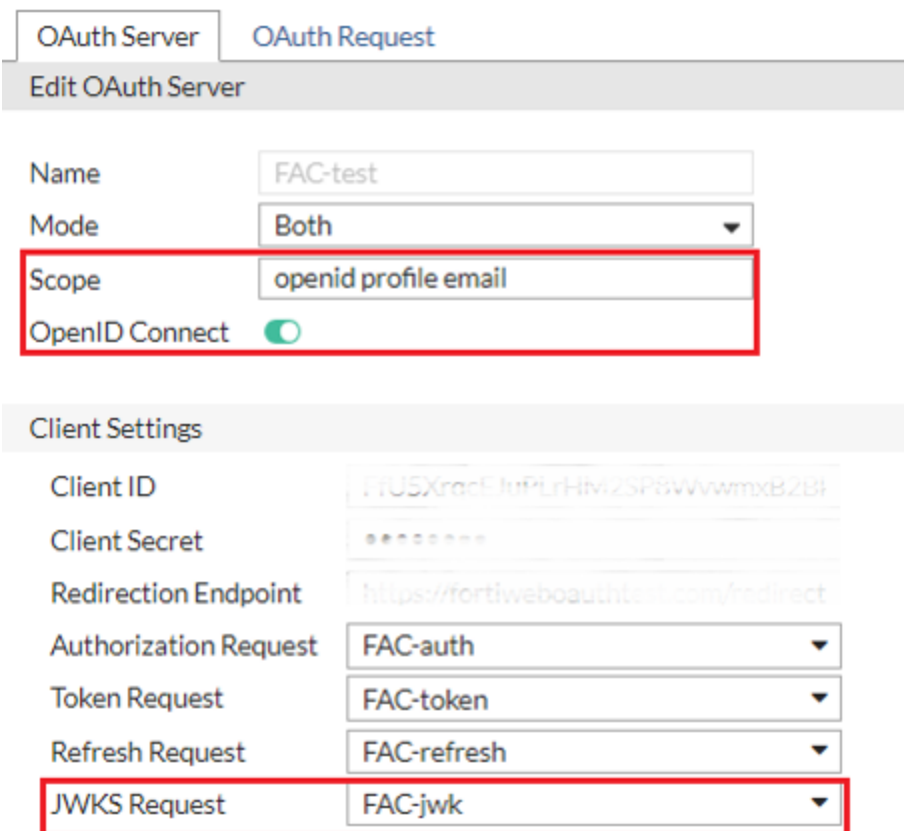


Password expired:



### Does Site Publish support OpenID Connect (OIDC)?

OAuth OIDC is supported from 7.4.0 onwards. Users are required to toggle the **OpenID Connect** switch under the **OAuth Server** and add at least "openid" to the **Scope** field. If more information is needed, additional scopes can be added, such as profile, email, etc.



Sample Configuration for FortiAuthenticator

Client type: **Confidential** Public

Authorization grant types: Password-based **Authorization code**

Client ID:

Client secret:

Policy:

Access token expiry: 56000

Redirect URIs:

---

**Relying Party Scopes**

Scope	Scope Type	Delete
<input type="text" value="openid"/>	<input type="text" value="Default"/>	<input type="button" value="X"/>

[+ Add Relying Party Scope](#)

---

**Claims**

Scope	Name	User Attribute	Delete
<input type="text" value="openid"/>	<input type="text" value="firstname"/>	<input type="text" value="First name"/>	<input type="button" value="X"/>
<input type="text" value="openid"/>	<input type="text" value="lastname"/>	<input type="text" value="Last name"/>	<input type="button" value="X"/>
<input type="text" value="openid"/>	<input type="text" value="email"/>	<input type="text" value="Email"/>	<input type="button" value="X"/>

## Troubleshoot Site-Publish Issues

Compared with User/HTTP authentication, Site-Publish provides more flexible and advanced features such as single sign-on (SSO) and combination access control and authentication such as Two-factor authentication.

The sections below will introduce troubleshooting methods according to Site-Publish deployment scenarios:

- Common troubleshooting methods
- Typical authentication failures
- Two-factor authentication issues
- SAML issues
- Kerberos Issues

### Common troubleshooting steps for Site-Publish issues

1. For all issues, it's better to double check the necessary configuration steps for Site-Publish:
  - Remote servers are created in **User > Remote Server**;
  - Remote servers are added to **Application Delivery > Site Publish > Authentication Server Pool**;
  - Site Publish Rule is created in **Application Delivery > Site Publish > Site Publish Rule**;
    - Published Site, Path, Client Authentication Method, and Authentication Server Pool are configured correctly;

- Delegation servers and parameters are correctly configured;  
Please Note that some fields such as URL Path KCD SPN are case sensitive. You must input the exact upper or lower case strings.
  - The Site Publish Rule is added into a Site Publish Policy;
  - The Site Publish Policy is selected in a Web Protection Profile;
  - The Web Protection Profile is selected by the server-policy to protect the target website.
2. Check the connectivity & availability of remote servers for authentication server pool:  
You can check the connectivity and service availability via below steps:
- Ensure the IP address and service ports configuration on FortiWeb comply with which are provided by the remote servers;
  - Use ping to confirm no connectivity issue between FortiWeb and the remote server;
  - Use the Test button ("Test LDAP" or "Test Radius") in **User > Remote Server > LDAP/Radius Server** to test if the remote server can be connected successfully;
  - Use browsers or other test clients rather than FortiWeb to visit the backend server to confirm if the backend server is reachable;
  - Use a different remote server to determine if the authentication just fails with a specific type of remote server;
  - Capture packets on FortiWeb and the remote server to determine if the authentication queries are sent out by FortiWeb, if responses are correctly received by FortiWeb or delayed, and if the queries are received by the remote server, etc.
3. Enable Event log for site-publish rule and check the login failure logs on FortiWeb.  
To generate event logs, go to **Application Delivery > Site Publish > Site Publish Rule > Edit a Rule > Alert Type**, select **Failed Only or All**, then you'll be able to see event logs when an authentication failure occurs. Such event logs are usually simple, but can help us to confirm the issue.

E.g.

```
v012xxxxdate=2022-05-05 time=15:19:19 log_id=11002003 msg_id=000006998393
device_id=FVVM08TM21000613 vd="root" timezone="(GMT-7:00)Mountain Time
(US&Canada)" timezone_dayst="GMTb+7" type=event subtype="system" pri=alert
trigger_policy="N/A" user=daemon ui=daemon action=login status=failure
msg="User user01 [Site Publish] login failed on portal.testdomain.com from
172.30.212.181"
```

4. Check logs on the remote servers.

FortiWeb supports using remote servers including LDAP, Radius, KDC, SAML servers to authenticate clients, and also support

If authentication queries are sent out from FortiWeb and received by remote servers, while eventually fail to be authenticated, logs with detailed process or failure reasons can usually be generated by these servers. Checking such logs often helps to find the cause of failures.

Particularly, if FortiAuthenticator is used as the remote servers, you can check two types of FortiAuthenticator logs:

- Event logs: **FortiAuthenticator > Logging > Log Access > Logs**
- Debug logs: visit [HTTPS://<FortiAuthenticator\\_IP>/debug/](https://<FortiAuthenticator_IP>/debug/).

Please refer to an 2FA auth failure caused by invalid token as below:

The screenshot shows the FortiAuthenticator VM interface with a log table and a web browser window. The log table lists various authentication events, with one entry highlighted: 'Local user authentication with FortiToken failed: invalid token'. The browser window shows the URL 'https://10.65.164/radius/' and a dropdown menu for 'RADIUS Authentication'. Below the browser, a detailed log snippet shows the RADIUS authentication process, including messages like 'Fortinet-FAC-Challenge-Code = "001"', 'State = 0x31', and 'Authentication failed'.

5. Check site-publish diagnose logs:

It's simple to enable site-publish related diagnose logs, which can provide very detailed information for the packet processing flow:

```
# diagnose debug flow filter module-detail site-publish 7
# diagnose debug flow filter flow-detail 0 # available since 7.4.1
# diagnose debug flow trace start # available since 7.4.1
# diagnose debug timestamp enable
# diagnose debug enable
```

Besides, if you're not sure if the issue is related to other FortiWeb features, or need logs of the complete user access session, please also enable diagnose flow logs for further investigation.

```
# diagnose debug flow filter flow-detail 7 #Enables messages from each packet
processing module and packet flow traces
# diagnose debug flow filter HTTP-detail 7 #HTTP parser details
# diagnose debug flow filter server-ip 192.168.12.12 #The VIP in RP mode or
the real server IP in TP/TI mode
# diagnose debug flow filter client-ip 192.168.12.1 #The client IP
# diagnose debug flow trace start
```

Some site-publish diagnose failure logs are as below:

Remote server is not reachable:

```
[SP: MAIN][WARN](./waf_module/site_publish.c: 6736): LDAP server [10.65.1.97, 636,
1] is down by health check, then stop and auth failed
```

```
[SP: MAIN][DBG](./waf_module/site_publish.c: 6776): fail to auth [401]: username =
  user01, password = [X]
Incorrect username or password:
[SP: MAIN][INFO](./waf_module/site_publish.c: 6736): got active IP [10.65.1.96]
  from health check
[SP: MAIN][DBG](./waf_module/site_publish.c: 6776): fail to auth [401]: username =
  user01, password = [X]
[SP: MAIN][DBG](./waf_module/site_publish.c: 1135): elog : username: [user01]
Incorrect service principal name when the Authentication Delegation is Kerberos
  Constrained Delegation:
[SP: MAIN][DBG](./waf_module/site_publish.c: 10500): kerberos constrained
  delegation
[SP: MAIN][DBG](./waf_module/site_publish.c: 7981): spn rule is single_server
[SP: MAIN][ERR](./waf_module/site_publish.c: 5290): fail to AS of KCD
  [host/test1.sitepublish.fortiweb@SITEPUBLISH.FORTIWEB]
[SP: MAIN][ERR](./waf_module/site_publish.c: 10518): fail to check AS of KCD,
  bypas
```

## 6. Capture packets on FortiWeb and the remote server to analyze the authentication traffic flow.

Analyzing packet interaction between FortiWeb and the remote server are usually the ultimate method to troubleshoot authentication failures, especially when logs on either FortiWeb or remote servers are insufficient.

You can get the following information from captured packets:

- If the authentication queries and requests are sent out by FortiWeb and received by the remote server;
- If responses (accept or challenge) are sent back by the remote server and received by FortiWeb;
- If there is any delay when FortiWeb sending out a request, or the remote server sending back the response;

Clients, FortiWeb and remote servers usually have their own timeout settings for the authentication session. As long as either of these timeout periods elapses before the response is received, it may lead to an authentication failure.

This problem is very common. Latency in the Internet, special or misconfigured topology often result in such issues.

- If the traffic interaction complies with the application or protocol requirement and definition;
 

This method requires in-depth understanding of authentication protocols and state machine interaction such as Radius, LDAP/LDAPS, SAML, etc. A simple way to narrow down the issue is comparing the packet flow between a successful authentication and an unsuccessful access.

For some uncommon servers and user-defined servers, this way is useful to find the protocol compatibility problem.

## 7. Some issues are related to browser behaviors. They might be issues that can be resolved by updating to the latest version. You can also change a browser and try again.

### If the browser does not prompt authentication window or form

When the authentication form is not prompted by the browser when visiting the target URL or Path, you can check the following:

- Check if there is any missing configuration.
  - Check if the correct site publish rule is included in site publish policy, and the policy is included in the web protection profile used in the server-policy;
  - Check if the Published Site & Path are correctly configured;

For regular expression, use the built-in Regular Expression Validator to confirm the published site domain can be matched; for Path or URL, confirm it's case sensitive.

- Particularly, check if any remote server is included in the authentication Server Pool selected by the site publish rule.

This is a common issue of configuration missing that often occurs in customers' sites. Just remember to add Remote Servers to a server pool used by a site publish rule.

- Check if the Path/URL matches URL Access rules.

In 6.3 and later builds, URL Access Rule is processed before Site Publish, so if the certain URL/Path matches a URL Access Rule with Action "Pass", the site-publish rule will be skipped,

To resolve this issue, you can remove the conflicted URL Access Rule or configure the Action of the URL Access Rule as "Continue", then FortiWeb will continue processing the request and site publish rules will be matched.

Sometimes if you suspect other WAF features cause the issue, you can check **FortiWeb Admin Guide > Key concepts > Sequence of scans** to see if any other features processed prior to Site-Publish are configured. You can remove the feature to try again.

## If authentication fails

Authentication failures have different causes:

- Login user/password or token mistakes.

If the username, password, or token (2FA method) is wrong, the browser usually has kinds of behaviors such as keeping a pop-up sign-in window, prompting "Invalid credentials" or "Login Failed" message.

- Check if remote server members in the Authentication Server Pool are reachable from FortiWeb.

If the remote server IP is not reachable, service port is unreachable (or incorrectly configured), or has other configuration mistakes such as Radius server secret, one can make a quick judgment from the error messages or browser behavior.

The error messages vary according to different client authentication methods or remote servers. For example, the browser may keep popping up the Sign in window (HTTP Basic Authentication method), or the Authentication Form will prompt a warning message like "Failed to connect LDAP server" or "RADIUS response timeout", etc.

IP unreachable or Invalid secret

**Authentication Required**

**Bad response from RADIUS server**

**Please enter your RSA SecurID to continue**

Username:

Passcode:

Incorrect port

**Authentication Required**

**RADIUS response timeout**

**Please enter your RSA SecurID to continue**

Username:

Passcode:

IP or service unreachable

**Authentication Required**

**Failed to connect LDAP server**

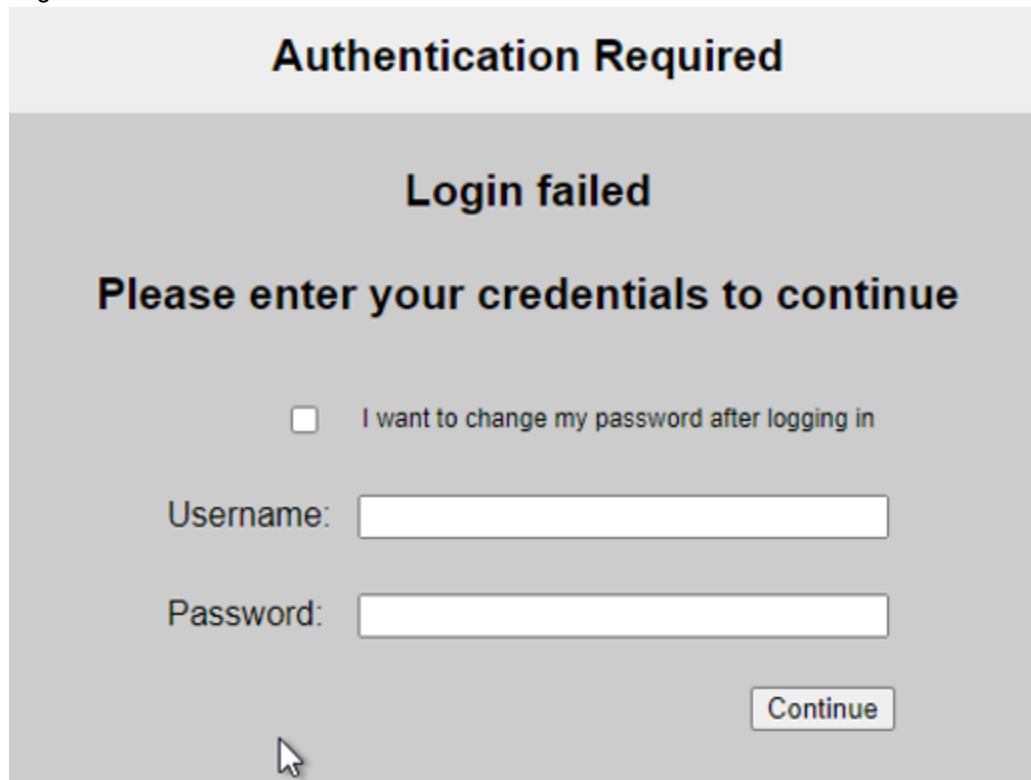
**Please enter your credentials to continue**

I want to change my password after logging in

Username:

Password:

Login failed



You can check the connectivity and service availability issues with steps in above section: "[Common troubleshooting steps for Site-Publish issues](#): Check the connectivity & availability of remote servers for authentication server pool".

- Check if the backend server configured in Authentication Delegation behaves as expected.
  - Double confirm that the corresponding servers such as KDC server for authentication delegation is correctly configured;
  - Check if access to the backend server directly can be successful, rather than pass through FortiWeb.
  - Change and test with a different Authentication Delegation type;
  - For Form Based Delegation:
    - If needed, clone the predefined templates, and edit the settings as your desire
  - For Kerberos delegation:
    - Please refer to the following section "Kerberos issues" for more details.
- Some special requirement or notes on configuration:
  - For Two-factor site-publish rules, "Client Authentication Method" needs to be "HTML Form Authentication".

Two-factor authentication requires configuring the "Client Authentication Method" as "HTML Form Authentication".

When choosing "HTTP Basic Authentication", the browser will keep on prompting the Sign in window, because this browser-specific method cannot display a second authentication form that allows users to enter a token code.
  - When Authentication Delegation is "HTTP Basic" in Site Publish Rule, "Basic Authentication" should

be enabled in the backend IIS while Forms Authentication should be disabled to avoid conflict. This is a restriction from the IIS side.

- Increase the auth-timeout when remote servers' response is slow

In the real environment, you may find the LDAP/Radius/SAML/NTLM/OAuth servers are slow to answer authentication queries by analyzing diagnose logs or captured packets. You can adjust the authentication timeout setting to prevent the query from failing.

```
configure system global
    set auth-timeout <milliseconds_int>
end
```

<milliseconds\_int> is the number of milliseconds that FortiWeb will wait for the remote authentication server to respond to its query. The valid range is 1–60,000 and the default value is 2000.

Besides Authentication server pool members for Site-Publish, this setting also affects remote authentication queries for administrator accounts.

## Two-factor authentication issues

Steps to troubleshoot two-factor authentication issues:

1. Check the Radius server configuration on FortiWeb; you can remove the 2FA configuration on the Radius server and use “Test Radius” button to confirm;
2. Remove 2FA authentication configuration on the Radius server, check if authentication can be successful if with only Radius;
3. Check FortiWeb configuration to ensure that “Client Authentication Method” is configured as “HTML Form Authentication” in the site-publish rule;
4. Check logs on Radius server to see if any clear failure logs:
  - If the Radius server is FortiAuthenticator, please refer to the above section to check detailed logs: 4.2 > Common troubleshooting > Check logs on the remote servers.
5. Capture packets on the front-end and back-end side. Analyze the traffic flow to see if any delays, response loss or abnormal packets.
  - Check if there is another request sent by the same client before the authentication process is done. An extra request will interrupt 2FA process and result in cookie reset;
  - A common example of such an extra request is favicon.ico. If it's the case, you can try to add a URL Access rule to deny (Action is Deny) this request;
  - If there are other requests such as the ones generated by JS script in the web code, you may try to add a URL Access rule to bypass (Action is Pass) this request
6. For further analysis, please also enable diagnose logs for site-publish simultaneously.

Refer to above section "[Common troubleshooting steps for Site-Publish issues: Collect diagnose logs](#)".

## SAML issues

1. Most SAML issues are configuration issues.

You'd better double verify the configuration on both IDP side and SP/FortiWeb side:

**FortiWeb > User > Remote Server > SAML Server:**

- **Entity ID:** the unique identity of SP; the host is the domain name of vserver. The prefix must be HTTPS.
- **IdP Metadata:** upload a valid IdP metadata file, which is exported from the IdP;  
For any changes on the IdP, please export the metadata file and upload to FortiWeb again.
- **IdP Entity ID:** double confirm this ID displayed after the IdP metadata file uploaded is identical to that shown on the IdP
- After SAML Server is configured, click **Generate Service Provider Metadata** to export a metadata file, and import the file to IdP.

If you change any item of SAML server, you must regenerate Service Provider Metadata file and reconfigure IDP. Particularly, please make sure the "Location" in the metadata file matches the "Published Site" (Domain) configured in the Site-publish rule.

E.g.

```
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="HTTPS://portal.testdomain.com/new_saml_server/saml.sso/SLO/POST"/>
```

#### On IdP Side (AD FS, FortiAuthenticator, etc.):

- **SP Metadata:** import the one generated on FortiWeb;  
For any changes on SAML Server, it's better to update this file again.
- Make sure the user information (UPN or Email) is mapped to EPPN (urn:oid:1.3.6.1.4.1.5923.1.1.1.6), because FortiWeb uses the value of the EPPN attribute to identify users uniquely.

#### FortiWeb > Application Delivery > Site Publish > Site Publish Rule:

- The correct SAML Server is selected;
- The **Published Site** should be consistent with the host of SAML Server's Entity ID.

#### 2. Other checking points:

- All IdP and SP configuration are case sensitive;
- Make sure the clocks of all the related servers (DC, FortiWeb, IDP, etc.) are synchronized;
- For cross domain environments, if the AD Domain trusts each other, you can share one ADFS instance. But if not, you would need one ADFS instance for each AD.
- If IDP is ADFS, the global logout url is HTTPS://<ADFS\_Service\_FQDN>/adfs/ls/?wa=wsignout1.0

#### 3. Enable and check diagnose logs:

```
# diagnose debug flow filter module-detail site-publish 7
# diagnose debug flow filter flow-detail 0 # available since 7.4.1
# diagnose debug flow trace start # available since 7.4.1
# diagnose debug timestamp enable
# diagnose debug enable
```

#### 4. Collect SAML related logs with below steps for dev team analysis:

- Edit /data/etc/saml/shibboleth/\*.logger, switch the default level on the top to DEBUG.  
/data/etc/saml/shibboleth#cat shibd.logger  
log4j.rootCategory=DEBUG, shibd\_log #The default level is WARN  
/data/etc/saml/shibboleth#cat native.logger  
log4j.rootCategory=DEBUG, native\_log #The default level is WARN  
**Note:** Don't forget to restore to the default level WARN to avoid performance issues.
- Restart proxyd & shibd
- Reproduce the issue

- Collect the logs under `/var/log/shibboleth/`. You may clear them before you test it  
You can copy these logs to `/var/og/gui_upload` and download them from GUI.

```
~# ls -l /var/log/shibboleth/
-rw-r--r--  1 root  0  9744 May 13 14:44 native.log
-rw-r--r--  1 root  0  30712 May 13 14:44 shibd.log
```

## Kerberos issues

### 1. Check Kerberos related configuration

The most common issues caused by Kerberos authentication failures are also configuration mistakes. When issues occur, you need to check the configuration on FortiWeb and the backend KDC server.

This section will not focus on configuration details for different KDC servers, but only introduce some general considerations or mistakes in both FortiWeb & KDC settings.

#### FortiWeb > User > Remote Server > KDC Server:

- **Delegated Realm:** It should be all capitalized. It's the domain of the domain controller (DC) that the KDC belongs to. Typically the UPN (User Principal Name) used for login has the format `username@delegated_realm`.
- **Shortname:** An alias of the realm you specified. The shortname can include the domain name of the realm that is not fully qualified. With a shortname being configured, the format of UPN can be `username@shortname`

A shortname is used in a scenario when the complete Kerberos realm (e.g. TEST.FortiWebDEMO.COM) is different from what a client gets from their username (e.g. the username FortiWeb gets from the IDP is an email address like `(xxx@FortiWebDEMO.COM)`). If the customer can set the UPN as the username returned to FortiWeb, shortname is not needed; otherwise, FortiWeb would have to set a shortname to make Kerberos work.

#### FortiWeb > Application Delivery > Site Publish > Site Publish Rule:

- There are two kinds of **Authentication Delegation**:
  - **Kerberos:** also called the Regular or Basic Kerberos Delegation; available only when Client Authentication Method is HTML Form Authentication or HTML Basic Authentication. You just need a `username&password` for delegation.
  - **Kerberos Constrained Authentication:** available when Client Authentication Method is Client Certificate, SAML or NTLM. You just need UPN (User Principle Name); the delegator will help you get access tickets.
- **Delegated HTTP Service Principal Name (SPN):** Make sure the Service Principal Name is configured with exactly the same string and upper/lower case with that configured in AD; and, all realm such as the domain name after `@` should be upper case

The format is like:

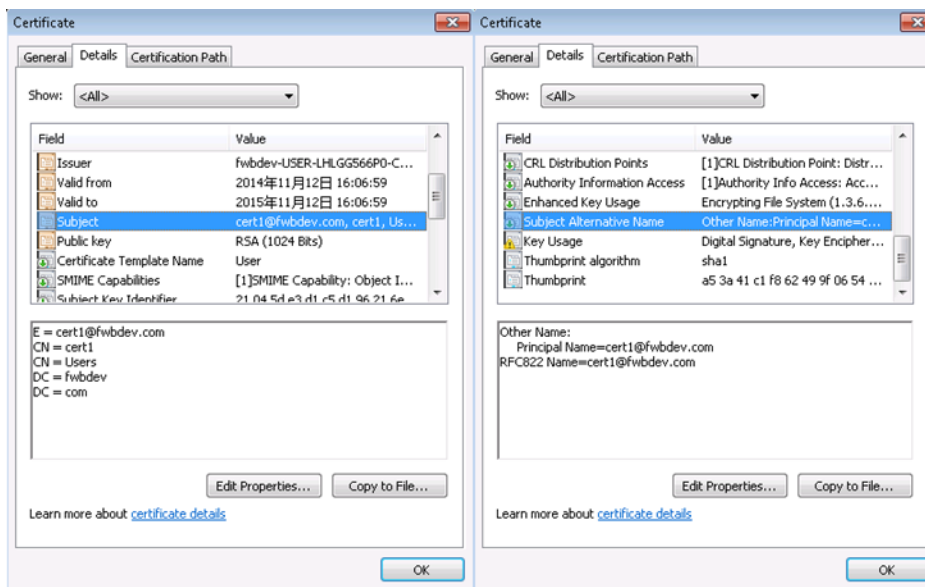
```
<protocol >/<exchange_server_hostname>/<realm>
```

- **protocol:** HTTP
- **exchange server hostname:** USER-LHLGG566P0 (case-insensitive), you may also use the full name `USER-U3LOJFPLH1.FortiWebdemo.com`
- **realm:** FortiWebDEMO.COM; should be capital  
E.g. `HTTP/USER-U3LOJFPLH1.FortiWebdemo.com@FortiWebDEMO.COM`

- **Default Domain Prefix Support:** For Regular Kerberos delegation only. The domain controller usually requires users to log in with the username format domain\username such as EXAMPLE\user1. Alternatively, enable this option and enter EXAMPLE for Default Domain Prefix, the user enters user1 for the username value and FortiWeb will automatically add EXAMPLE\ to the HTTP Authorization: header before it forwards it to the web application
- **Keytab File:** For Kerberos Constrained Delegation only. Select the keytab file configuration for the AD user that FortiWeb uses to obtain Kerberos service tickets for clients.  
For instructions on how to generate the keytab file, see FortiWeb Admin Guide > Application Delivery > Site Publishing > Creating an Active Directory (AD) user for FortiWeb - Keytab File.
- **Service Principal Name for Keytab File:** For Regular Kerberos delegation only. It's the SPN that you used to generate the keytab specified by Keytab File. Don't forget the realm suffix.

Particular requirement for **Client Certification Authentication:**

- Double check that **Client Certificate Verification** is correctly configured and bound to the server-policy.
- For Username Location in Certificate in Site Publish rule, here's an example.  
The username we need is cert1@fwbdev.com, then you may specify the location you want, Subject or Subject Alternative Name (SAN). However, the most exact one is UPN (aka Other Name > Principal Name) in SAN, so you'd better keep the default.



**Some Tips on KDC servers:**

- Create an HTTP-delegator which is a domain account to do authentication delegation. Please refer to FortiWeb Admin Guide > Application Delivery > Site Publishing > Creating an Active Directory section for details.
- Make sure the account & its password never expire.
- Don't use \$setspn -A .... Instead, use \$setspn -S ... to create SPN for the account

2. Other checking points:

Make sure the clocks of all the related servers (DC, FortiWeb, IDP, etc.) are synchronized, otherwise Kerberos tickets will be invalid.

### 3. Collect information for further investigation:

Diagnose logs when the issue happens:

```
# diagnose debug flow filter module-detail site-publish 7
# diagnose debug flow filter flow-detail 0 # available since 7.4.1
# diagnose debug flow trace start # available since 7.4.1
# diagnose debug timestamp enable
# diagnose debug enable
```

### 4. Test with FortiWeb backend tool krb\_test and collect the output:

- Login to FortiWeb backend shell.

Here is the usage below:

```
FortiWeb # fn krb_test
[krb_test error] (krb_test.c: 744): usage: krb_test -s <webserver SPN> [options] -h <host> -l <url> [...] <credentials>
[krb_test error] (krb_test.c: 744): options:
[krb_test error] (krb_test.c: 744):   -H: custom host header
[krb_test error] (krb_test.c: 744):   -t: use SSL tunnel
[krb_test error] (krb_test.c: 744):   -T: kerberos use spnego (default krb5)
[krb_test error] (krb_test.c: 744):   -c: client certificate file (PEM or DER)
[krb_test error] (krb_test.c: 744):   -e: client private key file (ditto)
[krb_test error] (krb_test.c: 744):   -a: port of web access (default: 80)
[krb_test error] (krb_test.c: 744):   -m: connection timeout (default: 2 secs)
[krb_test error] (krb_test.c: 744): credential types:
[krb_test error] (krb_test.c: 744):   basic: -u <user UPN> -p <password>
[krb_test error] (krb_test.c: 744):   KCD:   -u <delegated UPN> -n <delegator UPN> -k <delegator keytab>
[krb_test error] (krb_test.c: 744): examples:
[krb_test error] (krb_test.c: 744):   krb_test -s http://webservers@DC.COM -h 192.168.1.1 -H mail.dc.com -l /owa/ -u user@DC.COM -p cred
[krb_test error] (krb_test.c: 744):   krb_test -s http://webservers@DC.COM -t -a 8080 -h 192.168.1.1 -l /owa/ -u user@DC.COM -p cred
[krb_test error] (krb_test.c: 744):   krb_test -s http://webservers@DC.COM -t -c user.crt -e user.key -h 192.168.1.1 -l /owa/ -u user@DC.COM -p cred
[krb_test error] (krb_test.c: 744):   krb_test -s http://webservers@DC.COM -h 192.168.1.1 -l /owa/ -u user@DC.COM -n HOST/delegator@DC.COM -k delegator.keytab
[krb_test error] (krb_test.c: 744):
```

#### Note:

**-s:** the same with Delegated HTTP Service Principal Name

**-h:** IP or domain name of the backend web server (aka pserver); if you use **-H**, the value of Host header in request will be overwritten.

**-t:** Use SSL tunnel for the backend web server. **-c** and **-e** are used for client certificate authentication for basic Kerberos:

**-u:** UPN for login, and the format must be username@DOMAIN.COM

**-p:** it's password

for KCD:

**-u:** ditto

**-n:** delegator's UPN, it's the same with Service Principal Name for Keytab File

**-k:** file path of your keytab file in FortiWeb (you should upload it first)

An example of the successful result: (response returns 200 OK)

```

FortiWeb # fn krb_test -s httpowa2010.fwbqa.com@FWBQA.COM -h 10.0.1.9 -l /owa/ -u qa001@FWBQA.COM -p fortinet
[krb_test debug] (krb_test.c: 748): ===== INITIALIZATION =====
[krb_test debug] (krb_test.c: 749): SPN: http://owa2010.fwbqa.com@FWBQA.COM
[krb_test debug] (krb_test.c: 750): SSL: off
[krb_test debug] (krb_test.c: 755): host: 10.0.1.9
[krb_test debug] (krb_test.c: 759): port: 80
[krb_test debug] (krb_test.c: 760): timeout: 2
[krb_test debug] (krb_test.c: 761): urls: 1
[krb_test debug] (krb_test.c: 764): [ /owa/ ]
[krb_test debug] (krb_test.c: 766): thread-safe: yes
[krb_test debug] (krb_test.c: 767): mode: basic
[krb_test debug] (krb_test.c: 768): UPN: qa001@FWBQA.COM
[krb_test debug] (krb_test.c: 770): password: fortinet
[krb_test debug] (krb_test.c: 777): krb_type : krb5
[krb_test debug] (krb_test.c: 789):
starting...
[krb_test debug] (krb_test.c: 797): ===== AS =====
load flag
load file
[krb_test debug] (krb_test.c: 821): ===== TGS =====
[krb_test debug] (krb_test.c: 452): ===== CREATE CONNECTION =====
[krb_test debug] (krb_test.c: 495): ===== REQUEST-0 [1795] =====
GET /owa/ HTTP/1.1
User-Agent: Fortiweb
Host: 10.0.1.9:80
Authorization: Negotiate YIIIEBAYJkoZihvcSAQ1CAQBUggTFMIE26ADAqEFoQmCA061bWmFACAaAAACgop1YYID8TCCA+2qAwIBBAEGLVQ0JRQ55DT02LJDAtoAMCA0ghGzAZGwRodhRwGxFvd2EYmDEwLz3YnFhLmNva0CA7Ewg0toAMCArkHA
wIB56KASB8Eggb0gognd92o4MUsotxFzKqYMBWKEsUJAZA354b35jTfHLhIQ0TumVjgKHRBgZX/RbRb9Sk1BP5P9++2ob0j0RDIxWj1Saw+eNemq15+aqg/Yk0w5VEkvY2+KLuH7mMU70HDJUTdsd/w9c9pg5LzmcKXqntZ0JuZ+68Q92FhIroW09
YmR4SH2dWdsnmwHSA1Xt3j1lqAWdWuH7EDYNOipNggr19UR9EtX7hooFVl/vLlLasal/9Wm1040Yl+50Y0xogYRMBtwAbiqLLMtcBTS0cys903CyrmsI+sZnH1BUwvZ01Bq4L0wzCCBf6akHAmo/w020/0xsLMxydmdQldtAdZ8MuqCYq1GWN9
LRBYyFBkj7ahjg5h0VQ689qAq00R22fYy6e390Bsd697fnoaf27WYmYkVYQwntBz1sE5Hz0VjE7249Y7eDhHf0skzb3hrf0i63H+3WdcITZlerbbkFfZGEZ3Ty009RtyRkcegeVehcz3mluo03i0Wkua0i3j0051D99ByAm4Gf
+ZkP0fTWJZfz++1jwDRc2NdFKmmTRL+GhYmVJ6Fqpb/+01CYt3wfsrQawzVhX725XQqB+WUmf036kH25fL9aa13KEj1jso0p4NBRH+XSxUz6p0wqxLMPom/7KbDnTCGrSCYdI6x0QnUv4Q13qRwz/d3W8mj9eU2WkRfNf2T1sGQMdCn70t+LKR
ZxoaSaeG0PUy3+cd0EY7nj6faDqto/caySHf0knbq1IBAmE2CfybVRj4328Bral/3F0n99rDwoXeGvk+r+71p2JVF2HxIkUpBvM3p6ah7mBY8Hfm/qnb14pRLbNDwC6dksLZorH1nDbG27M9zIU9o/1mHyYpsGjV+JNRS/S8mwGskXZD1JG2
KfyjRkBaoc557kdvyjxj47UmdKryxjBfZSLkXxYbA1l6TEryfB7te+FSQmHlKEV6f1VbcYQ/av/NPR04H0F/q8q5M0uh7d23/0XCCGTZTfHYX0Ltnobxwz0t0B8cG1tcWu0Q3AV2Pn/q0TPke4BN0y044dnxKPT/Las1ADfn/7bFm9SURG
0250/28S53Y41wqSR0wY+HNEEBj1s0ZxSL38SH87wKmp03j3q1W6Ymthc+saHk+3B5Kwkr0kGwgcmgw1BEq8vQ8V3p158EgQwHqoL1407ZedkMkRSBWR1vay1Xam1387w0d11Z0085HmH0vabxn1TQsyxSPZ3Tog19c/1so10
Seyxctn3RT0q052G6AgnXqDhJwC+q0pAx7V0VHGhNYUPx5fa3TqRfEb8XuhFwC2u07svCw6eN5SD0gTHEKrv0b3VGAaFjovTYSMteq6sX1KMMyVjVfZ3J34UNLmq18guyrB8Vf6qyQz2dLGYsV5sb0AYFw=
Accept: */*

[krb_test debug] (krb_test.c: 505): ===== RESPONSE-0 [1280] =====
HTTP/1.1 200 OK
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-IIS/7.5
    
```

If the test fails, that means there are some problems in Kerberos authentication or backend communication. Please note the debug information on the screen.

If the test succeeds, that means configuration or login input may be incorrect. Need to check them and keep the parameters consistent with those in krb\_test.

## Application Delivery - Caching

### FAQ

#### How to enable Caching?

Follow the steps below to enable web cache for a server policy in Reverse Proxy, TTP or WCCP modes:

1. Enable Web Cache in **System > Config > Feature Visibility**;
2. Enable Web Cache when creating or editing an HTTP server policy in **Policy > Server Policy**, then a web cache policy will be automatically created in **Application Delivery > Caching**;
3. You can click the icon **View Configuration** besides the **Web Cache** option in the server-policy edit page, or visit **Application > Caching** to edit the configuration of a web cache policy;
4. In the **Edit Web Cache Policy** page, click **Create New** to add one or multiple web cache rules.

Notes:

- Web cache rule is a **MUST**, otherwise the web cache policy will not be matched;
- If multiple rules are configured in one policy, then these rules will be matched in order. That is to say, when the first rule is matched, the other rules followed will be skipped and not take effect any more.

#### What can be cached and what cannot be cached?

Caching generally works best with data that doesn't change. Things like static web pages, images, movies, and music all typically work well.

FortiWeb will NOT cache responses if the request:

- Has fields such as Cache-Control: no-cache/no-store/; Pragma:no-cache
- Contains the header:
  - Authorization
  - Proxy-Authorization

FortiWeb also will NOT cache if the response:

- Has a Set-Cookie: field
- Has a Vary: field
- Has fields such as Cache-Control: no-cache/no-store/private; Pragma:no-cache; Cache-Control: max-age=0
- Proxy-Authorization
- Connection
- Proxy-Authenticate
- TE
- Trailers
- Transfer-Encoding #So Transfer-Encoding: chunked is NOT supported
- Upgrade

#### **What does Key Generation Factor in Web Cache Rule mean?**

Subsequent visits will match the cache rule only if all key generation factors in the request are the same as the request/response that has been cached.

For example, if both Host&URL are selected in the Key Generation Factor, then a request with a different Host will not match the cached content.

Cookies can be enabled in **Key Generation Factor > Cookies** with a specific cookie name configured in **Add Cookie Name**, which allows caching a response when the request header includes "Cookie: <name>=<value>".

#### **What is the maximum size of a file that can be cached?**

The maximum of a single file that can be cached is 8 MB.

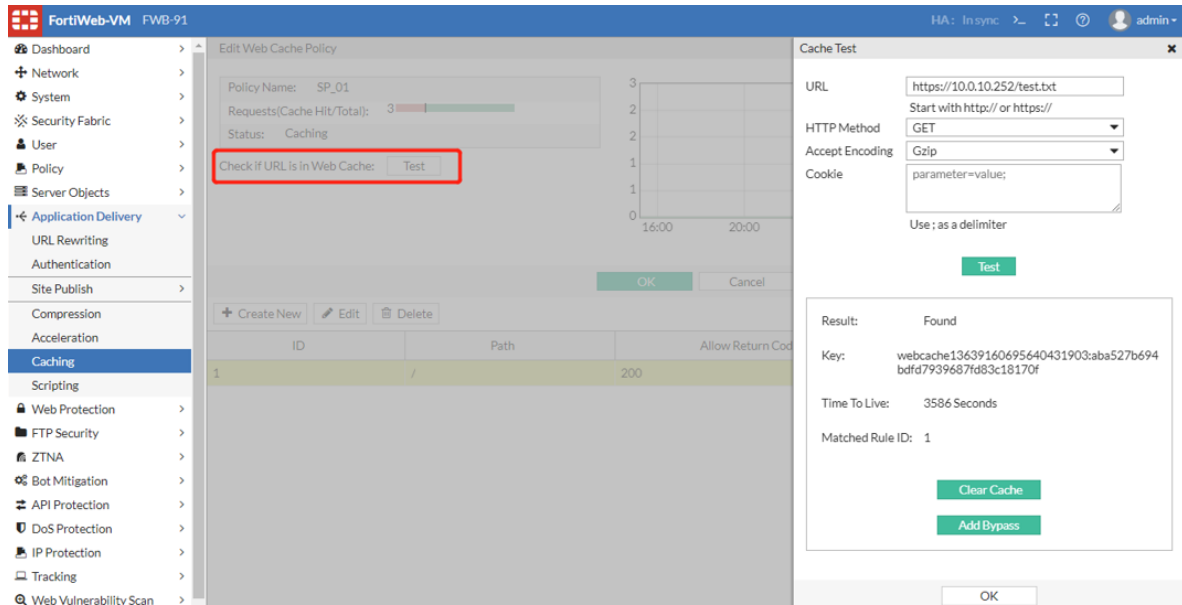
FortiWeb uses the header `Content-Length` to identify the size of the entity-body. If the `Transfer-Encoding` is chunked, the content will not be cached.

## **Troubleshoot for caching issues**

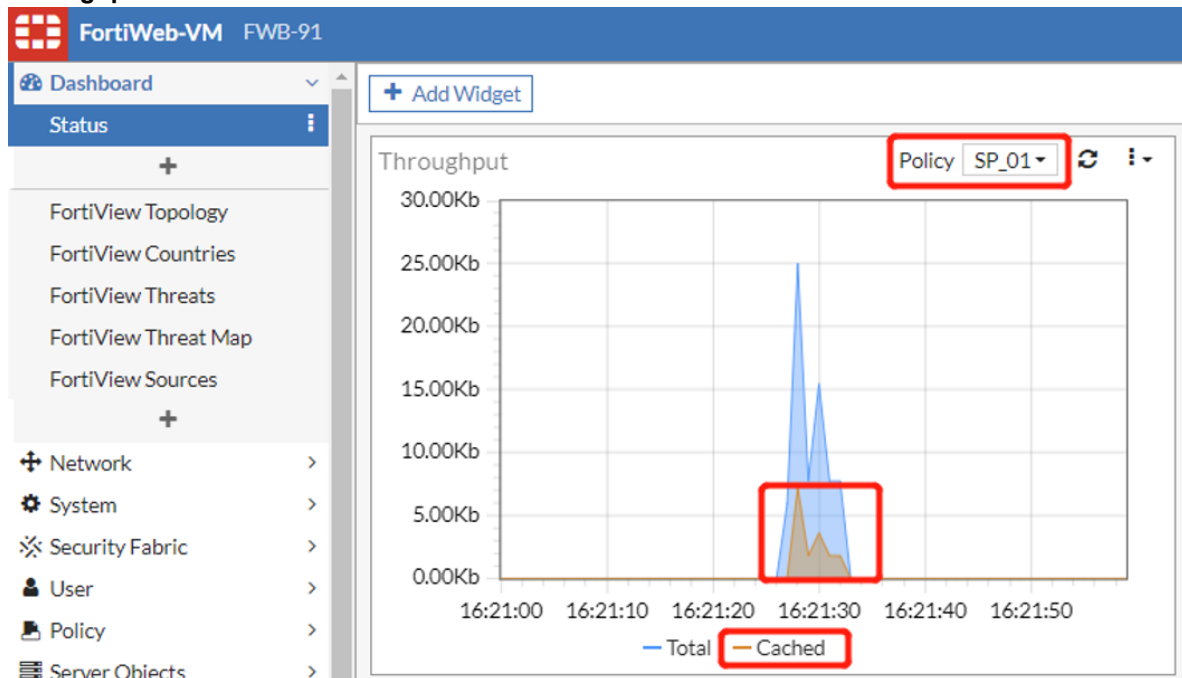
There are several methods for troubleshooting if a URL is not cached as expected:

1. Check web cache configuration;  
Examine if the specific headers of the request match the cache rule: Host, Path/URL, HTTP Method, Return Code, File Type and Key Generation Factors.

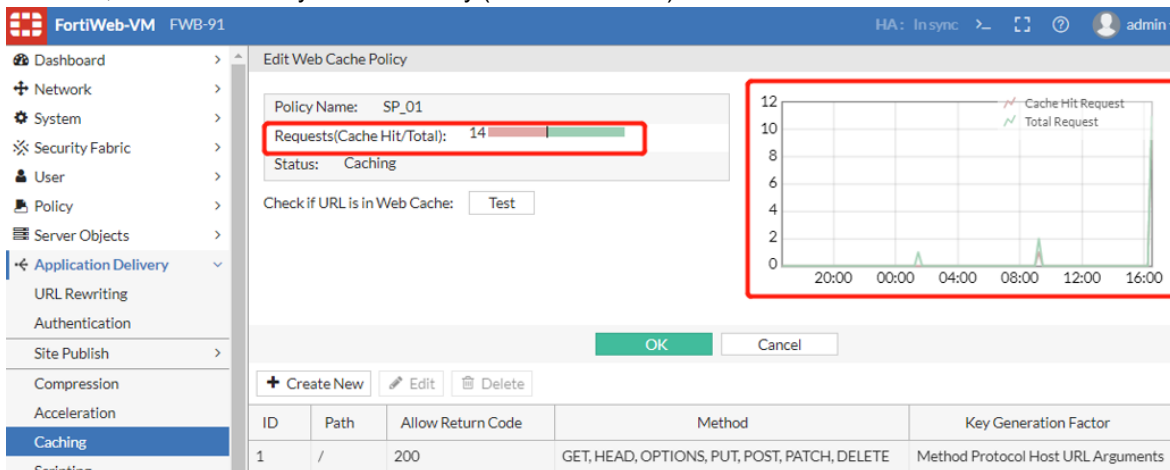
- On 7.0.2 & later builds, click the button **Test** to check if a URL can hit the web cache:



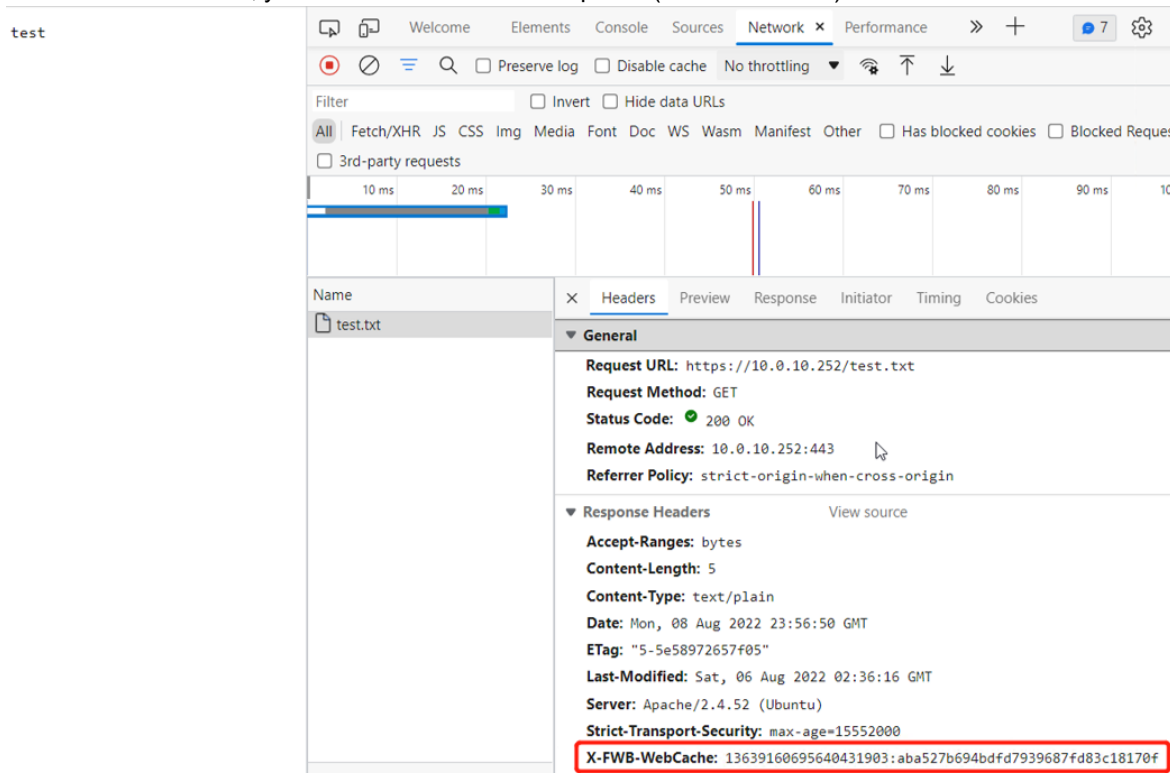
- On 7.0.2 & later builds, when cached content is hit, there will be statistics in **Dashboard > Status > Throughput:**



- On 6.3.x & later builds, you can also check if the Requests (Cache Hit/Total) count increase. However, this count usually has time delay (max 15 minutes) after the cache is hit.



- Check if the response is replied by FortiWeb or the back-end server. On 7.0.0 & later builds, you can also check if the Requests (Cache Hit/Total) count increase.



On 6.3, you need to capture packets on FortiWeb and check if the new request is sent to the back-end server. If a request is not sent to the back-end server while the client can receive the replay, cache content should be hit.

- You can also enable diagnose logs to check more processing details or collect information for further analysis.

```
FWB # diagnose debug flow filter module-detail web-cache 5
FWB # diagnose debug flow filter flow-detail 0 # available since 7.4.1
FWB # diagnose debug flow trace start # available since 7.4.1
FWB # diagnose debug enable
```

**Example for a successful cache hit:**

```
[web cache][DBG_H](./waf_module/web_cache.c:3973): web_cache_process: begin
[web cache][DBG_H](./waf_module/web_cache.c:3141): process_web_cache_s2c_hash_
table: begin
[web cache][DBG_H](./waf_module/web_cache.c:3145): process_web_cache_s2c_hash_
table: WEB_CACHE_CACHE_HT_HIT in response
[web cache][INFO](./waf_module/web_cache.c:3148): process_web_cache_s2c_hash_
table: The WEB content is from WEB Cache!
[web cache][DBG_H](./waf_module/web_cache.c:281): req_match_single_rule: match web
cache rule success : /
```

**Example for cache hit failure:**

```
[web cache][DBG_H](./waf_module/web_cache.c:3973): web_cache_process: begin
[web cache][DBG_H](./waf_module/web_cache.c:3141): process_web_cache_s2c_hash_
table: begin
[web cache][DBG_H](./waf_module/web_cache.c:3168): process_web_cache_s2c_hash_
table: WEB_CACHE_HT_PREPARE_CACHE in response
[web cache][INFO](./waf_module/web_cache.c:3170): process_web_cache_s2c_hash_
table: The WEB content is from Physical server!
[web cache][DBG_H](./waf_module/web_cache.c:281): req_match_single_rule: match web
cache rule success : /
```

## Application Delivery - Lua Script

From 7.0.2, FortiWeb supports Lua scripts to perform actions that are not currently supported by the built-in feature set. You can use Lua scripts to write simple, network aware pieces of code that will influence network traffic in a variety of ways.

In FortiWeb, the scripting language only supports HTTP and HTTPS policy in Reverse Proxy mode. And, FortiWeb uses the lua version 5.4.

Please refer to the Script Reference Guide for more details.

## FAQ

### What's the order of multiple scripts matching?

When multiple scripts are selected in one server policy, the system will load scripts one by one. If there are multiple same events defined in the scripts, the event running order is the same as the loading order.

### How to troubleshoot Scripting issues?

If you find your customized scripting does not work as expected, follow the steps below for troubleshooting:

1. Ensure diagnose debug to check if the output matches the events and actions defined in the selected scripts:

```
# diagnose debug proxy scripting-core 7 #scripting initiating and loading
information
# diagnose debug proxy scripting-user 7 #scripting user debug logs
# diagnose debug timestamp enable
# diagnose debug enable
```

For example, if the predefined script HTTP\_GET\_COMMANDS is selected in a server-policy, then below logs will be printed HTTP requests hit the policy. You can also add extra debug print with debug() or other built-in functions to diagnose the problem you encounter.

```
<18: 7:39>[script-core]: flua init session ctx 0x7fdc0b0fc000, core 0x7fdc29008200
<18: 7:39>[script-core]: FLUA init http substream ctx 0x7fdc2e768680, session ctx
0x7fdc0b0fc000!
<18: 7:39>[script-user]: ===== Dump HTTP request header =====
<18: 7:39>[script-user]: host: 10.0.10.191, path: /new, url: /new, method: GET,
version: HTTP/1.1
<18: 7:39>[script-user]: HEADER: Host[1]: 10.0.10.191
<18: 7:39>[script-user]: HEADER: User-Agent[1]: curl/7.83.1
<18: 7:39>[script-user]: HEADER: Accept[1]: */*
<18: 7:39>[script-user]: ===== Dump HTTP request header done =====
<18: 7:39>[script-user]: ===== Dump HTTP response header =====
<18: 7:39>[script-user]: status code: 404 reason: Not Found
<18: 7:39>[script-user]: HEADER: Content-Length[1]: 201
<18: 7:39>[script-user]: HEADER: Date[1]: Thu, 20 Oct 2022 01:01:45 GMT
<18: 7:39>[script-user]: HEADER: Server[1]: Apache/2.4.38 (Win64) OpenSSL/1.1.1b
PHP/7.0.5 mod_jk/1.2.42
<18: 7:39>[script-user]: HEADER: Content-Type[1]: text/html; charset=iso-8859-1
<18: 7:39>[script-user]: HEADER: return_header[1]: HTTP/1.1 404 Not Found
<18: 7:39>[script-user]: ===== Dump HTTP response header done =====
<18: 7:39>[script-core]: FLUA exit ctx 0x7fdc2e768680, core 0x7fdc29008200
<18: 7:39>[script-core]: FLUA exit ctx 0x7fdc0b0fc000, core 0x7fdc29008200
```

2. Collect your script, diagnose debug logs and the FortiWeb configuration file, send them to support for further analysis if you fail to find the cause.

## Application Delivery - Waiting Room

If you find your Waiting Room feature does not work as expected, follow the steps below for troubleshooting:

1. Run the following diagnose debug commands:

```
# diagnose policy wr-state list <policy-name>
# diagnose debug proxy cmdb-module 7
# diagnose debug proxy thread-wr 7
# diagnose debug flow filter module-detail waiting-room 7
```

2. Run the following commands:

```
# diagnose debug flow trace start
# diagnose debug timestamp enable
# diagnose debug flow filter flow 0
# diagnose debug enable
```

3. Here is an example output of the debug command:

- diagnose policy wr-state list <policy-name>

This command check the waiting room policy statistics based on the specified server policy.

```

FortiWeb #
FortiWeb #
FortiWeb # diagnose policy wr-state list root.FWB_Policy_Default_AutoTest

policy(FWB_Policy_Default_AutoTest)

ctrl(autotest)
  waf_wr_state_cnt           :           0
  remaining_slots_for_new_users :         1
  total_active_users         :           0
  total_waiting_number       :           0
  new_users_per_min          :           0
  avg_users_to_origin         :           0
  latest_wr_enter_origin_ts   :           0
  critical_cfg_change_ts     :           0
  is_threshold_reached       :           0

ctrl(content_2)
  waf_wr_state_cnt           :           1
  remaining_slots_for_new_users :         0
  total_active_users         :           1
  total_waiting_number       :           1
  new_users_per_min          :           2
  avg_users_to_origin         :           1
  latest_wr_enter_origin_ts   :    1696993173
  critical_cfg_change_ts     :           0
  is_threshold_reached       :           0

FortiWeb #
FortiWeb #

```

- diagnose debug proxy cmdb-module 7  
This command shows the debug information for waiting room configuration load status.

```

FortiWeb #
FortiWeb # [cmdb-module]: rcv waf-profile event
[cmdb-module]: waf_reload_profile_mod_exist: module pointer[0x7f7c999db000] opmode[2] adom id[1] current adom id[1] main type[71] sub-type[71] reload level[16] event type[1]
[cmdb-module]: waf_reload_profile_mod_exist: module pointer[0x7f7c99a73000] opmode[2] adom id[1] current adom id[1] main type[71] sub-type[71] reload level[16] event type[1]
[cmdb-module]: waf_reload_profile_modules: module pointer[0x7f7c99a73000] opmode[2] adom id[1] current adom id[1] main type[71] sub-type[71] reload level[16] event type[1]
[cmdb-module]: (reload_waiting_room_policy:3815)
[cmdb-module]: (reload_waiting_room_policy:3844) waiting room policy test's total_active_usr changed from 1 to 100. Force eligible slots reallocation
[cmdb-module]: (reload_waiting_room_policy:3862) read db to get global wr state for policy FWB_Policy_Default_AutoTest, adom_id = 1, ret = -1
[cmdb-module]: waf_reload_profile_mod_exist: module pointer[0x7f7c99a76000] opmode[2] adom id[1] current adom id[1] main type[71] sub-type[71] reload level[16] event type[1]
[cmdb-module]: waf_reload_profile_modules: module pointer[0x7f7c99a76000] opmode[2] adom id[1] current adom id[1] main type[71] sub-type[71] reload level[16] event type[1]
[cmdb-module]: (reload_waiting_room_policy:3815)
[cmdb-module]: (reload_waiting_room_policy:3844) waiting room policy test's total_active_usr changed from 1 to 100. Force eligible slots reallocation
[cmdb-module]: (reload_waiting_room_policy:3862) read db to get global wr state for policy FWB_CA_Policy, adom_id = 1, ret = -1

FortiWeb #
FortiWeb #

```

- diagnose debug proxy thread-wr 7  
This command shows the debug information for waiting room thread.



2) The Session Key configured in offline profile (if not configured, ASPSESSIONID, PHPSESSIONID, or JSESSIONID) must be used in HTTP.

## Why doesn't a WAF protection module work?

Some modules can disable other modules, such as URL access. When a certain module does not work, we should think about this. Here are some examples.

1) When URL access action is Pass, it can disable all security features after Global Object White List & URL Access, please refer to the module sequence in the following FAQ item.

2) IP white list can disable all security features after IP List Check.

3) When matched known engine, WAF will disable some RBE related features and all modules that may cause false positives. These modules are listed as follows

- HTTP Flood

- HTTP Access Limit

- Custom Access Policy

- GEO IP

- Malicious IP

- HTTP\_Protocol Constraints

- Robot Check

- Bot Deception

- Biometrics Based Detection

- Threshold Based Detection

4) Some OWA URLs will result in errors, so FortiWeb will disable these modules below.

- All response followup modules are disabled

- File Security

- Webshell Detection

- Chunk Decode

- File Uncompress

- Signature

- URL Rewriting

- File Compress

- Machine Learning

## What's the sequence of WAF module scans in 7.0.0?

The WAF module scan sequence in 7.0.0 is shown as below for your reference:

WAF\_X\_FORWARD\_FOR,

```
WAF_SESSION_MANAGEMENT, //Client management
WAF_IP_LIST_CHECK,
WAF_IP_INTELLIGENCE,
WAF_QUARANT_IP,
WAF_BOT_MITIGATION_MOD,
WAF_BOT_MANAGEMENT,
WAF_GEO_BLOCK_LIST,
WAF_HTTP_WEBSOCKET_SECURITY,
WAF_HSTS_HEADER,
WAF_PROTECTED_SERVER_CHECK,
WAF_ALLOW_METHOD_CHECK,
WAF_ACTIVE_SCRIPT,
WAF_MOBILE_IDENTIFICATION,
WAF_HTTP_DOS_HTTP_FLOOD,
WAF_HTTP_DOS_MALICIOUS_IP,
WAF_HTTP_ACCESS_LIMIT,
WAF_TCP_FLOOD_PREVENTION,
WAF_HTTP_AUTHENTICATION,
WAF_GLOBAL_WHITE_LIST,
WAF_ADFS_PROXY,
WAF_CUSTOM_RESPONSE_POLICY,
WAF_URL_ACCESS_POLICY,
WAF_MOBILE_API_PROTECTION,
WAF_PADDING_ORACLE_POLICY,
WAF_HTTP_PROTOCOL_CONSTRAINS,
WAF_FILE_PARSE,
WAF_FILE_UPLOAD,
WAF_WEBSHELL_DETECTION,
WAF_CHUNK_DECODE,
WAF_FILE_UNCOMPRESS,
WAF_WEB_CACHE, // NOTE: it has to be placed before the modules which will modify the original packs
WAF_BOT_DECEPTION,
WAF_ROBOT_CHECK, // ML bot detection
WAF_CSRF_CHECK,
```

```
WAF_MITB_CHECK,  
WAF_PARAMETER_VALIDATION_RULE,  
WAF_AJAX_BLOCK,  
WAF_BOT_CLIENT, // Biometric based bot detection  
WAF_WEB_ACCELERATION,  
WAF_XML_VALIDATION,  
WAF_JSON_VALIDATION,  
WAF_SERVER_PROTECTION_RULE, // Signature  
WAF_SYNTAX_BASED_DETECTION,  
WAF_SITE_PUBLISH,  
WAF_THREAT_WEIGHT,  
WAF_HIDDEN_FIELDS,  
WAF_CUSTOM_ACCESS_POLICY,  
WAF_BOT_CUSTOM_ACCESS, // Threshold based bot detection  
WAF_USER_TRACKING,  
WAF_API_MANAGEMENT,  
WAF_OPENAPI_VALIDATION,  
WAF_CORS_CHECK,  
WAF_URL_REWRITING_POLICY,  
WAF_URL_ENCRYPTION,  
WAF_MLEARNING, // Machine Learning framework  
WAF_API_RECORD, // Machine Learning API discovery  
WAF_FILE_COMPRESS,  
WAF_COOKIE_SECURITY,  
WAF_HTTP_HEADER_SECURITY,  
WAF_PROFILE,  
WAF_HTTP_STATISTIC,  
WAF_CLIENT_CERTIFICATE_FORWARD
```

### How does Web Protection modules support **Transfer-Encoding: chunked**?

With chunked transfer encoding, the HTTP server sends data to the receiver in a series of chunks instead of waiting until the complete segment is available. This is important especially when fetching dynamic content with unknown content length.

Some web protection modules support handling chunked data in HTTP response, but the behavior is different between 7.0.2 and previous builds.

On 7.0.1 and previous builds, there is an option `set chunk decoding enable/disable` for each server policy.

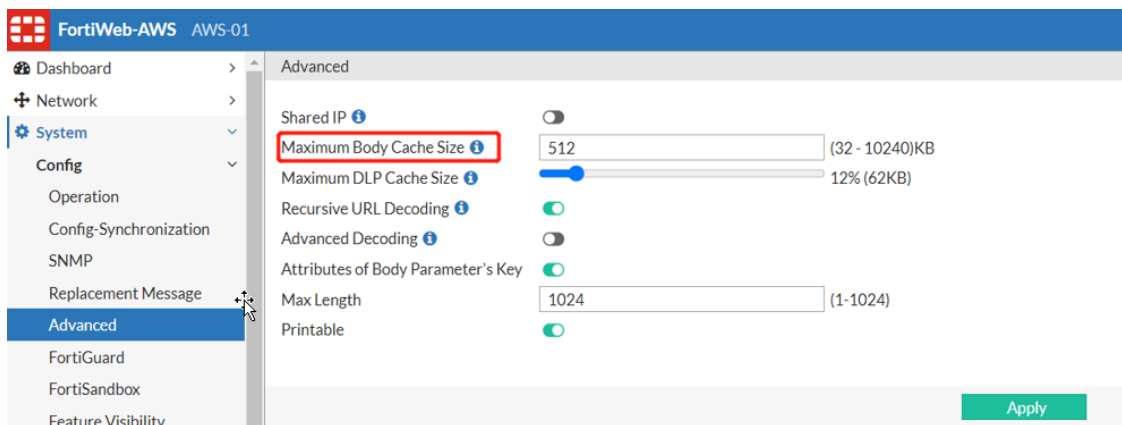
- It's enabled by default. FortiWeb will decode all the chunked responses, and convert it to body with a Content-Length header. In certain cases such as legacy clients only accept chunked responses, the clients will fail to process the response.
- If chunk decoding is disabled, the critical WAF modules that depend on the chunk decoded data will not be able to work.

From 7.0.2, FortiWeb replaced `set chunk decoding enable/disable` with `set chunk encoding disable/enable`.

- The default configuration is disabled, which equals to `set chunk decoding enable` in 7.0.1; FortiWeb will decode chunked response and convert it with Content-Length.
- When configured as `set chunk encoding enable` on 7.0.2, FortiWeb decodes and reassembles the chunked response, performs the WAF modules' operations, and encodes the new content with chunked again, then sends it to the clients.

From 7.0.2, when `set chunk encoding enable`, instead of delaying sending packets to the client until all content is available, the server will:

- Send the response in chunks.
- Add a `Transfer-Encoding: chunked` header to the chunks.
- Apply markers within the content to indicate the length of each chunk and whether that particular chunk is the last chunk that the server is sending.
- Under some conditions, chunk decoding module will not take action:
  - No web protection profile is bound to a server policy;
  - No modules enabled in a web protection profile;
  - Modules that depend on chunk decoded data are not enabled in web protection profile (e.g. compress, xml validation);
  - When chunked response size exceeds `max-cache-size`, FortiWeb will not decode chunked content.



For purpose of troubleshooting chunk decoding/encoding issues, you can enable the diagnose log as below:

```
diagnose debug flow filter module-detail chunk-decode-encode 7
diagnose debug enable
```

These are the web protection that depend on chunk decoding/encoding:

- WAF\_AJAX\_BLOCK
- WAF\_XML\_VALIDATION
- WAF\_WEB\_ACCELERATION
- WAF\_ROBOT\_CHECK
- WAF\_MLEARNING
- WAF\_HIDDEN\_FIELDS
- WAF\_API\_RECORD
- WAF\_USER\_TRACKING
- WAF\_FILE\_COMPRESS
- WAF\_FILE\_UNCOMPRESS
- WAF\_URL\_ENCRYPTION
- WAF\_LINK\_CLOAKING
- WAF\_URL\_REWRITING\_POLICY
- WAF\_CSRF\_CHECK
- WAF\_SERVER\_PROTECTION\_RULE
- WAF\_BOT\_DECEPTION
- WAF\_BOT\_CLIENT
- WAF\_MITB\_CHECK

### How does Cookie Security work when persistence types that may change cookies are used in Server Pool?

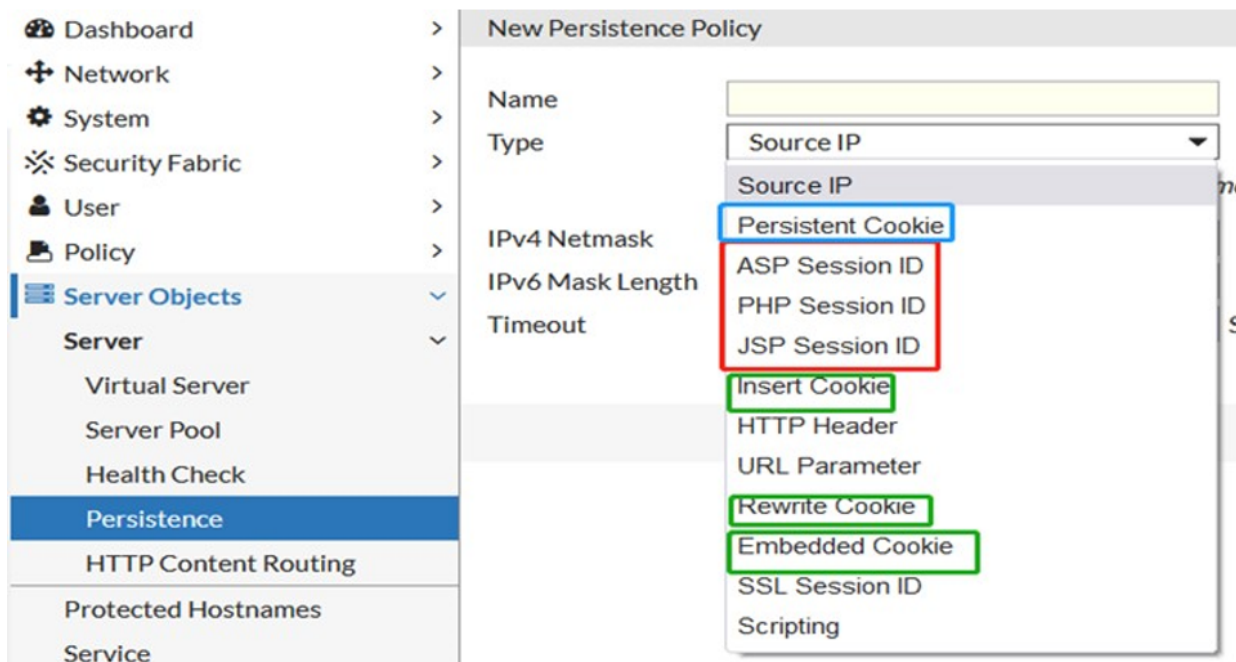
If both Cookie Security policy and cookie related Persistence types are enabled in one server-policy, there might be conflicts when both modules are trying to change the cookie values. The Cookie Security module will not handle cookies in some situations to avoid such conflicts.

With Persistence Types as below on 7.0.1 and earlier builds:

- PHP Session ID, ASP Session ID, JSP Session ID: Cookie Security handling will be bypassed;
- Insert Cookie/Rewrite Cookie/Embedded Cookie: Cookie Security handling will be bypassed;
- Persistent Cookie: Cookie Security check/set works

With Persistence Types as below on 7.0.2 and later builds:

- PHP Session ID, ASP Session ID, JSP Session ID: Cookie Security check/set works;
- Insert Cookie/Rewrite Cookie/Embedded Cookie: Cookie Security handling will be bypassed; (the same as before)
- Persistent Cookie: Cookie Security check/set works (the same as before)



When the behavior is different from your expectation, you can enable diagnose commands as below for troubleshooting:

```
# diagnose debug flow filter module-detail cookie-security 7
# diagnose debug proxy svr-balance 7
```

## Web Protection - Known Attack

- How do I create a custom signature that erases response packet content?
- What ID numbers do I use to specify a Signature Violation filter when I use the CLI to create a custom access rule?
- How do I reduce false positives and false negatives?

## FAQ

### How do I create a custom signature that erases response packet content?

For 6.4.0 and later releases, we don't recommend to use custom signatures to modify packets because signature is designed to detect malicious patterns instead of changing packet, and the erasing action of signature is actually masking, not deleting.

Please use "URL rewrite" to delete response header or mask response body for any releases after 6.4.0. Please refer to FortiWeb Administration Guide > Application Delivery > Rewriting & Redirecting for details.

For releases before 6.4.0, do the following.

1. Create a custom signature rule that includes the following values:

Direction	Response
<b>Expression</b>	Either a simple string or a regular expression that matches the response to erase.
<b>Action</b>	<b>Alert &amp; Erase</b> The erase action replaces the content specified by Expression with xxx.

2. Add an appropriate target:

- RESPONSE\_BODY
- RESPONSE\_HEADER
- RESPONSE\_STATUS

The RESPONSE\_STATUS is not erased in the raw packet.

If the target is RESPONSE\_HEADER or RESPONSE\_STATUS, the body of the response is still displayed.

3. Add the rule to a custom signature group, and then add the group to a signature policy that you can add to an inline or Offline Protection profile.

For detailed custom signature creation instructions, see "Defining custom data leak & attack signatures" in FortiWeb Administration Guide.

## What ID numbers do I use to specify a Signature Violation filter when I use the CLI to create a custom access rule?

The `waf custom-access rule` command allows you to configure custom access rules, which can include Signature Violation filters. When you configure the `signature-class` option, use one of the following IDs to specify the category of signature to match:

<b>Cross Site Scripting</b>	01000000
<b>Cross Site Scripting (Extended)</b>	02000000
<b>SQL Injection</b>	03000000
<b>SQL Injection (Extended)</b>	04000000
<b>Generic Attacks</b>	05000000
<b>Generic Attacks (Extended)</b>	06000000
<b>Known Exploits</b>	09000000

For example, the following command creates a custom rule that detects SQL injection attacks, such as blind SQL injection:

```
config waf custom-access rule
  edit "sql-inject"
    set action block-period
    set severity High
    set trigger "notification-servers1"
  config signature-class
    edit 03000000
      set status enable
```

```
        next
      end
    next
  end
  config waf custom-access policy
    edit "sql-inject-policy"
      config rule
        edit 1
          set rule-name "sql-inject"
        next
      end
    next
  end
end
```

For more information on the `waf custom-access rule` command, see the *FortiWeb CLI Reference*:

<https://docs.fortinet.com/product/fortiweb/>

## How do I reduce false positives and false negatives?

If FortiWeb is identifying legitimate requests as attacks (false positives), complete the following troubleshooting steps:

1. If your web protection profile uses a signature policy in which the extended version of a signature set is enabled (for example, **Cross Site Scripting** in FortiWeb Administration Guide), disable it.  
The extended signature sets detect a wider range of attacks but are also more likely to generate false positives.  
For details, see "Blocking known attacks & data leaks" in FortiWeb Administration Guide.
2. Specify the appropriate URL as an exception in the signature configuration. To create this exception, click either the **Exception** link in the **Message** field of the attack log item or **Advanced Mode** in the **Edit Signature Policy** dialog box.  
For details, see "Configuring action overrides or exceptions to data leak & attack detection signatures" in FortiWeb Administration Guide.
3. If the configuration changes do not solve the problem, capture the packet that FortiWeb has incorrectly identified as an attack and contact Fortinet Technical Support for assistance.  
Fortinet can resolve the issue by modifying the attack signature.

If FortiWeb is identifying attacks as legitimate requests (false negatives), complete the following troubleshooting steps:

1. Use the **Advanced Mode** option to ensure that the signature policy that your web protection profile uses has the following configuration:
  - All the appropriate signatures are enabled.
  - The enabled signatures do not have exceptions that permit the attack packets.
2. If your signature configuration is correct, capture the packet that FortiWeb did not identify as an attack and contact Fortinet Technical Support for assistance.  
Fortinet can resolve the issue by adding an attack signature. In the meantime, you can resolve the problem by creating a custom signature. For details, see "Defining custom data leak & attack signatures" in FortiWeb Administration Guide.

For additional information about reducing false positives, see "Reducing false positives" in FortiWeb Administration Guide.

## Can signature attack be detected in WebSocket traffic?

When **Web Protection > Protocol > WebSocket > Enable Attack signature** is enabled, attack signatures in WebSocket message body can be detected.

But if WebSocket traffic has extension header and the extension header is allowed in WebSocket security rule, FortiWeb does not promise to detect attack signatures.

When you select the WebSocket Security policy in **Policy > Web Protection Profile > Protocol**, do select the signature in **Known Attacks > Signatures**.

From 7.0.2 and newer builds, signature attacks can be detected when websocket data is masked or compressed.

## Can signature attack be detected in gRPC traffic?

- Signature in Request Header  
For signatures selected in Web Protection Profile, they can be detected in gRPC request header.
- Signature in Request Body  
When **Web Protection > Protocol > gRPC > gRPC Security Policy > Enable Attack signature** is enabled, and **Host, Request URL, IDL File, Request Message Name, and Response Message Name** are set correctly in **Web Protection > Protocol > gRPC > gRPC Security Rule**, attack signatures in gRPC message can be detected. The Request Rate Limit and Request Size Limit can also be scanned.

There are some debug commands to check the debug info.

```
diagnose debug flow filter module-detail grpc-security 7
diagnose debug flow trace start
diagnose debug enable
```

The Host and URL info in debug:

```
[work 1][flow] ssn 13 policy grpc strm 0 dir 0 subclient 0 client http get sub stream[0], version:2, substream count:2
[gRPC Security][Info]: (./waf_module/grpc_security.c:686): Process in Request.
[gRPC Security][Info]: (./waf_module/grpc_security.c:406): Current URL: [/routeguide.RouteGuide/RouteChat], HOST: [grpc.fwbqa:40051]
[gRPC Security][Info]: (./waf_module/grpc_security.c:410): Rule URL: [/routeguide.RouteGuide/RouteChat], HOST: [1][grpc.fwbqa:40051]
```

The message decoded in debug:

```
[gRPC Security][Info]: (./waf_module/grpc_security.c:686): Process in Request.
[gRPC Security][Debug]: (./waf_module/grpc_security.c:655): print decoded enable
[gRPC Security][Debug]: (./waf_module/grpc_security.c:665): Decoded:
{
  message = First message 001 The xx credit card number is [4096688354171422]
}
```

Attack Logs in gRPC request header, request body, and response body.

Main Type	Signature Detection
Sub Type	Generic Attacks(Extended)
Signature Subclass Type	Command Injection
Signature ID	060050030
Message	HTTP Header(cmd.exe) triggered signature ID 060050030 of Signatures policy aaa

Main Type	Signature Detection
Sub Type	Generic Attacks
Signature Subclass Type	Command Injection
Signature ID	050050030
Message	GRPC Request Body triggered signature ID 050050030 of Signatures policy aaa

Main Type	Signature Detection
Sub Type	Personally Identifiable Information
Signature Subclass Type	Credit Card Number
Signature ID	100010001
Message	GRPC Response Body triggered signature ID 100010001 of Signatures policy aaa

## Web Protection - Advanced Protection

---

### FAQ

#### Why does my Advanced Protection rule that has both Signature Violation and HTTP Response Code filters not detect any violations?

When you use **Web Protection > Advanced Protection > Custom Policy > the Custom Rule tab** to create a custom rule, FortiWeb links items in the list of filters with an AND operator. It uses the rule to evaluate both requests and responses. When the rule has both a Signature Violation and a HTTP Response Code filter, a malicious request violates the signature filter and the corresponding response matches the response code filter. But neither the request nor the response can violate both filters at the same time to generate a match.

To solve this problem, create a separate custom rule for each type of filter. For details, see "Combination access control & rate limiting" in FortiWeb Administration Guide.

#### What's the difference between the Packet Interval Timeout and Transaction Timeout filters in an Advanced Protection rule?

Both Packet Interval Timeout and Transaction Timeout protect against DoS attacks. In most cases, the attacks are some form of slow HTTP attack.

Packet Interval Timeout evaluates the time period between packets that arrive from either the client or server (request or response packets). If the time exceeds the maximum the timeout specifies, FortiWeb takes the action specified in the rule.

However, other types of slow attacks can keep the server occupied and still maintain a minimal data flow. For example, if an attack sends a byte of data per second, it can continue a GET request indefinitely but stay within the Packet Interval Timeout.

The Transaction Timeout evaluates the time period for a transaction—a GET or POST request and its complete reply. In most cases, a transaction lasts no longer than a few milliseconds or, for slower applications, a few seconds.

To detect the widest range of attacks, specify both Packet Interval Timeout and Transaction Timeout filters when you create an Advanced Protection rule.

For details, see "Combination access control & rate limiting" in FortiWeb Administration Guide.

## Why is the Signature Violation filter I added to my Advanced Protection custom rule not working?

To add a Signature Violation filter to an Advanced Protection custom rule, you select **Signature Violation** as the filter type.

However, for the filter to work, the following configuration steps are also required:

- In the Edit Custom Rule dialog box, select at least one signature category. By default, no categories are selected. When you select a category, FortiWeb prompts you to enable all or some of the signatures in the category.
- Ensure that the signatures that correspond to the categories you selected in the rule are enabled in the signature policy (**Web Protection > Known Attacks > Signatures**).

You select the custom policy that contains the rule and corresponding signature set when you create a protection profile.

For details, see "Combination access control & rate limiting" and "Blocking known attacks & data leaks" in FortiWeb Administration Guide.

## How do I prevent cross-site request forgery (CSRF or XSRF) with a custom rule?

A cross-site request forgery attack takes advantage of the trust that a site has in a client's browser to execute unwanted actions on a web application.

You can add CSRF protection rules or combine it with other methods to protect CSRF/XSRF attacks:

### To create a CSRF protection rule to protect against CSRF/XSRF attack. (Recommended)

1. Enable the attribute "Same Site" in Cookie Security. This attribute will declare that your cookie should be restricted to a first-party or same-site context.
2. Check "Referer" in custom rule.

**Note:** The first method (adding CSRF protection rule) is the most effective. Adding a custom rule with "Referer" header to detect CSRF is very ineffective and can be bypassed easily. However, if needed you can combine two or all of the methods.

### To add an advanced access control rule that detects cross-site request forgery (CSRF)

1. Go to **Web Protection > Advanced Protection > Custom Policy**, and select the **Custom Rule** tab.
2. Click **Create New**.

3. Configure the action and trigger settings for the rule.  
For detailed information on these settings, see "Combination access control & rate limiting" in FortiWeb Administration Guide.
4. Click **Create New** to add a rule entry.
5. For **Filter Type**, select **HTTP Header**, and then click **OK**.
6. Configure these settings:

<b>Header Name</b>	<b>Referer</b>
<b>Header Value Type</b>	<b>Regular Expression</b>
<b>Header Value</b>	A regular expression that matches the address of your website. For example, if your website is http://211.24.155.103/, use the following expression: <code>^http://211\24\155\103.*</code>

7. Click **OK** to save the rule entry, and then click **OK** to save the rule.
8. Go to **Web Protection > Advanced Protection > Custom Policy**, and select the **Custom Policy** tab to group the custom rule into a policy.  
For details about creating policies, see "Combination access control & rate limiting" in FortiWeb Administration Guide.
9. To apply the policy, select it as the **Custom Policy** in a protection profile. For details, see "Configuring a protection profile for inline topologies" or "Configuring a protection profile for an out-of-band topology or asynchronous mode of operation" in FortiWeb Administration Guide.  
Attack log messages contain `Custom Access Violation` when this feature detects an unauthorized access attempt.

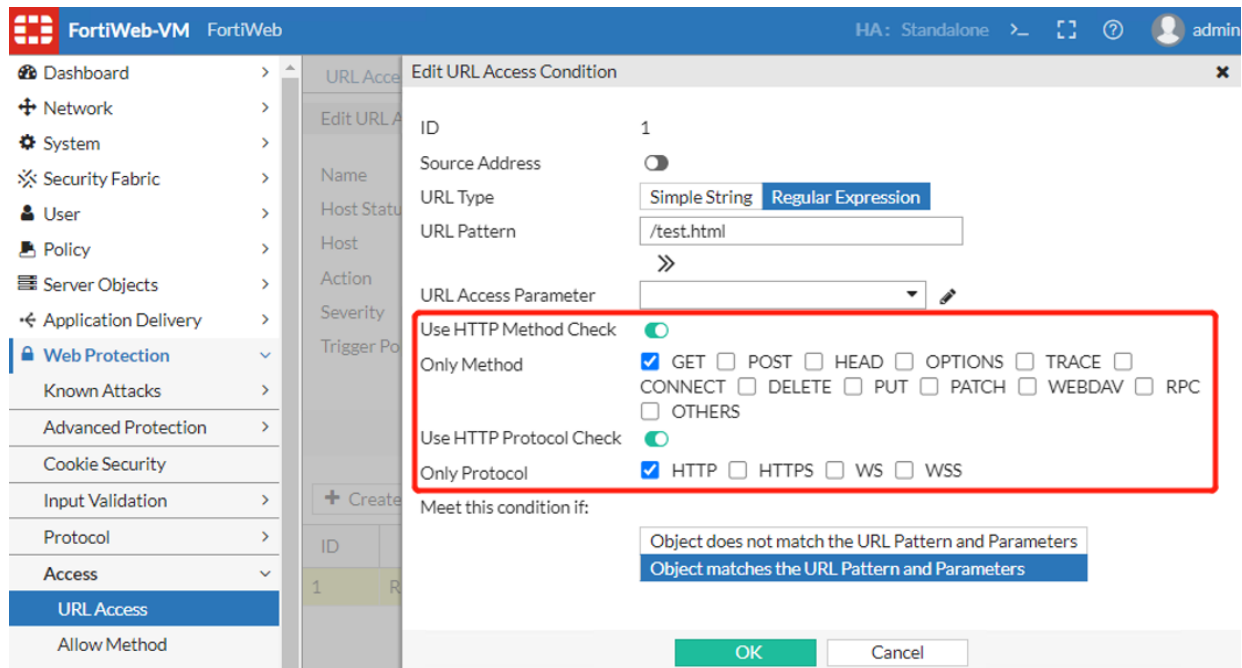
## Why a URL access rule doesn't work?

Please check:

- 1) The URL Pattern value in a URL access rule shouldn't include the parameter part. That is to say that the value here only matches against the URL string before the question mark.
- 2) URL access rules may be skipped by previous rule if previous rule has been matched because all of the rules are checked by their sequences.

## Does a URL access rule support matching specific HTTP methods or HTTP protocols?

From 7.0.2, you can specify the HTTP methods and HTTP protocols when defining a URL access rule. Only that requests matching the enabled methods or protocols will continue with URL Pattern check.



## Why are requests still forwarded to backend servers when the client IP has been already blocked?

Please check:

- 1) Period block IP only works on new TCP connections. If there are requests on the old TCP connection which was established before the IP be blocked, the request on the old TCP connection will still be forwarded.
- 2) Customers can choose Client ID based period block for images after 7.0.0. This kind of period block will drop the requests on the old TCP connection.

## Why does the reCAPTCHA verification fail even though the custom rule settings are correct and the request is legitimate?

The reCAPTCHA verification fails even though the client is legitimate and required verifications are done within the Validation Timeout period (**Bot Confirmation** settings in **Web Protection > Advanced Protection > Custom Policy > Custom Rule**).

This may be caused by a change of reCAPTCHA verification API. FortiWeb sends API calls to a Google reCAPTCHA service URL to complete the reCAPTCHA verification. Google recently changed this URL to <https://www.google.com/recaptcha/api/siteverify>.

To verify if FortiWeb is configured with this latest URL, run `diagnose debug flow filter module-detail recaptcha 7`. The output should be as follows:

```
[reCAPTCHA] [DBG] (./waf_module/recaptcha.c:678): recaptcha_api_
url:https://www.google.com/recaptcha/api/siteverify, recaptcha_api_timeout:10
```

If the URL is not right, run the following to change it:

```
config system recaptcha-api
set url https://www.google.com/recaptcha/api/siteverify
```

end

Please note this URL is subject to change by Google. Please refer to [https://developers.google.com/recaptcha/docs/verify#api\\_request](https://developers.google.com/recaptcha/docs/verify#api_request) for the latest URL and make sure FortiWeb is configured with the latest URL.

This issue may occur in other WAF modules integrated with reCAPTCHA verification, including:

- HTTP Flood Prevention
- HTTP Access Limit
- Threshold Based Detection
- ML Based Bot Detection

## Which modules support Client ID based period block and which modules do not support?

The modules below support Client ID based period block from 7.0.0:

- HTTP-request-flood-prevention-rule
- user-tracking rule
- xml-validation rule
- json-validation rule
- openapi-validation-policy
- csrf-protection
- bot-deception
- input-rule
- custom-protection-rule
- signature
- api-rules
- syntax-based-attack-detection
- HTTP-protocol-parameter-restriction
- webshell-detection-policy
- file-upload-restriction-policy
- threshold-based-detection policy
- custom-access rule
- cookie-security
- site-publish-helper policy
- mobile-api-protection mobile-api-protection-rule
- url-encryption url-encryption-rule
- bot-detection-policy
- known-bots – only bad bot need support

These modules do not support Client ID based period block from 7.0.0:

- padding-oracle - IP-based statistics
- layer4-access-limit-rule - IP-based statistics
- layer4-connection-flood-check-rule – IP-based statistics
- ip-intelligence – IP-based only

- machine-learning-policy
- HTTP-connection-flood-check-rule – IP based
- ftp-file-security
- ftp-command-restriction-rule

## Why doesn't MITB work?

Please check:

- 1) Make sure the request URL matches that rule and the response page is in HTML format with status code 200.
- 2) Make sure there's a form tag in the response HTML page and the form's action URL matches the POST URL in MITB rule.
- 3) Make sure the type of password input tag is "password" indeed, or FortiWeb's MITB script can't locate the password.
- 4) Make sure the value of the Content Security Policy header doesn't block the execution of FortiWeb's MITB script.

## Why does WSDL import fail?

Below are several common non-bug reasons:

- 1) When WSDL imports a local schema, the schema should be uploaded to FortiWeb first.
- 2) When WSDL imports a schema from network, FortiWeb should be able to access the network.
- 3) If the GUI alerts that the WSDL format is incorrect, you should correct the format before uploading. There is a website for verifying the WSDL format:

<https://www.wsdl-analyzer.com/>

- 4) The max import/include schema level is limited to 256.

Also, you can see the specific error information returned by the GUI.

## Why doesn't WSDL Validation work?

There are often similar questions caused by incorrect configuration. For WSDL validation, the configurations should be the same between WSDL and the device.

- 1) The request url of the XML protection rule should be the same as the url of WSDL location.
- 2) The backend IP/domain of the device should be the same with the IP/domain of WSDL location.
- 3) The backend port of the device should be the same with the port of WSDL location.

The above three points can confirm the only service on the network.

## Web Protection - Input Validation

- [Why sometimes fail to upload files to the server when file security is enabled? on page 168](#)
- [Why does file security not work? on page 168](#)
- [Why does the server receive packets from the client even if parameter validation deny is triggered? on page 168](#)
- [Why isn't the 'Whole Suffix Files' file type check working as expected? on page 168](#)

### FAQ

#### Why sometimes fail to upload files to the server when file security is enabled?

Check if 'Hold Session While Scanning File' is enabled first. When it is enabled, FortiWeb will upload files to FortiSandbox and wait for scan results before sending the file to the server. This process may take some time, please check if the server will disconnect while waiting.

#### Why does file security not work?

FortiWeb parses files up to 5M by default, and if it exceeds 5M, the requests will be bypassed.

If you want to increase this value, please configure it as below.

```
config system antivirus
set uncomp-size-limit 102400
end
```

#### Why does the server receive packets from the client even if parameter validation deny is triggered?

When a HTTP request is divided into multiple TCP packets, before the packet which includes the denied parameter appears, the previous TCP packets will still be transmitted to the server.

#### Why isn't the 'Whole Suffix Files' file type check working as expected?

The "Whole Suffix Files" feature is designed to verify file extensions. A file is recognized as a match if its extension corresponds to the file type specified in the "Whole Suffix Files" settings.

However, hackers can manipulate this by forcibly altering the file extension, such as changing "abc.pdf" to "abc.txt". To effectively block PDF files disguised with a .txt extension, you should configure the settings to inspect the file content. This is done by selecting "Text Files" and then specifying "PDF" within that category. The "Text Files" setting examines the actual payload of the file to determine its true type.

## Web Protection - Bot Mitigation

- [Why can't I see the bot\\_client.js be injected into the response page for Biometric Based Detection?](#) on page 169

### FAQ

#### Why can't I see the bot\_client.js be injected into the response page for Biometric Based Detection?

Please check from two aspects:

- 1) Double check if the request matches the rule or not.
- 2) Be aware that if the client is considered as not a bot, its good client status will be kept for 30 minutes. So FortiWeb won't do biometric based checking to this client within 30 minutes.

#### How are Known Bots > Known Search Engines being matched?

On 7.0.1 and previous builds, Known Search Engine is only determined by matching IP address of HTTP requests with predefined IP ranges. In this way, it's prone to trigger false negatives and false positives.

On 7.0.2, Known Search Engine is determined by a mixed of conditions:

- The first 24-bits of source IP or XFF IP checking.  
E.g. if the IP range is 104.250.147.218 to 104.250.147.219, then the condition will be matched if the source IP in the request is within 104.250.147.1 and 104.250.147.255.
- The header field "User Agent" checking.
- All IP checking and User Agent checking can have mix matching known engines.

E.g, if a request IP belongs to Google bots and the User Agent belongs to Bing, then this request will still be matched.

The predefined Known\_engine data including User Agents and IP Ranges are defined in /data/etc/known\_engines.xml, which will be updated as a part of the signature update with FDS versions.

Taking an item from /data/etc/known\_engines.xml for example, a request sent by curl as below will match the Known Bots Engines:

```
curl -ikv -H "X-Forwarded-For: 104.250.147.100" -A "Gigabot/"  
https://www.example.com/test.html
```

**Notes:** In this test, an X-Forwarded-For rule with **Use X-Header to Identify Original Client's IP and Block Using Original Client's IP** is linked to the web protection profile for the server policy.

```
<item id="0006" name="Gigablast">  
<ip_range id="1">  
<ip_start>104.250.147.218</ip_start>  
<ip_end>104.250.147.218</ip_end>  
</ip_range>  
...  
...  
<advanced id="none">
```

```

<user_agents>
<!-- cases
Gigabot/2.0att
Gigabot/2.0 (gigablast.com)
Gigabot/2.0/gigablast.com/spider.html
Gigabot/2.0; http://www.gigablast.com/spider.html
Gigabot/3.0 (http://www.gigablast.com/spider.html)
GigabotSiteSearch/2.0 (sitesearch.gigablast.com)
-->
<pattern value="Gigabot/" />
<pattern value="GigabotSiteSearch/" />
</user_agents>
</advanced>
</item>

```

Use the following troubleshooting methods when a request is not matched by the Known Search Engines:

**1. Enable diagnose log to check the processing details:**

```

diagnose debug flow filter module-detail known-bots 7
diagnose debug enable

```

**E.g. a sample output of matching case:**

```

[Known Bots][DEBUG](bot_management_module_process-880): inside bot management
process.
[Known Bots][DEBUG](check_ip_in_ke-271): inside check ip in ke.
[Known Bots][DEBUG](check_ip_in_ke-316): found IP match: id and name : 0006
Gigablast
[Known Bots][DEBUG](check_ip_in_ke-346): found UA match: unit->name : Gigablast
[Known Bots][INFO](check_ip_in_ke-360): match benign bots (1, 0006) and make
action.
[Known Bots][INFO](bot_management_make_action-80): inside make bm make action
[Known Bots][INFO](http_statistic-147): Direction is client to server and first
packet, do hit-count statistic.
[Known Bots][INFO](http_statistic-154): Direction is client to server and first
packet, do known engines, bad bots and regular statistic.

```

**2. Check if the source IP (or XFF IP) or the User Agent in HTTP header is included in /data/etc/known\_engines.xml.**

## Web Protection - API Protection

- Why do I get an error message “Not a valid YAML file for OpenAPI” while uploading a valid YAML file on the “OpenAPI file” page? on page 170

## FAQ

### Why do I get an error message “Not a valid YAML file for OpenAPI” while uploading a valid YAML file on the “OpenAPI file” page?

An OpenAPI document may be represented either in JSON or YAML format. FortiWeb only supports OpenAPI files written in YAML format. A valid OpenAPI document not only conforms to YAML syntax but also to the

OpenAPI Specification. You can utilize Swagger Editor to validate your OpenAPI document online/offline: <https://swagger.io/docs/open-source-tools/swagger-editor/> for more details.

## Web Protection - IP Protection

- [Why do I get an error message “Not a valid YAML file for OpenAPI” while uploading a valid YAML file on the “OpenAPI file” page? on page 170](#)
- [How to troubleshoot GEO IP false positives/false negatives? on page 171](#)
- [Why are GEO-IP locations different from FortiGuard? on page 171](#)

## FAQ

### How to troubleshoot IP Reputation false positives/false negatives?

We generally follow below process to troubleshoot:

- 1) Check if the IP reputation database (IRDB) is upgraded to the latest.

Please check via **System > Config > FortiGuard > License information > IP Reputation**.

- 2) If the IRDB is the latest, use below shell cmd on FortiWeb to check if the IP could match the IRDB on the device.

```
FortiWeb # fn sh
~# bonet_test /var/log/irdb_sig.db 1.1.1.1
ip count = 139727, all types[botnetv1|botnet|proxy|phishing|spam|tor|others]
CategoryIdName 1 Botnet
CategoryIdName 2 Anonymous Proxy
CategoryIdName 3 Phishing
CategoryIdName 4 Spam
CategoryIdName 5 Others
CategoryIdName 6 Tor
IP unmatched in irdb.
```

- 3) If the cmd shows unmatched, then FortiWeb needs to notify the IRDB team to check if this IP needs to be added to IRDB in the next version.

- 4) If the cmd shows matched, then maybe IRDB was disabled by other modules.

### How to troubleshoot GEO IP false positives/false negatives?

Follow below process to troubleshoot:

- 1) Check if the GEO DB is upgraded to the latest.

Please check via **System > Config > FortiGuard > License information > GEO DB**.

- 2) If GEO DB is upgraded to the latest, then FortiWeb needs to notify the GEODB team to check if this IP needs to be modified for the next GEODB release.

### Why are GEO-IP locations different from FortiGuard?

GEO-IP on FortiWeb is updated twice a month. However, FortiGuard is updated in real time.

### How does “Action” of an IP List policy work with the matching Types “Trust IP”, “Block IP” and “Allow Only”?

The “Action” of an IP List policy can be configured as “Deny (no log)”, “Block Period” or “Alert & Deny”.

There are three types of IP lists:

- **Block IP**—The source IP address that is distrusted, and is permanently blocked from accessing your web servers, even if it would normally pass all other scans.
- **Trust IP**—The source IP address is trusted and allowed to access your web servers, unless it fails a previous scan. For details, see "Sequence of scans" in FortiWeb Administration Guide.
- **Allow Only**—If the source IP address is in the Allow Only range, it will be passed to other scans to decide whether it's allowed to access your web servers. If not, FortiWeb will take actions according to the trigger policy.

If no Allow Only is configured, then the source IP addresses which are neither in the Block IP nor Trust IP list will be passed directly to other scans.

The Action works as below when different IP List types are configured:

- For Trust IP, the Action actually will NOT take effect for the IP addresses matched;
- For Block IP & Allow Only, the Action will take effect accordingly for the IP addresses matched.

## Machine Learning - Anomaly Detection

### FAQ

- [How to handle false positives for ML Based Anomaly Detection? on page 173](#)
- [Which content-types are supported by ML? on page 173](#)
- [Which charset are supported by ML? on page 173](#)
- [What are the major specification & limitation of machine learning - Anomaly Detection on page 174](#)
- [How to find out the SVM threat model database version? on page 175](#)
- [Why is machine learning anomaly case-sensitive with URL and parameter name? Can we turn it off? on page 175](#)
- [After how many minutes or hours the “unconfirmed” parameter will be discarded by the garbage collector? on page 176](#)
- [Is there a way to check how many samples are discarded due to ‘sample-limit-by-ip’ in the machine learning database? on page 176](#)
- [Is Sample Collection mode Extended removed in the 6.4 version? I don’t see it in GUI or CLI configuration on page 176](#)
- [The 6.3 option “dynamically update when parameters change is enabled” is no longer available in 6.4/7.0. Are there any mechanism changes? on page 176](#)
- [How does noisy samples impact machine learning function, and how to alleviate the impact? on page 177](#)

### Machine learning trouble-shooting

- [ML based Anomaly Detection does not learn parameters successfully on page 177](#)
- [ML based Anomaly Detection status does not change from Unconfirmed to Running stage on page 179](#)

- [ML based Anomaly Detection does not block traffic on page 179](#)
- [Machine Learning - Anomaly Detection upgrade&compatibility issues on page 180](#)

## FAQ

### How to handle false positives for ML Based Anomaly Detection?

There are two svm-types: standard and extended. If standard is selected, the system automatically disables the svm models which can easily trigger false positives. If extended is selected, the system enables all svm models.

So when you find unexpected false positives, please just leave svm-type as standard (By default).

### Which content-types are supported by ML?

Support list:

- multipart/related
- application/soap+xml
- text/xml, application/xml, application/vnd.syncml+xml, application/vnd.ms-sync.wbxml
- multipart/form-data
- text/html
- application/x-www-form-urlencoded
- text/plain
- multipart/x-mixed-replace
- application/rss+xml
- application/xhtml+xml
- application/json, text/json

Unsupported:

- message/HTTP
- application/rpc
- application/x-amf
- application/vnd.syncml+wbxml

### Which charset are supported by ML?

FortiWeb machine learning supports most of the popular character sets. You can check with CLI as below:

```
FortiWeb # config waf machine-learning-policy
FortiWeb (machine-learning) # edit 1
FortiWeb (1) # config allow-domain-name
FortiWeb (allow-domain-n~m) # edit 1
FortiWeb (1) # set character-set
AUTO                AUTO
BIG5                 BIG5
GB2312               GB2312
ISO-2022-JP          ISO-2022-JP
ISO-2022-JP-2       ISO-2022-JP-2
```

ISO-2022-KR	ISO-2022-KR
ISO-8859-1	ISO-8859-1
ISO-8859-2	ISO-8859-2
ISO-8859-3	ISO-8859-3
ISO-8859-4	ISO-8859-4
ISO-8859-5	ISO-8859-5
ISO-8859-6	ISO-8859-6
ISO-8859-7	ISO-8859-7
ISO-8859-8	ISO-8859-8
ISO-8859-9	ISO-8859-9
ISO-8859-10	ISO-8859-10
ISO-8859-15	ISO-8859-15
Shift-JIS	Shift-JIS
UTF-8	UTF-8

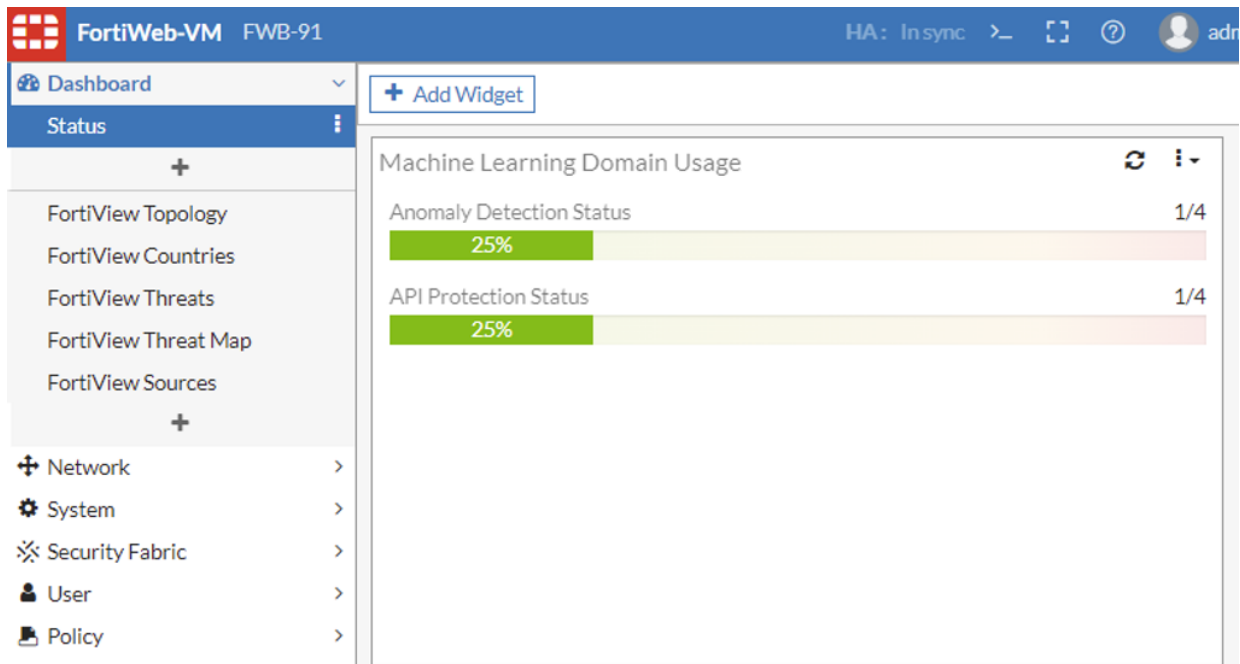
## What are the major specification & limitation of machine learning - Anomaly Detection

1. One server policy can only enable one machine learning policy;
2. One machine learning policy can create one or more domains; no matter how many machine learning policies are enabled;
3. One URL can learn maximum 128 parameters;
4. One domain can learn maximum 1000 parameters;
5. The maximum number of domains is listed as below.

These specs are the result of a comprehensive evaluation based on the memory of the platform. It cannot be changed easily, otherwise there will be a risk of insufficient memory, thereby may affect other normal business forwarding, and there is no workaround for now.

Platform	Domains in all ML policies
100D/100E	4
400C/400D/400E	6
600D/600E	16
1000D/1000E/3000D/3000DFsx/4000C	32
2000E/3000E/3010E/4000D	64
2000F/3000F	96
4000F	192
VM	
memory<=4G	4
memory<=8G	8
memory<=16G	16
memory>=16G	32

From 7.0.2, the maximum number of domains for Anomaly Detection & API Protection supported by different platforms can be seen via **Dashboard > Status > Add Widget > ML Domain Usage**.



## How to find out the SVM threat model database version?

You can see the version in 'diag sys update info'. SVM database is included in the general FortiWeb signature database:

```
FWB-AWS-M01 # diagnose system update info
FortiWeb signature
-----
Version: 0.00296
Expiry Date: Fri Aug 19 2022
Last Update Date: Thu Aug 19 14:00:09 2021
Next Update Date: Thu Aug 19 16:00:00 2021

Historical versions
-----
0.00271
```

## Why is machine learning anomaly case-sensitive with URL and parameter name? Can we turn it off?

Machine learning is case-sensitive with URL&parameter name, just because case-sensitive is by default in Linux systems.

No option to turn it off at present.

## After how many minutes or hours the “unconfirmed” parameter will be discarded by the garbage collector?

A parameter is in unconfirmed status initially, and it will be set to be Confirmed if the parameter is contained in the requests from a certain number of different source IPs within the given time. Otherwise, the parameter will be discarded.

`ip-expire-cnts` defines "the number of different source IPs", while the `ip-expire-intval` defines the given time period.

The valid range for `ip-expire-intval` is 1-24 in hours, and the default value is 4. The valid range for `ip-expire-cnts` is 1-5, and the default value is 3.

## Is there a way to check how many samples are discarded due to ‘sample-limit-by-ip’ in the machine learning database?

There is no way to check such statistics. Samples exceeding the threshold per 30 minutes will not be collected any more.

This is different from the “Collected Sample” displayed in the Tree View tab. “Collected Samples” means the “effective” samples. For example, when this number reaches 400, machine learning will start to build the initial mode; when it reaches 1200 and find there are a few patterns generated (the model is considered to be stable), machine learning switches to standard mode.

## Is Sample Collection mode Extended removed in the 6.4 version? I don’t see it in GUI or CLI configuration

Yes, options to configure `sample-collecting-mode` are removed from 6.4 GUI & CLI. You can think that the process is similar while some of the modes’ implementation have been changed and simplified – machine learning works in initial mode (like normal or fast mode as in 6.3) at first (when samples reaches the `start-min-count`, default 400), and will switch to standard mode with more effective samples (when the number of samples accumulates to `switch-min-count`, default 1200, and `switch-percent` is smaller than the value you set; please refer to the CLI guide for detailed description).

## The 6.3 option “dynamically update when parameters change is enabled” is no longer available in 6.4/7.0. Are there any mechanism changes?

6.4/7.0 machine learning uses different mechanisms to detect changes. The new refreshing mechanism uses a sliding window instead of boxplot to simplify ML.

Related CLI commands are as below; you can also check the detailed meaning in FortiWeb CLI Reference.

<code>sliding-win-time</code> <code>&lt;sliding-win-time_int&gt;</code>	<p>After the standard model is built, FortiWeb keeps updating it according to the newest samples so that the model can be up to date even when your domain changes, such as when new URLs are added and existing parameters provide new functions.</p> <p><code>sliding-win-time</code> defines how frequently FortiWeb updates the standard model.</p> <p>The valid range is 15-1440 in minutes.</p>	15 (minutes)
<code>sub-window-size</code> <code>&lt;sub-window-size_int&gt;</code>	<p>If there isn't any new pattern generalized during the <code>sliding-win-time</code>, the system will not update the standard model until the number of samples reaches the <code>sub-window-size</code>.</p> <p>The <code>sub-window-size</code> can be set as 50 or 100.</p>	50
<code>sub-window-count</code> <code>&lt;sub-window-count_int&gt;</code>	<p>Every time the standard model is updated, FortiWeb counts it as one <code>sub-window-count</code>. If a certain times of <code>sub-window-count</code> have passed and there isn't any sample coming in for a pattern, FortiWeb considers this pattern outdated, and will discard it.</p> <p>The <code>sub-window-count</code> can be set as 20, 40, or 80.</p> <p>For example, assuming the <code>sub-window-count</code> is 20, then FortiWeb will discard a pattern if there isn't any sample collected for it after the model has been updated for 20 times consecutively.</p>	40

## How does noisy samples impact machine learning function, and how to alleviate the impact?

If a string is learned during the collecting stage, it'll not be blocked in the running stage. That's the difference when using "cmd" and "mode".

Noisy samples can be detected during the sample collection period. Some samples can be treated as abnormal samples and excluded from the samples used to build the anomaly detection model. However, if such samples account for a large proportion, they'll usually not be detected as noise.

Another possible way to alleviate this problem is to enable signature profiles. Once a request is blocked by signature, it'll not be learned as a sample.

Below sections are troubleshooting methods for some typical issues.

## Machine learning trouble-shooting

### ML based Anomaly Detection does not learn parameters successfully

If there isn't any data shown in the Machine Learning - Anomaly Detection module, first run `grep ml` to confirm the issue. If `/bin/ml_init` is displayed in the printout, it means this module doesn't work at all. This results in no data shown.

The following reasons might cause this issue:

- Charset is not supported.
- Request or response packets are not valid.

#### Verifying the charset

Machine Learning - Anomaly Detection collect samples of a domain to learn its URLs and parameters including the parameter name and value. If the charset used by the domain can't be recognized by the ML based Anomaly

Detection module, it's impossible for it to parse the data properly. As a result, it can't build up a valid machine learning model.

The following charsets are supported:

BIG5; GB2312; ISO-2022-JP; ISO-2022-JP-2; ISO-2022-KR; ISO-8859-1; ISO-8859-2; ISO-8859-3; ISO-8859-4; ISO-8859-5; ISO-8859-6; ISO-8859-7; ISO-8859-8; ISO-8859-9; ISO-8859-10; ISO-8859-15; Shift-JIS; UTF-8;

FortiWeb identifies the charset defined in the `Content Type`: header of the response packets, for instance, `Content-Type:text/html; charset=xxx`. Charset can also be included in the HTTP response body as `<META ... charset=xxx">`.

- If the charset is supported, FortiWeb will continue the model building process.
- If there isn't any charset defined, FortiWeb will take it as UTF-8 and continue the model building process. On the Overview section, the Page Charset will be shown as Default.
- If the charset defined in `Content Type`: isn't one of the supported charset, the machine learning model can't be built.

### Verifying the request and response packets

The system checks the charset defined in the response packets, so the response packets should be valid at first:

- The response code must be 200 or 302;
- The maximum bytes buffered for HTTP response body is 2048; charset cannot be learnt if it's out of this range.

The request packet should have parameters in its URL or request body. Refer to the following examples.

- **Parameters in URL.** In this example, the parameter is `testargument=2000`.  
`http://www.testdomain.com/autotest/test.html?testargument=2000`
- **Parameters in the body.** In this example, the parameter is `myparameter=123`.  

```
POST /autotest/csh/mlarg3.php HTTP/1.1
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.12.2
Host: testmydomain
Cookie: cookiesession1=3473FD0DAS38CIHAIRSOZ3D9RDVTB577;
X-Forwarded-For: 2.2.2.2
Content-Length: 23
Content-Type: application/x-www-form-urlencoded
myparameter=123
```

The content-type of both the request body and response body should be one of the following:

- `multipart/related`
- `application/soap+xml`
- `text/xml`, `application/xml`, `application/vnd.syncml+xml`, `application/vnd.ms-sync.wbxml`
- `multipart/form-data`
- `text/html`
- `application/x-www-form-urlencoded`
- `text/plain`
- `multipart/x-mixed-replace`

- application/rss+xml
- application/xhtml+xml
- application/json, text/json

Content types such as message/HTTP, application/rpc, application/x-amf, and application/vnd.syncml+wbxml are not supported.

Run the following commands to get more debug info on ML based Anomaly Detection.

```
diagnose debug application machine-learning 7 or diagnose debug flow filter
module-detail anomaly-detection 7
```

```
diagnose debug enable
```

## ML based Anomaly Detection status does not change from Unconfirmed to Running stage

1. Check if the “Collected Samples” reaches 400 (the default start-min-count), which is the default number for an initial model to be built up;
2. Check if new requests meet the requirements of `ip-expire-intval` (1-24 hours) and `ip-expire-cnts` (source IPs).

You can set both value as 1 to make it easier for test.

3. Sending traffic from single source and multiple XFFs:

- Enable Inline Protection Profile and choose “Use X-Header to Identify Original Client's IP”.
- Need to use public IP addresses to test instead of private IPs.
- Sometimes you may use curl to verify the functionalities, however please note that the behavior of different curl versions may vary. It's better to double check the traffic/request actually sent out with packet capture or FortiWeb tlog.

E.g, with curl 7.68.0 on Ubuntu 20.0.4, the XFF IP 102.11.2.3 will be recognized as the “Original Source” in tlog with the 1st curl command as below. But on Win10 with curl 7.78.0, just the 1st curl command cannot be identified as the “Original Source”; the other 3 formatted commands will take effect and trigger the machine learning process.

```
curl http://direct.ama01.com/index.php?new_para=123 -H 'X-Forwarded-
For:102.11.2.3'
curl http://direct.ama01.com/index.php?new_para=123 -H "X-Forwarded-
For:102.11.2.3"
curl http://direct.ama01.com/index.php?new_para=123 -H X-Forwarded-For:102.11.2.3
curl http://direct.ama01.com/index.php?new_para=123 -H X-FORWARDED-FOR:102.11.2.3
```

## ML based Anomaly Detection does not block traffic

1. In **Web Protection > ML Based Anomaly Detection > Tree View**, click **Test Sample**, then enter a parameter value to verify whether it will be detected as an anomaly at the current strictness level.

Only if a parameter is recognized as an anomaly first by HMM model, it will be then sent to SVM model to double check if it's a real attack.

2. Check if FortiWeb works in Active-Active-Standard or Active-Active-High-Volume mode, which are not supported yet on 6.3 & 6.4.

This issue has been resolved on FortiWeb 7.0 and later releases.

## Machine Learning - Anomaly Detection upgrade&compatibility issues

FortiWeb 6.4 uses Redis while 6.3 uses MySQL. So after upgrading from 6.3 to 6.4, old machine learning data will be lost.

Upgrading from 6.3/6.4 to 7.0 is supported.

## ZTNA troubleshooting and debugging

### Common troubleshooting issues

As FortiWeb ZTNA solution is integrated with FortiWeb, FortiClient and FortiClient EMS, issue troubleshooting sometimes needs checking on all these three components.

There are several ways or steps for ZTNA related issues troubleshooting:

1. Check if FortiWeb is connected to EMS;
2. Check if Tags and endpoint client information are synchronized to FortiWeb:
  - Compare information between FortiWeb and EMS
  - Check Event logs to see configuration or EMS data sync failures
  - Check diagnose log or fcnacd.log
3. Check if the daemon fcnacd & fcsync are stable:
  - Check if pid changes
  - Check if there is any daemon coredump file under `/var/log/gui_upload`
4. If browsers do not prompt selecting client certificate:
  - Check on FortiClient endpoint to see if certificate is signed successfully
  - Check client certificate verification configuration on FortiWeb
5. If ZTNA rule/tag matching does not meet expectation:
  - If a visit is blocked, check Attack logs to see if any if it's caused by ZTNA violation;
  - Check ZTNA or HTTP content-routing related diagnose logs to see processing details
6. If the issue need further investigation, please collect below logs:
  - `/var/log/debug/fcnacd.log` and `/var/log/debug/fcsync_log`
  - Configuration file
  - Client information from "diagnose system endpoint-control clients"

ZTNA related diagnose logs:

```
# diagnose debug flow filter module-detail ztna 7 # available since 7.4.1
# diagnose debug flow trace start # available since 7.4.1
# diagnose debug proxy svr-balance 7
# diagnose debug proxy thread-ztna-sync 7
# diagnose debug timestamp enable
# diagnose debug enable
```

Currently FortiWeb does not have very rich ZTNA logs. Here we list the related Event/Attack/Traffic logs as below:

1. Event logs:
  - EMS/fctems configuration changes;
  - Tag sync > Add/delete tag configuration;
  - Sync data success/failure > caused by EMS connect/disconnect
2. Attack logs:
  - HTTP Connection Failure logs when client certificate verification failed
  - Zero Trust Access logs when traffic matches ZTNA rule with Action Alert\_Deny by ZTNA, or matches the default Action Alert\_Deny of ZTNA profile;
  - No attack logs when ZTNA rule/profile is matched and the Action is Accept or Deny (No log)
  - No attack logs when ZTNA tags are matched or not matched in HTTP content-routing policy
3. Traffic logs:
 

When ZTNA profile/rule is matched and the Action is Accept, there will be a traffic log, but currently no ZTNA information within it.

## FortiClient EMS connection issues

- Check the network and FortiClient EMS port accessibility on FortiWeb:
  - Ping the IP address or the Domain Name of the FortiClient EMS;
 

Note: only IPv4 & Domain Name are supported; IPv6 is not supported by FortiClient EMS
  - Use execute telnettest command to check if EMS service is reachable:
 

```
FWB # execute telnettest 10.65.1.98:443
Connected
```
- Use execute & diagnose commands to check FortiClient EMS status on FortiWeb:
  - Run execute fctems is-verified <EMS>
 

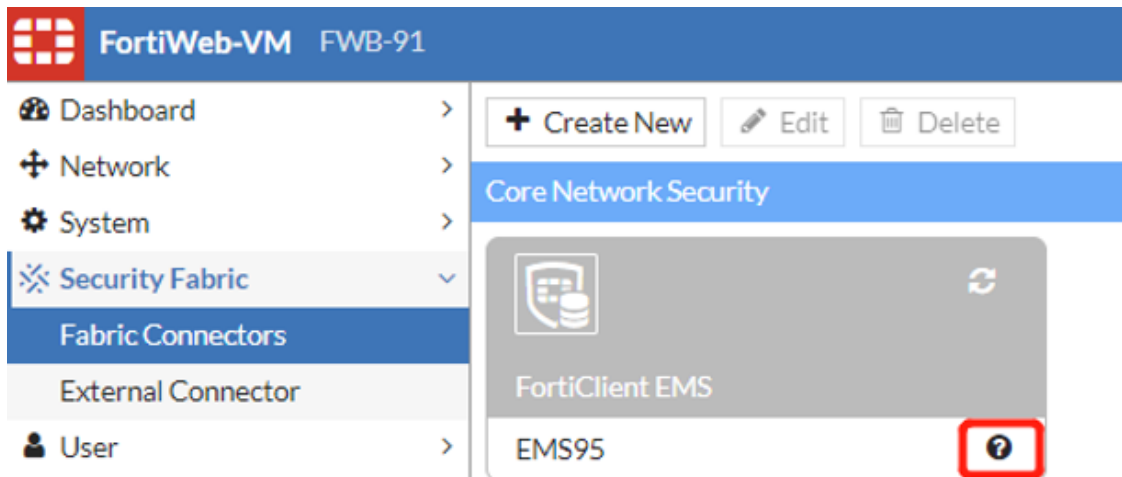
```
FWB-91 # execute fctems is-verified EMS95
Configured FortiClient EMS has not been verified.
This message means that the FortiClient EMS certificate has not been verified by FortiWeb yet. You need to verify it via execute fctems verify <EMS> or click Authorize on GUI.
FWB # execute fctems is-verified EMS95
Configured FortiClient EMS has been verified.
This status means that the FortiClient EMS certificate has been verified by FortiWeb, while FortiWeb is not necessarily authorized by EMS.
Once the FortiClient EMS has been verified, the system will add configuration of fingerprint and EMS_SN as below:
config system endpoint-control fctems
  edit "EMS95"
    set server 10.0.10.95
    set capabilities fabric-auth silent-approval websocket websocket-malware
      push-ca-certs
    set fingerprint
      B7:0B:6E:A4:7A:8F:7F:2F:E1:4A:18:F4:0E:34:65:C8:F0:A6:A7:F7:C7:D2:6
      0:43:A5:49:A0:F6:35:EA:A1:C3:85:87:E1:15:95:B3:12:42:D3:80:96:50:10
      :EA:1C:2C:49:85:DC:F1:B5:EB:10:24:5A:61:A7:37:E8:64:31:CF
    set EMS_SN FCTEMS8822003349
  next
end
```
  - Run diagnose system endpoint-control test <EMS>
 

```
FWB # diagnose system endpoint-control test EMS95
```

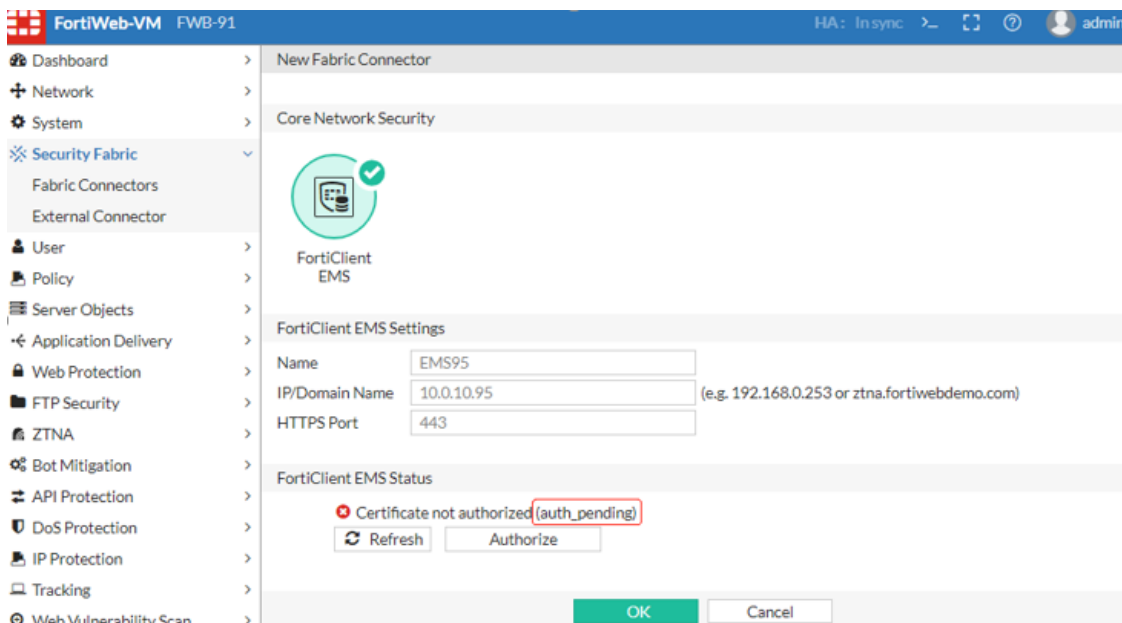
Connection test had an error -3: EMS server connection failed. Authentication denied

#This message indicates FortiWeb has not been authorized, or denied by FortiClient EMS, or the EMS certificate has not been verified by FortiWeb. When adding a new FortiClient EMS connector, FortiWeb and FortiClient EMS need to verify/authorize each other.

- Check the FortiClient EMS status and failure reasons on FortiWeb or FortiClient EMS GUI:
  - The EMS status will be shown with a question mark if FortiClient EMS fabric connection has not been established:



- Check the FortiClient EMS status with failure reasons in the Edit page.
  - auth\_pending: It means FortiWeb has not been authorized by FortiClient EMS, or the FortiClient EMS certificate has not been verified by FortiWeb.
  - auth\_deny: It means FortiWeb authorization has been denied by FortiClient EMS.
  - cert\_unauthorized: It means FortiClient EMS certificate has not been verified by FortiWeb, but FortiWeb has been authorized by EMS.
  - cert\_unknown: It means FortiClient EMS certificate cannot be retrieved, which is usually caused by the EMS IP/Domain or Port is not reachable.



## ZTNA Tags sync issues

Normally, ZTNA tags created on FortiClient EMS will be synchronized in a few seconds after FortiClient EMS connection is established. If new tags or tag changes (e.g. delete) are not updated correctly to FortiWeb, please follow these steps to troubleshoot:

1. Use the methods in section “Check FortiClient EMS connection issues” to confirm if FortiClient EMS is connected successfully and stably.
2. Add a new Zero Trust Tagging rule on FortiClient EMS, check if the new tag can be synchronized to FortiWeb or not.
3. Check if the daemon fcnacd is stable:
  - Execute “fn pidof fcnacd” several times to check if the pid changes
  - Check /var/log/gui\_upload to see if there is any fcnacd or fcsync core dump files
4. Enable diagnose log on FortiWeb to check the sync details.

```
# diagnose debug application fcnacd 7 #communication logs between FortiWeb & EMS
# diagnose debug enable
```

E.g. check the output of `api/v1/report/fct/host_tags` for a successful tag sync process:

```
: [2022-08-09-23:34:10] [ec_ems_context_submit_work:431] Call submitted
  successfully.
obj-id: 10, desc: REST API to get updates about host tags., entry:
  api/v1/report/fct/host_tags.
: [2022-08-09-23:34:10] [ec_ez_worker_process:273] Processing call for obj-id: 10,
  entry: "api/v1/report/fct/host_tags"
: [2022-08-09-23:34:10] [ec_ez_worker_process:348] Call completed successfully.
obj-id: 10, desc: "REST API to get updates about host tags.", entry:
  "api/v1/report/fct/host_tags".
```

For more detailed fcnacd logs, please download `/var/log/debug/fcnacd.log`.

Login to the backend shell, check the output in `/var/log/debug/fcnacd.log` or copy it to `/var/log/gui_upload` and download it via GUI for further checking.

Check the output of `api/v1/report/fct/host_tags` to see if tags are included in the json content:

E.g. check the output of `api/v1/report/fct/host_tags` for a successful tag sync process:

```
: [2022-08-10-00:38:37] [ec_ez_worker_prep_data_url:177] Full URL:
  https://10.65.1.99/api/v1/report/fct/host_tags?&updated_after=2022-06-
  29%2006%3A47%3A03%2E5700870&send_mac=true
: [2022-08-10-00:38:37] [ec_ems_context_submit_work:431] Call submitted
  successfully.
obj-id: 10, desc: REST API to get updates about host tags., entry:
  api/v1/report/fct/host_tags.
: [2022-08-10-00:38:37] [ec_ez_worker_process:273] Processing call for obj-id: 10,
  entry: "api/v1/report/fct/host_tags"
: [2022-08-10-00:38:37] [ec_ez_worker_process:293] reply:
  ""
{"result": {"retval": 1, "message": null}, "data": {"is_final": true, "updated_
  after": "2022-06-29 06:47:03.5700870", "is_zipped": true, "unzipped_size":
  474, "data":
  "eJx1kMlugzAQhF8l8jmphMpP4JYUcslitT21Iv1wJKsajCyTdoo4t0LMhVVetrZb6z1zt4IGm4
  a0ZqzsiSphDSwJFacODaVismNCCm5hhMaCxpKXkiExprB6ZfkRX05sYcSu9rpJzydnWiaLRZCuu4
  DtFqV4rpIwUJhUTXt1OcDW7x1psUCVtEx1+yCkg/O9Le+8k+43nuFtvcIvsGhrSs7V96HRHMQTe
  1YcwfGV3Pfi6OGgt+aP6jqppZCpe52Qs5r927y9VQH0FPQTos+QjlEOIP+r1uEIUs2O5YmLHMj9g
  uztZplucbj1E/8NNwfhHNWw7LjjK4thQVusR4yEo963oqGKy9e0DDxo4Q+PgQRpZuIkr7vfwAn/py
  S"}}
  ""
: [2022-08-10-00:38:37] [fcems_json_unzip:267] unzipped:
  ""
```

```

{"is_snapshot":false,"tag_info":{"all_registered_clients":{},"Low":{},"Medium":
  {},"High":{},"Critical":{},"Zero-day Detections":{},"IOC Suspicious":
  {},"REvil_IOC_registry_key":{},"REvil_IOC_crt":{},"REvil_IOC_exe":{},"A":
  {},"B":{},"Tag_99_02":{},"Test_Tag_01":{},"Tag_Fabric_On":{},"Tag_Fabric_
  Off":{},"Tag_Dev":{},"Tag_Malicious":{},"tag_members":{},"uid_tag_lists":
  {},"uid_info":{"576C5ABC6ECE47CB9E1DEFF82C0454D6":{"host_tag_update_
  time":"2022-06-29 06:47:03.5700870"}}}
""
: [2022-08-10-00:38:37] [ec_ez_worker_process:348] Call completed successfully.
obj-id: 10, desc: "REST API to get updates about host tags.", entry:
  "api/v1/report/fct/host_tags".
    
```

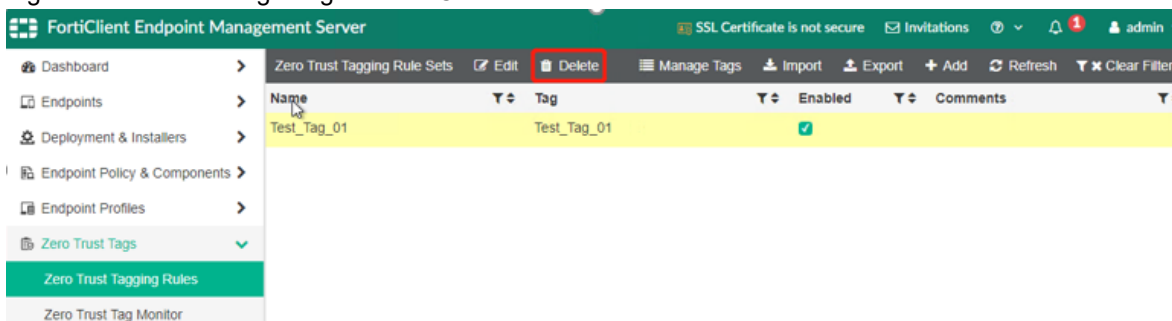
All EMS tags are synchronized and contained in the above unzipped json content. You can check if the newly-added tag is included or the removed tag is NOT included. If the new tag is NOT included, you may check if it is an EMS problem rather than a FortiWeb issue.

To improve the readability, the above json content is transferred with a json formatter and simplified:

```

{
  "tag_info":{
    "Test_Tag_01":{
    },
    "Tag_Fabric_On":{
    },
    "Tag_Fabric_Off":{
    },
    "Tag_Dev":{
    },
    "Tag_Malicious":{
    }
  },
  "uid_info":{
    "576C5ABC6ECE47CB9E1DEFF82C0454D6":{
      "host_tag_update_time":"2022-06-29 06:47:03.5700870"
    }
  }
}
    
```

5. Particularly, if you are deleting a tag, please double confirm not only the tagging rule is deleted, but also the tag is deleted in “Manage Tags” in FortiClient EMS.



6. A tag referenced in a ZTNA rule or HTTP Content-routing policy will NOT be removed from FortiWeb immediately after the tag is removed from FortiClient EMS. Only if the tag is removed from ZTNA rule or HTTP Content-routing policy, it will be removed by FortiWeb automatically; FortiWeb will check if a current tag saved in configuration is used or not in each tag sync cycle. When the system boots up, if it has been removed from FortiClient EMS and not used in any ZTNA rule or HTTP Content-routing policy any more, the tag will be deleted.

## Endpoint client information sync issues

Information of all endpoint clients registered to the FortiClient EMS will be synchronized to FortiWeb. If you find that an endpoint is not synchronized or information changes are not updated to FortiWeb, please follow the below steps for troubleshooting:

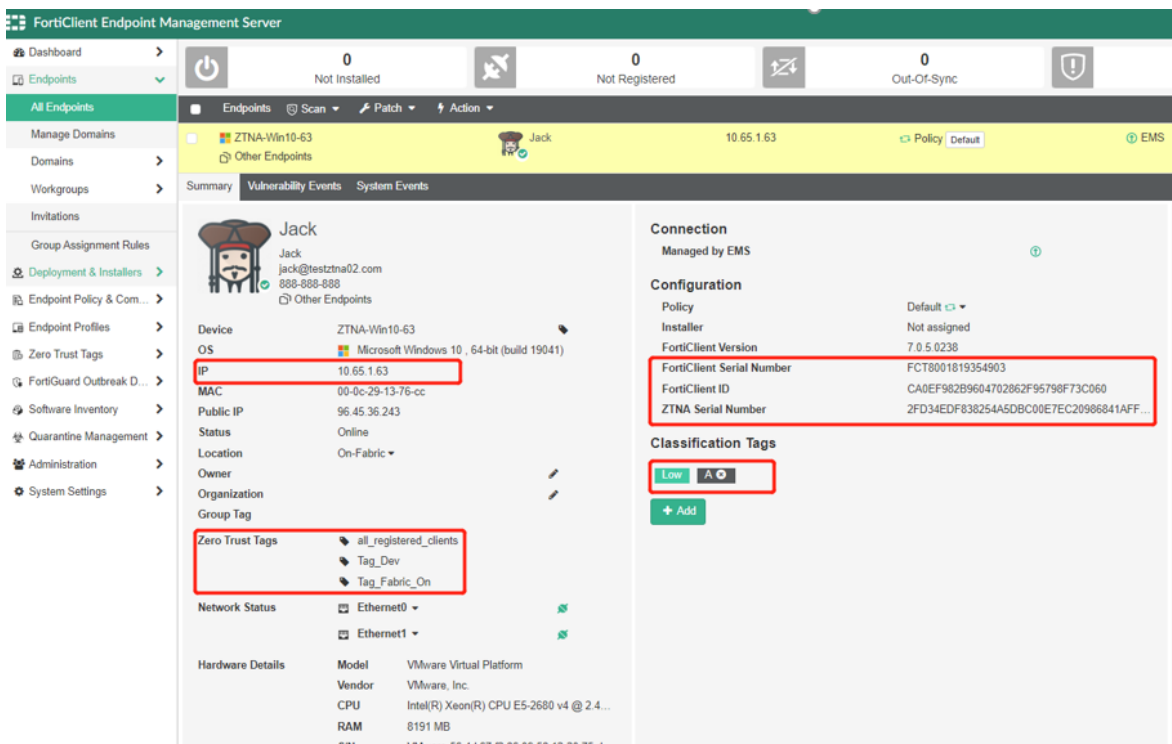
1. Check diagnose system endpoint client on FortiWeb to see if the client information is up-to-date: You can add filters to search a specific endpoint client:

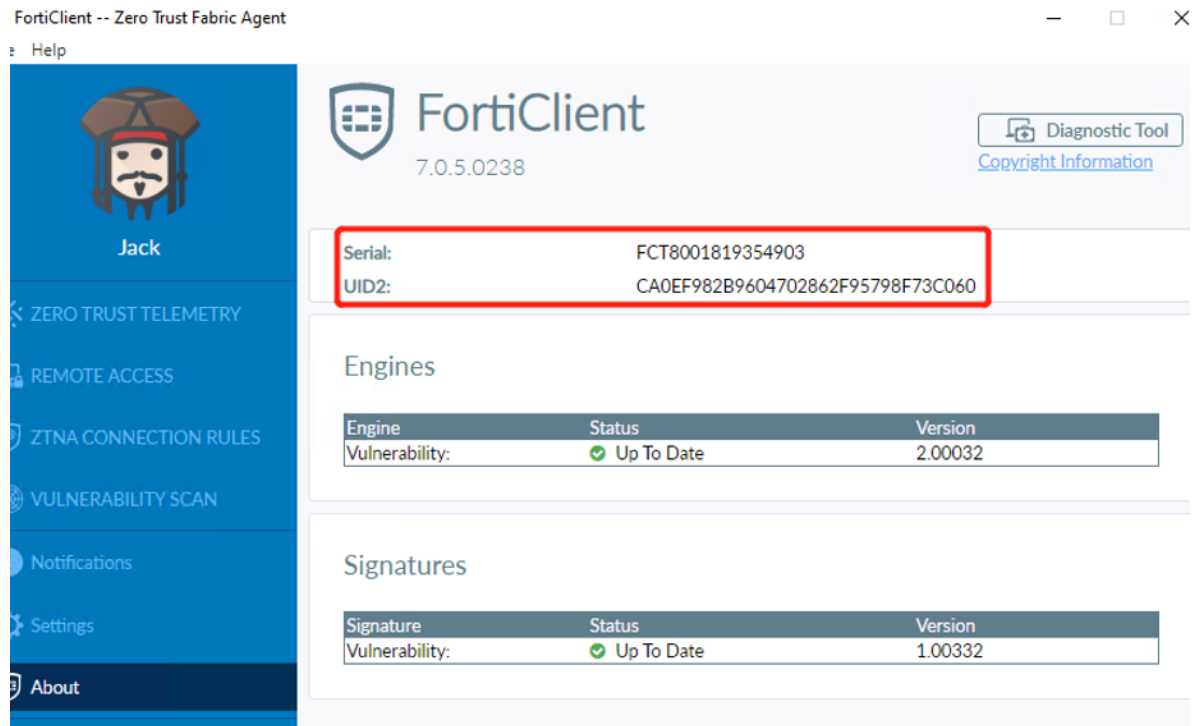
```
FortiWeb # diagnose system endpoint-control clients <IP> <MAC> <FCT_SN>
```

Each filter option can be set as “any” for all.

2. Compare client info on FortiWeb with the endpoint info shown in FortiClient EMS **Endpoints > All Endpoints**, and that displayed in FortiClient.

Pay attention to the circled info: EMS SN, FortiClient ID / UID, IP and Tags.





If **Show Zero Trust Tag on FortiClient GUI** is enabled in FortiClient EMS **Endpoint > Profiles > System Settings**, you can also see the ZTNA tags on the FortiClient.

3. If there is no Endpoint information or some information is not up-to-date on FortiWeb, check if FortiClient EMS is connected successfully and stably first, with the methods mentioned in section "Check FortiClient EMS connection issues".
4. Check if the daemon fcnacd is stable:
  - a. Execute `fn pidof fcnacd` several times to check if the pid changes.
  - b. Check `/var/log/gui_upload` to see if there is any fcnacd or fcsync coredump files.
5. If FortiClient EMS is connected while client information is not updated, enable diagnose log on FortiWeb to check if there is any sync failure.

```
# diagnose debug application fcnacd 7 #communication logs between FortiWeb & EMS
# diagnose debug enable
```

E.g. check the output of `api/v1/report/fct/uid_tags` to see if the tag changes is reflected in logs:

```
: [2022-08-09-23:34:10] [ec_ems_context_submit_work:431] Call submitted
  successfully.
obj-id: 12, desc: REST API to get updates of tags associated with FCT UID., entry:
  api/v1/report/fct/uid_tags.
: [2022-08-09-23:34:10] [ec_ez_worker_process:273] Processing call for obj-id: 12,
  entry: "api/v1/report/fct/uid_tags"
: [2022-08-09-23:34:10] [ec_ez_worker_process:348] Call completed successfully.
obj-id: 12, desc: "REST API to get updates of tags associated with FCT UID.",
  entry: "api/v1/report/fct/uid_tags".
```

For more detailed fcnacd logs, please download `/var/log/debug/fcnacd.log`.

6. Log in to the backend shell, check output in `/var/log/debug/fcnacd.log` or copy it to `/var/log/gui_upload` and download it via GUI for further checking.
 

Particularly when you find tags are not updated to a specific client, check the output of `api/v1/report/fct/uid_tags` to see if tags are included in the json content:

E.g. the output of `api/v1/report/fct/uid_tags` below is when a new tag "" is applied to the client, UID `CA0EF982B9604702862F95798F73C060`:

```
[2022-08-10-14:08:47] [ec_ez_worker_prep_data_url:177] Full URL:
https://10.65.1.99/api/v1/report/fct/uid_tags?&updated_after=2022-08-
10%2020%3A28%3A25%2E7803527&uid_
offset=CA0EF982B9604702862F95798F73C060&send_mac=true
[2022-08-10-14:08:47] [ec_ems_context_submit_work:431] Call submitted
successfully.
obj-id: 12, desc: REST API to get updates of tags associated with FCT UID., entry:
api/v1/report/fct/uid_tags.
[2022-08-10-14:08:47] [ec_ez_worker_process:273] Processing call for obj-id: 12,
entry: "api/v1/report/fct/uid_tags"
[2022-08-10-14:08:47] [ec_ez_worker_process:293] reply:
""
{"result": {"retval": 1, "message": null}, "data": {"uid_offset":
"CA0EF982B9604702862F95798F73C060", "updated_after": "2022-08-10
21:08:41.8294435", "is_zipped": true, "is_final": true, "unzipped_size":
558, "data":
"eJxl0TlvGzEMBuC/Umg2C4oi9eFNH6epQJduRXG4xEJyg00E9iUdjPvvVbyduwkQ30cieVMf82F
cppfxOF+Xq9rfVI4410ApBYvskLylGsQFX53JaPGr5tROT+3Sy3/flFe4I2qvtFDWlCMUwxY4uwi
hFgOOxIoZKDjntbsHztOp9URU624jJGtqQg07LsQLUSLESRSEpsDc7VbIT0I/YvinTBELgm4aAM
xmQBWUuCQK2nSW2E6HsdLe+ntt0s7jM/HuZ37JLasd/1tHgwEtNjZNPcSGDAua4em2OTqlv3Vj3V
6uszP48/zg1aISAg1RJP7oFxA8MFoGJJLLHEIgfz/WmmfD84gyJkoQfbEwFQqpOgQUCSWkEqWULb
Oj7e/av2zU69v1+W+9o/3w7S0cZnv14REgB40fiO9R79n/d1Tb92IWtflH0gJmbU="}}
""
[2022-08-10-14:08:47] [fcems_json_unzip:267] unzipped:
""
{"uid_tag_lists":{"CA0EF982B9604702862F95798F73C060":{"members":[{"tag_
uid":"152C12CA-D346-4C7A-9FD3-725653E2A44C","tag_name":"A"}, {"tag_
uid":"1B63FB05-0648-4CA6-A60A-5A2B56C944F6","tag_name":"B"}, {"tag_
uid":"3C058754-A4DB-4D13-AB39-65B949CF2121","tag_name":"all_registered_
clients"}, {"tag_uid":"879444E3-9065-4D43-BB53-37C1703D6B7F","tag_name":"Tag_
Fabric_On"}, {"tag_uid":"D2225201-A3C6-4790-8931-EB7B45AE9928","tag_
name":"Tag_Dev"}, {"tag_uid":"E504C22B-C824-42DF-BA70-055AD9BDC59D","tag_
name":"Low"}],"host_tag_update_time":"2022-08-10 21:08:41.8294435"}}}
""
[2022-08-10-14:08:47] [_handle_json_tag_list:93] Add 1 member tags for
FCTEMS8822003003
[2022-08-10-14:08:47] [ec_ez_worker_process:348] Call completed successfully.
obj-id: 12, desc: "REST API to get updates of tags associated with FCT UID.",
entry: "api/v1/report/fct/uid_tags".
```

All EMS tags applied to a specific client will be contained in the unzipped json content. One can check if the newly-added tag is included or the removed tag is NOT included. If the new tag is NOT included, one may check if it is an EMS problem rather than a FortiWeb issue.

To improve the readability, the above json content is transferred with a json formatter and simplified:

```
{
  "uid_tag_lists": {
    "CA0EF982B9604702862F95798F73C060": {
      "members": [
        {
          "tag_uid": "152C12CA-D346-4C7A-9FD3-725653E2A44C",
          "tag_name": "A"
        },
        {
          "tag_uid": "1B63FB05-0648-4CA6-A60A-5A2B56C944F6",
          "tag_name": "B"
        }
      ]
    }
  }
}
```

```

{
  "tag_uid": "3C058754-A4DB-4D13-AB39-65B949CF2121",
  "tag_name": "all_registered_clients"
},
{
  "tag_uid": "879444E3-9065-4D43-BB53-37C1703D6B7F",
  "tag_name": "Tag_Fabric_On"
},
{
  "tag_uid": "D2225201-A3C6-4790-8931-EB7B45AE9928",
  "tag_name": "Tag_Dev"
},
{
  "tag_uid": "E504C22B-C824-42DF-BA70-055AD9BDC59D",
  "tag_name": "Low"
}
],
"host_tag_update_time": "2022-08-10 21:08:41.8294435"
}
}
}

```

You can only see the content of `uid_tag_lists` when tags applied to a client are changed, either added or removed. Without tag changes, the content of the `uid_tag_lists` will be empty:

```

: [2022-08-10-14:08:53] [fcems_json_unzip:267] unzipped:
""
{"uid_tag_lists":{}}
""

```

## ZTNA Access Control issues 1 - browsers do not prompt certificate selecting

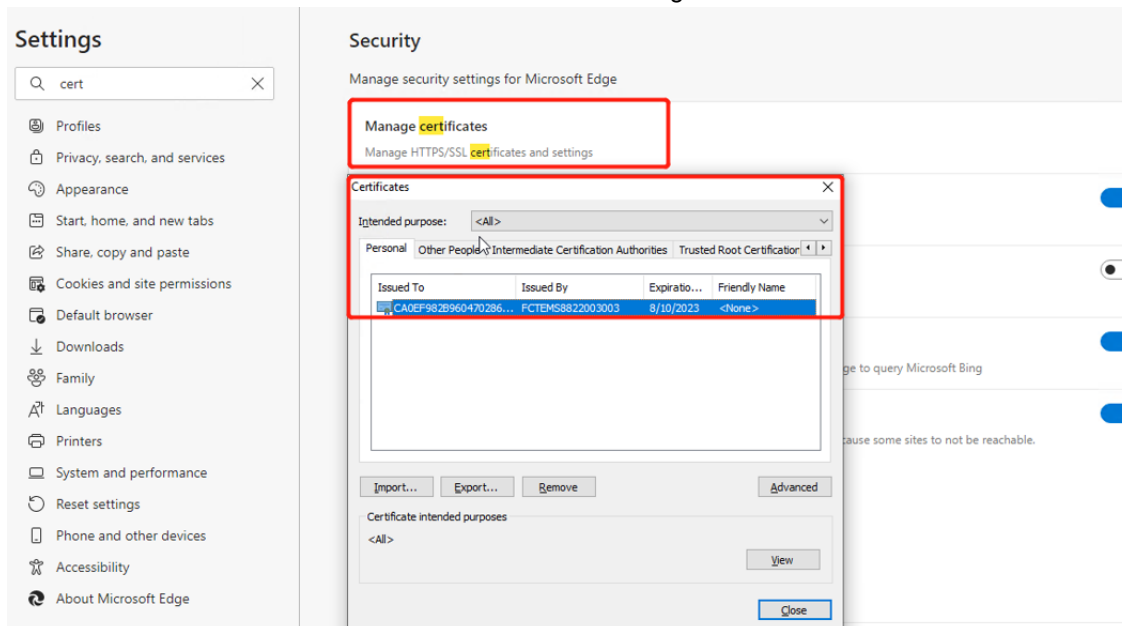
HTTPS with client certificate verification is a must when a ZTNA profile is applied to a server policy. So to use ZTNA, you need to create a certificate verification rule and select it in Advanced SSL settings > Certificate Verification for HTTPS, or enable SNI and select one in a SNI policy.

If the browser does not pop up the FortiClient certificate when you visiting a server policy, please follow these steps for troubleshooting:

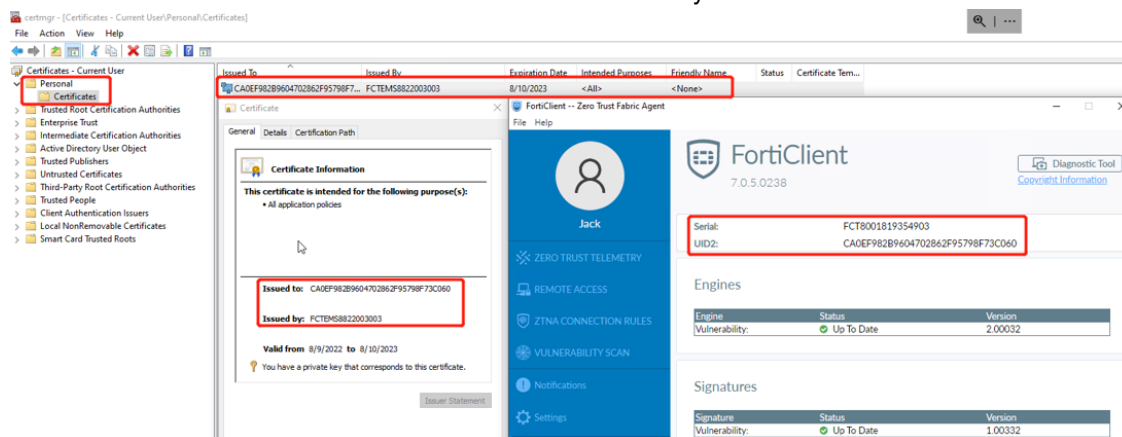
1. Check if the FortiWeb and server policy is reachable;
  - Disable ZTNA profile first and guarantee the server policy works without ZTNA;
  - Refer to "Diagnose server-policy connectivity issues" above for more troubleshooting methods
2. Check if the client certificate is signed and stored on the FortiClient PC;
  - Confirm the FortiClient is connected to the correct FortiClient EMS;
3. Check if the client certificate is available on the client PC;
 

Use either of the below two ways to check:

- Check if the client certificate is available in the browser storage:



- Search & open “Manage user certificates” on the Client PC; the FortiClient certificate signed by FortiClient EMS should be seen in Personal certificate directory as below:

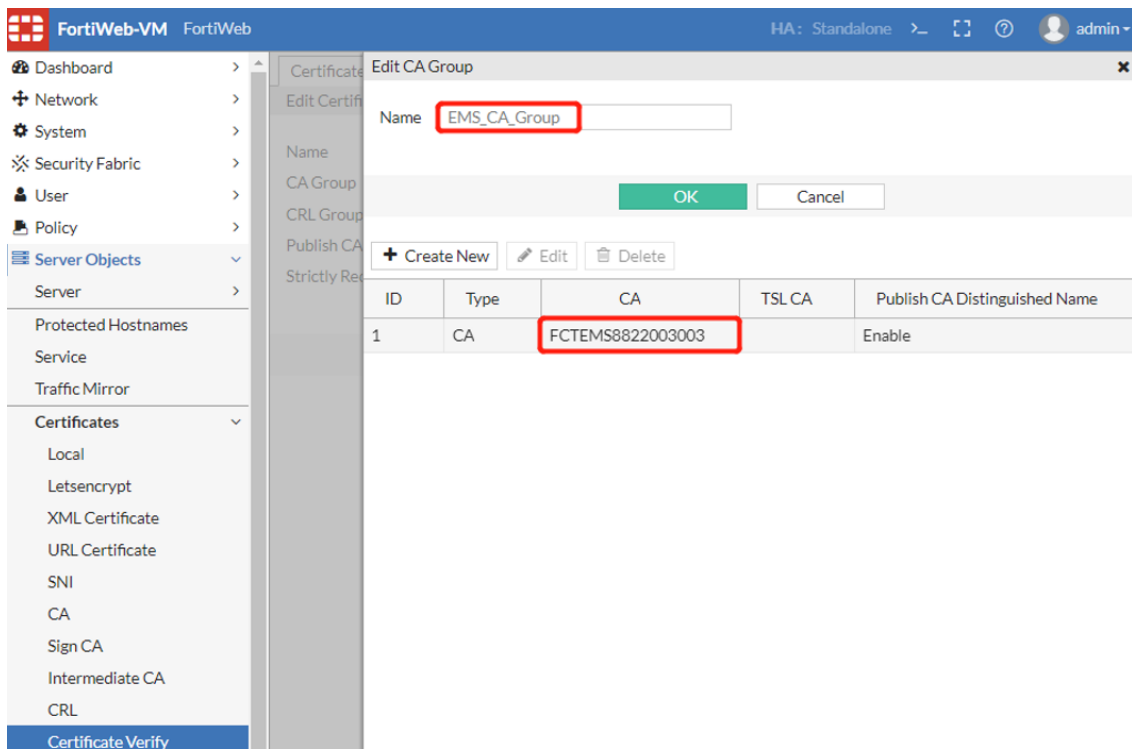
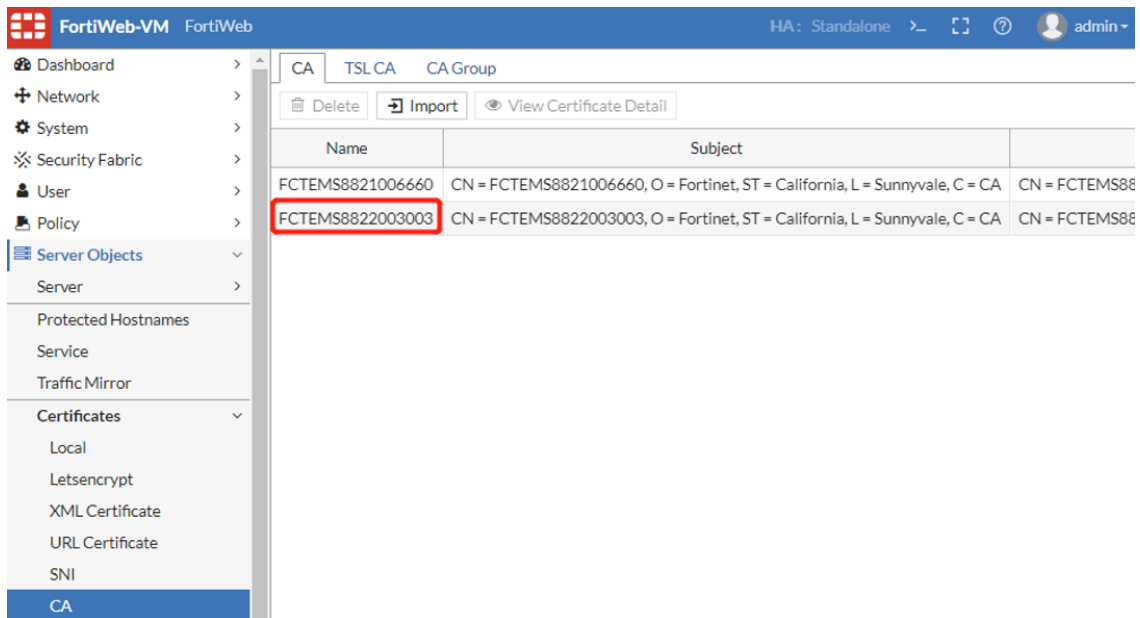


Please note if the certificate is not available, it might be a FortiClient or FortiClient EMS issue. You can try to disconnect and reconnect the FortiClient EMS to see if a new certificate can be fetched. This process may take a few seconds or more than one minute.

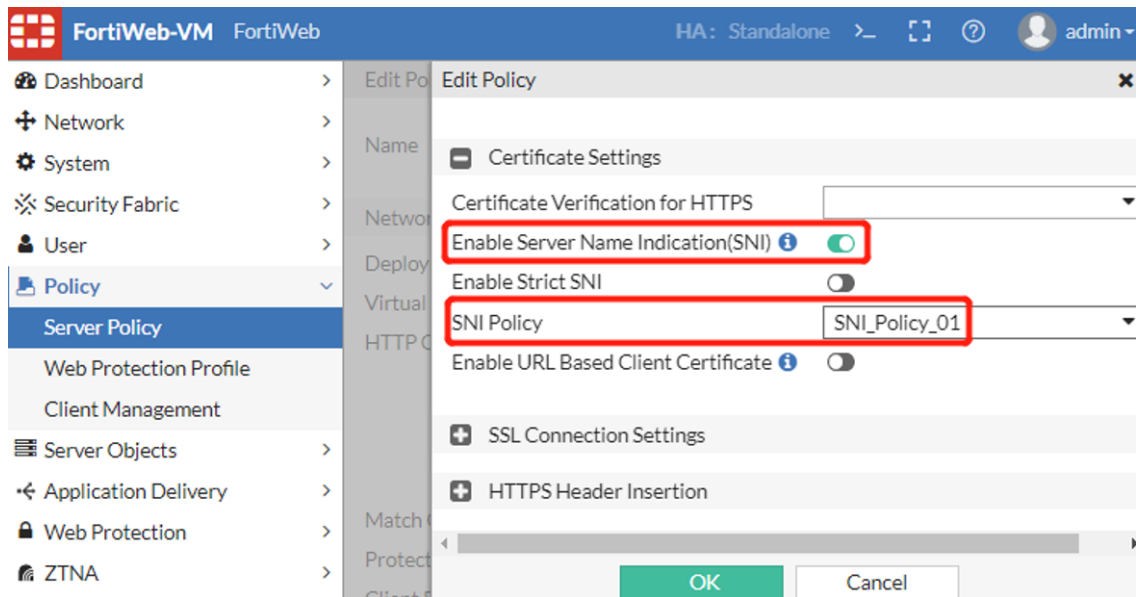
4. Check the SSL configuration on FortiWeb.

If client certificate verification is not configured properly, the browser will not prompt certificate selecting. Pay attention to these configuration:

- Confirm that the CA Group in Certificate Verify rule includes the correct CA certificate.  
 This CA certificate is the FortiClient EMS CA certificate (ZTNA) that can be found in FortiClient EMS in **System Settings > EMS Settings**;  
 This CA certificate is synchronized from FortiClient EMS and can be found on in FortiWeb **Server Objects > Certificates > CA**; the name is the EMS SN.



- Similarly, if you configure a SNI policy instead of directly selecting a client certificate verify rule, please make sure the correct certificate verify rule is configured for the SNI policy.



## ZTNA Access Control issues 2 - ZTNA tags are not matched as expected in ZTNA rules or HTTP Content-routing policy

When the client certificate is selected but ZTNA actions are not taken as expected, please troubleshoot from these aspects:

1. Confirm the client certificate is correct:
  - When multiple certificates are prompted by the browser, confirm the correct certificate is selected. Only when the UID (FortiClient ID) and the FortiClient EMS SN match, tag searching may continue.
  - Do not click **Cancel** selecting the certificate on browser, otherwise SSL handshake will fail (when Strictly Require Client Certificate is enabled in the Client Certificate Verify rule), then tag matching cannot be processed.
2. Confirm the Tags of the client match those configured in ZTNA rules:
  - Compare client information displayed in `diagnose system endpoint client` with that shown on FortiClient EMS or FortiClient; make sure that the key fields such as FortiClient ID/UID, EMS SN, IP, FCT\_SN, and Tags are the same.
  - Check the tag name carefully. Tags displayed in `diagnose system endpoint client` should be the same with that configured in ZTNA rule and originally created on EMS
    - Tags shown on FortiWeb CLI has a prefix as the EMS\_SN, but the prefix is not included in the diagnose output and FortiWeb GUI
    - Although FortiClient EMS and FortiWeb support almost all special characters as the tag name, we recommend using alphabet and numbers. Please examine and compare the tags carefully when you encounter tag matching failures.
3. Enable diagnose debug logs to check the detailed ZTNA processing:
 

```
# diagnose debug flow filter module-detail ztna 7 #ZTNA rule matching logs
# diagnose debug proxy svr-balance 7 #ZTNA server load balance logs
# diagnose debug proxy thread-ztna-sync 7 #ZTNA endpoint sync logs
# diagnose debug timestamp enable
# diagnose debug enable
```

**Example 1:** Server-policy + Certificate Verification + ZTNA Profile/Rule

```

<11: 8: 2>[SLB][DEBUG][line:0514]
<11: 8: 2>[SLB][DEBUG][line:0515] Prepare to run slb in pool
<11: 8: 2>[SLB][DEBUG][line:0058] -----Assign server -----
<11: 8: 2>[SLB][DEBUG][line:0061] Assign server IP: 2001:1234::a41:142
<11: 8: 2>[SLB][DEBUG][line:0068] Assign server port 443
<11: 8: 2>[SLB][DEBUG][line:0070] Connection Number 1
<11: 8: 2>[SLB][DEBUG][line:0072] -----Assign server finished-----
-----
<11: 8: 2>[ZTNA_RULE][INFO] Enter ZTNA rule match
<11: 8: 2>[ZTNA_RULE][INFO] Client cert issuer common name: FCTEMS8822003003
<11: 8: 2>[ZTNA_RULE][INFO] Client cert subject common name:
    CA0EF982B9604702862F95798F73C060
==> Certificate verification passed; start checking tags via UID fetched from
    certificate
<11: 8: 2>[ZTNA_RULE][INFO] ZTNA rule ztna_rule_01 match begin
<11: 8: 2>[ZTNA_RULE][INFO] ===Check GEO===: Unknown Country/Region
<11: 8: 2>[ZTNA_RULE][INFO] Matched ztna geo condition 1
<11: 8: 2>[ZTNA_RULE][INFO] ===Check EMS Tags===: client ems tags: 4, ems tag
    rule: 1
<11: 8: 2>[ZTNA_RULE][INFO] Check ZTNA ems tag condition 1
<11: 8: 2>[ZTNA_RULE][INFO] Check Client EMS tag: all_registered_clients
<11: 8: 2>[ZTNA_RULE][INFO] Check Client EMS tag: Tag_Sales
<11: 8: 2>[ZTNA_RULE][INFO] Check Client EMS tag: Tag_Fabric_On
<11: 8: 2>[ZTNA_RULE][INFO] Check Client EMS tag: High
<11: 8: 2>[ZTNA_RULE][INFO] Not matched any ztna ems tags condition
<11: 8: 2>[ZTNA_RULE][INFO] ZTNA rule ztna_rule_01 match finish, not matched
<11: 8: 2>[ZTNA_RULE][INFO] ZTNA rule ztna_rule_02 match begin
<11: 8: 2>[ZTNA_RULE][INFO] ===Check source address===: 10.65.1.63
<11: 8: 2>[ZTNA_RULE][INFO] Matched ztna source addr condition 1
<11: 8: 2>[ZTNA_RULE][INFO] ===Check EMS Tags===: client ems tags: 4, ems tag
    rule: 1
<11: 8: 2>[ZTNA_RULE][INFO] Check ZTNA ems tag condition 1
<11: 8: 2>[ZTNA_RULE][INFO] Check ZTNA rule EMS tag: FCTEMS8822003003_Tag_Fabric_
    On
<11: 8: 2>[ZTNA_RULE][INFO] Check ZTNA rule EMS tag: FCTEMS8822003003_Tag_Sales
<11: 8: 2>[ZTNA_RULE][INFO] Matched ztna ems tags condition 1
<11: 8: 2>[ZTNA_RULE][INFO] ZTNA rule ztna_rule_02 match finish, matched
<11: 8: 2>[ZTNA_RULE][INFO] Matched ztna-profile ztna_profile_01, ztna-rule ztna_
    rule_02, action 1
==> Action Code: 1: Accept; 4: Deny (no log); 6: Alert & Deny

```

### Example 2: HTTP Content-routing policy + Certificate Verification + ZTNA Profile/Rule

```

<11:36:55>[SLB][DEBUG][line:0825] HTTP Request URL : /sales/index.html
<11:36:55>[ZTNA_RULE][INFO] Client cert issuer common name: FCTEMS8822003003
<11:36:55>[ZTNA_RULE][INFO] Client cert subject common name:
    CA0EF982B9604702862F95798F73C060
==> Certificate verification passed; start checking tags via UID fetched from
    certificate
<11:36:55>[ZTNA_RULE][INFO] Check ZTNA rule EMS tag: FCTEMS8822002977_all_
    registered_clients #The ZTNA Tag configured in the policy
<11:36:55>[SLB][DEBUG][line:0878] not matched ztna ems tag
<11:36:55>[SLB][DEBUG][line:1146] Match item id(2) match_object(13) ret = -1.
==> The 1st HTTP content-routing policy not matched due to tags are not matched
<11:36:55>[SLB][DEBUG][line:0933] match request: /sales/index.html <-> /sales/.
<11:36:55>[SLB][DEBUG][line:1146] Match item id(1) match_object(2) ret = 0.
==> The 1st match object (URL) in the 2nd HTTP content-routing policy matched
<11:36:55>[ZTNA_RULE][INFO] Client cert issuer common name: FCTEMS8822003003

```

```

<11:36:55>[ZTNA_RULE][INFO] Client cert subject common name:
    CA0EF982B9604702862F95798F73C060
<11:36:55>[ZTNA_RULE][INFO] Check ZTNA rule EMS tag: FCTEMS8822003003_Tag_Sales
<11:36:55>[ZTNA_RULE][INFO] Check ZTNA rule EMS tag: FCTEMS8822003003_all_
    registered_clients
<11:36:55>[SLB][DEBUG][line:0875] matched ztna ems tag
<11:36:55>[SLB][DEBUG][line:1146] Match item id(2) match_object(13) ret = 0.
==> The 2st match object (ZTNA Tags) in the 2nd HTTP content-routing policy
    matched
<11:36:55>[SLB][DEBUG][line:1375] Hit content routing (CR_Policy_Sales).
==> The 2nd HTTP content-routing policy matched
<11:36:55>[SLB][DEBUG][line:0514]
<11:36:55>[SLB][DEBUG][line:0515] Prepare to run slb in pool
<11:36:55>[SLB][DEBUG][line:0126] scheduler_rr: server_count=1, backup =0
<11:36:55>[SLB][DEBUG][line:0058] -----Assign server -----
<11:36:55>[SLB][DEBUG][line:0061] Assign server IP: 10.65.1.66
<11:36:55>[SLB][DEBUG][line:0068] Assign server port 80
<11:36:55>[SLB][DEBUG][line:0070] Connection Number 1
<11:36:55>[SLB][DEBUG][line:0072] -----Assign server finished-----
-----
<11:36:55>[ZTNA_RULE][INFO] Enter ZTNA rule match
<11:36:55>[ZTNA_RULE][INFO] Client cert issuer common name: FCTEMS8822003003
<11:36:55>[ZTNA_RULE][INFO] Client cert subject common name:
    CA0EF982B9604702862F95798F73C060
<11:36:55>[ZTNA_RULE][INFO] ZTNA rule ztna_rule_03 match begin
<11:36:55>[ZTNA_RULE][INFO] ===Check source address===: 10.65.1.63
<11:36:55>[ZTNA_RULE][INFO] Matched ztna source addr condition 1
<11:36:55>[ZTNA_RULE][INFO] ===Check GEO===: Unknown Country/Region
<11:36:55>[ZTNA_RULE][INFO] Matched ztna geo condition 1
<11:36:55>[ZTNA_RULE][INFO] ===Check EMS Tags===: client ems tags: 4, ems tag
    rule: 1
<11:36:55>[ZTNA_RULE][INFO] Check ZTNA ems tag condition 1
<11:36:55>[ZTNA_RULE][INFO] Check ZTNA rule EMS tag: FCTEMS8822003003_High
<11:36:55>[ZTNA_RULE][INFO] Matched ztna ems tags condition 1
<11:36:55>[ZTNA_RULE][INFO] ZTNA rule ztna_rule_03 match finish, matched
<11:36:55>[ZTNA_RULE][INFO] Matched ztna-profile ztna_profile_02, ztna-rule ztna_
    rule_03, action 1
==> After HTTP content-routing policy matched, ZTNA profile/rule also matched

```

#### Example 3: When an incorrect client certificate is selected

```

<12:53: 6>[ZTNA_RULE][INFO] Client cert issuer common name: FCTEMS8822002977
<12:53: 6>[ZTNA_RULE][INFO] Client cert subject common name:
    CA0EF982B9604702862F95798F73C060
<12:53: 6>[ZTNA_THREAD][ERR] ztna get client tags from db failed, uid:
    CA0EF982B9604702862F95798F73C060, sn: FCTEMS8822002977
<12:53: 6>[ZTNA_RULE][DEBUG] Cannot get client ems tags or no ems tags
==> ZTNA fails to get the client tags from database due to failing to fetch the
    corresponding UID from the client certificate.

```

4. Sometimes you may find even if a tag is removed on FortiClient EMS, and the tag has been removed from the client displayed in diagnose system endpoint clients, it will still be matched in ZTNA rule. You may wait for one more minute and check the result again. In current implementation, there is a time gap between tags synchronized from FortiClient EMS to FortiWeb redis db and tags synchronized from redis db to proxyd cache. Proxyd sync interval is 60 seconds. It means that even if you see the tag is removed in diagnose system endpoint clients, this change will take more time to update to Proxyd.

## ZTNA Access Control issues 3 - Source IP or GEO IP are not matched in ZTNA rules

Source IP and GEO IP can be configured as conditions in a ZTNA rule. This improves the flexibility of ZTNA rules.

There are several tips when using Source IP or GEO IP rather than ZTNA Tags as a condition:

- The source IP to be matched is the source IP in the IP header of the request packet sent to FortiWeb, not the IP field in the endpoint information
- IP addresses in X-Forward-For headers will not be matched

You can enable diagnose debug logs to check process details.

## ZTNA issues in HA environment

In HA deployment, only the primary FortiWeb connects to FortiClient EMS and keeps pulling ZTNA tags and clients information from it, and then synchronizes these information to the secondary nodes.

In Active-Passive mode, only the primary FortiWeb processes ZTNA traffic, so if there is any issue, you just need to troubleshoot on the primary node according to above methods.

In Active-Active standard and Active-Active high volume HA modes, the situation is a little different - both the primary and secondary nodes may process ZTNA traffic. So when issues occur, you also need to consider troubleshooting on secondary nodes.

1. Make sure that HA status is stable and configuration are synchronized among all HA nodes;
2. In Active-Active standard and Active-Active high volume HA modes, make that server policy works well without ZTNA profile;
3. Check fcnacd diagnose logs to guarantee only the primary node communicates with FortiClient EMS;
4. Check if all endpoint clients information are synchronized among all HA nodes;
5. If the clients information are not synchronized among all HA nodes, or new client information cannot be synchronized from FortiClient EMS after HA failover, check with below points:

- Check if redis processes are working properly:

On the primary node, redis-server is working on 169.254.0.1:6389

```
# ps | grep redis-server | grep 6389
29158 root 55448 S /bin/redis-server 169.254.0.1:6389
```

On secondary nodes, redis-server is working on 169.254.0.2, 169.254.0.3 or other IP:

```
# ps | grep redis-server | grep 6389
22682 root 128m S /bin/redis-server 169.254.0.2:6389
```

- Check fcsync logs to see if there is any sync issues among HA nodes:

```
# diagnose debug application fcsync 7
# diagnose debug enable
```

For more details, log in to the backend shell, check the output in /var/log/debug/fcsync\_log or copy it to /var/log/gui\_upload and download it via GUI for further checking.

E.g. when secondary HA node switches to be the primary role, fcsync will monitor this event and re-initiate redis service and db sync process

```
/# tail -f /var/log/debug/fcsync_log
* Thu Aug 11 17:44:00 2022 : dbsync_msg_act.c[ 26]: <--- fcsync ---> recv msg
    from confd_ha, ha mode change, old role:2 new member id is:1
* Thu Aug 11 17:44:00 2022 : main.c [ 283]: running mode changed, old mode:2
```

```

* Thu Aug 11 17:44:00 2022 : main.c [ 182]: release cmdb poll:7 for fcsync
* Thu Aug 11 17:44:00 2022 : main.c [ 189]: release sync msg poll:9 for fcsync
* Thu Aug 11 17:44:02 2022 : main.c [ 368]: <--- fcsync 0 ---> start pid:25360
* Thu Aug 11 17:44:02 2022 : main.c [ 143]: init cmdb poll:7 for fcsync
* Thu Aug 11 17:44:02 2022 : main.c [ 155]: init trans poll for fcsync
* Thu Aug 11 17:44:02 2022 : main.c [ 170]: init config for fcsync
* Thu Aug 11 17:44:02 2022 : main.c [ 230]: <--- fcsync 1 ---> ha_mode:1
  pid:25360
* Thu Aug 11 17:44:02 2022 : main.c [ 257]: <--- fcsync 2 ---> ha role:1
* Thu Aug 11 17:44:02 2022 : main.c [ 258]: AP mode, role is 1, unknown:0
  master:1, slave:2
* Thu Aug 11 17:44:02 2022 : dbsync_redis.c [ 377]: <--- fcsync ---> dbsync_
  change_to_master:377 change to master
* Thu Aug 11 17:44:02 2022 : dbsync_redis.c [ 147]: old config:<bind
  169.254.0.2 127.0.0.1
> new config:<bind 169.254.0.1 127.0.0.1
* Thu Aug 11 17:44:02 2022 : dbsync_redis.c [ 385]: dbsync_change_to_
  master:385 restart_daemon change[3]
* Thu Aug 11 17:44:04 2022 : dbsync_redis.c [ 352]: s_pid:29158 root 52888 S
  /bin/redis-server 169.254.0.1:6389

```

**Notes:** Collect `/var/log/debug/fcsync_log` and `/etc/redis/redis_6389.conf` on both primary node and secondary nodes for support team analysis.

## HA issues

### FAQ

- [What is the requirement of FortiWeb nodes to establish an HA group? on page 196](#)
- [What is the basic configuration to set up HA? on page 196](#)
- [What is the requirement for heartbeat links? on page 197](#)
- [Does heartbeat work in layer 2 or layer 3 \(Network Type\)? on page 197](#)
- [Will HA nodes use physical MAC address or virtual MAC address for communication? on page 198](#)
- [How to manage HA nodes, especially the secondary nodes via SSH or GUI? on page 198](#)
- [Does FortiWeb synchronize session information in HA mode? on page 198](#)

### HA trouble-shooting

- [Common Troubleshooting Steps on page 199](#)
- [Troubleshooting HA issues when FortiWeb nodes are deployed on Hypervisors - Extra configuration on ESXi for HA deployment on page 200](#)
- [HA Status issue 1 - All nodes are Primary on page 202](#)
- [HA Status issue 2 - Unexpected switch over on page 203](#)
- [Traffic drops down in HA environment on page 205](#)
- [HA Synchronization issues on page 208](#)

## FAQ

### What is the requirement of FortiWeb nodes to establish an HA group?

To set up FortiWeb HA, the below configuration are required at least:

- ha mode
- ha group-id
- set hbdev <port\_id> #send heartbeat signals & synchronization data
- set monitor <port\_id> #not must but recommended; support physical & aggregate ports only (not support VLAN or 4-port switch)
- set tunnel-local 10.0.0.1 #when network-type is udp-tunnel
- set tunnel-peer 10.0.0.2 #when network-type is udp-tunnel

### What is the basic configuration to set up HA?

To establish normal HA status, 4S (4 Sames) are required:

- Same Platform
- Same Firmware Version
- Same Group ID
- Same Override option

In addition to the basic settings, you need to add HA members to Node Allocation and set Traffic Distributions for the high volume active-active mode.

### How is FortiWeb appliance elected to be the primary node?

On 7.0.2 and previous builds, FortiWeb HA nodes elect the primary role by these rules:

- If Override is disabled:  
Available ports number (Monitor) > Uptime > Priority > SN
- If Override is enabled:  
Available ports number (Monitor) > Priority > Uptime > SN

The Serial numbers are sorted by comparing each character from left to right, where 9 and z are the greatest values, and rank in the highest place at the sorted list. Since it's very rare that different nodes have the exact same uptime, SN is rarely compared.

From 7.0.4, corefile-ha-failover is supported. If it's enabled in server-policy setting, the election orders can be treated as below:

- If Override is disabled:  
Corefile (Monitor) > Available monitored ports (Monitor) > Uptime > Priority > SN
- If Override is enabled:  
Corefile (Monitor) > Available monitored ports (Monitor) > Priority > Uptime > SN

As above, the Corefile and Available ports share the same factor "Monitor" in selection, just the corefile has higher weight. So if a proxyd coredump is detected on the primary device, the weight of corefile-ha-failover will be reduced thus the total weight of Monitor will become lower than that of other secondary devices, then HA failover will take place.

In event logs, HA failover triggered by corefile-ha-failover will be also recorded like as “HA switch from primary to secondary, the effective factor of the election is Monitor”:

68	2022/11/09 16:40:11		daemon	HA-monitor-corefile	Stop HA corefile failover.
69	2022/11/09 16:40:09		daemon	HA-Switch	HA switch from primary to secondary, the effective factor of the election is Monitor .
70	2022/11/09 16:40:08		daemon	HA-monitor-corefile	Start HA corefile failover.

Please refer to [What to do when coredump files are truncated or damaged](#) for more detailed description of corefile-ha-failover.

### What is the requirement for heartbeat links?

Verify that heartbeat links are correctly configured and connected:

- Heartbeat interfaces should be dedicated ones, cannot be used as monitor interfaces or reserved management interfaces at the same time
- Ports that currently have an IP address assigned for other purposes (that is, virtual servers or bridges) CANNOT be re-used as a heartbeat link
- The heartbeat interface will be assigned with an IP address within 169.254.0.0/16, so do not configure other network interfaces (including VLANs) with this subnet
- Connect one heartbeat port to the same port number on the other HA group members.
- FortiWeb supports up to 2 heartbeat interfaces, however please make sure that the primary and secondary link is not crossed (that is, the primary heartbeat interface is not connected to the secondary heartbeat interface on the other appliance).
- If a switch is used to connect the heartbeat interfaces, the heartbeat interfaces must be reachable by Layer 2 multicast.

### Does heartbeat work in layer 2 or layer 3 (Network Type)?

Bases on different HA modes and platforms, heartbeat will work in layer 2 or layer 3

- Flat: by default, HA uses ether type 0x8890 to send layer 2 multicast heartbeat packets
- Udp-tunnel: one needs to specify the tunnel-local and tunnel-peer IP address and HA sends heartbeat packets via UDP port 6055 between these two IPs.

Platform	Hardware	VMware	KVM
HA mode supported	Active-Passive Active-Active-Standard Active-Active-High-Volume	Active-Passive Active-Active-Standard Active-Active-High-Volume	Active-Passive Active-Active-Standard Active-Active-High-Volume
Network Type	Flat	Flat, UDP Tunnel (AP & AAHV, Reverse Proxy mode)	Flat, UDP Tunnel (AP & AAHV, Reverse Proxy mode)
Platform	AWS	Azure	OCI
HA mode	Active-Passive Active-Active-High-Volume Manager	Active-Passive Active-Active-High-Volume	Active-Passive Active-Active-High-Volume

		Manager	
Network Type	UDP	UDP	UDP

### Will HA nodes use physical MAC address or virtual MAC address for communication?

The situation is different on different HA modes:

- Active-Passive mode: IP addresses on all traffic ports and VIPs on the primary node will use a virtual mac address formatted like “00:09:0F:A0:CC:02” to reply to a visit.  
The secondary nodes will still use the real-mac until it switches to be the primary node.
- Active-Active-Standard mode: the same as Active-Passive mode.
- Active-Active-High-Volume mode: IP addresses on the physical ports will still use the original mac address, while VIPs will use virtual mac address.

This implementation leads to extra configuration on the hypervisors (ESXI, etc.) to allow communication for such virtualized MAC addresses that do not actually exist on physical ports.

### How to manage HA nodes, especially the secondary nodes via SSH or GUI?

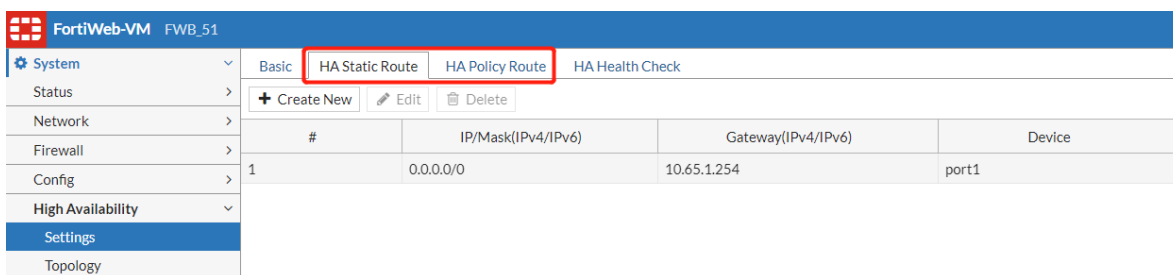
If HA is deployed in active-passive or standard active-active modes, it’s necessary to add a reserved management interface (or interfaces) and HA static/policy route to manage HA nodes, especially the secondary nodes.

- This option is not a MUST for HA setup but is necessary for active-passive and standard active-active modes, because in these two modes, the IP address and other settings on all interfaces will be synchronized to other HA members unless a port is set as “Reserved Management Interface”.
- If the reserved network interfaces are not in the same subnet with the management computer, you need to configure the next-hop gateways in HA Static Route or HA Policy route

CLI:

```
config system ha-mgmt-router-static
config system ha-mgmt-router-policy
```

GUI:



### Does FortiWeb synchronize session information in HA mode?

Session synchronization can be enabled for session fail-over protection, but it’s not supported by all HA modes.

- Session Pickup: Available only in Active-Active-Standard mode.  
Session information will be synchronized from the primary node to other HA members, so if HA failover takes place, the other node elected as the new primary will use the session information to resume connections without interruption.

Note: Only sessions that have been established for longer than 30 seconds will be synchronized.

- Layer 7 Persistence Synchronization: Available only in Active-Passive mode. Actually this feature is not implemented by synchronizing sessions. When this option is on, FortiWeb enforces session persistence between the primary and secondary appliances at the application layer.

## HA trouble-shooting

### Common Troubleshooting Steps

If a high availability (HA) cluster is not behaving as expected, use the following troubleshooting steps to help find the source of the problem:

1. Ensure the physical connections are correct:

- Ensure that the physical interfaces that FortiWeb monitors to check the status of appliances in the cluster (Port Monitor in HA configuration) are in the same subnet.
- Ensure that the HA heartbeat link ports are connected through crossover cables. Although the feature works if you use switches to make the connection, Fortinet recommends a direct connection.

2. Ensure the following HA configuration is correct:

- Ensure that the cluster members have the same Group ID value, and that no other HA cluster uses this value.
- Specify different Device Priority values for each member of the cluster and select the Override option. This configuration ensures that the higher priority appliance (the one with the lowest value) is maintained as the primary as often as possible.

3. Use the following commands to collect status information and diagnose logs for further analysis:

- `get system status / ha` #HA status & basic running config view
- `diagnose system ha` #More detailed HA information
- `execute ha dbver / md5sum / synchronize`
- `diagnose debug application hamain / hasync / hasync-base / hatalk`

<code>diagnose debug application hasync 7</code>	<p>Configures the debug logs for HA synchronization to display messages about the automatic configuration synchronization process, commands that failed, and the full configuration synchronization process.</p> <p>Run on both members of the HA cluster to confirm configuration synchronization and communication between the appliances.</p> <p>The valid range of log level is 0–7, where 0 disables debug logs for the module and 7 generates the most verbose logging.</p> <p>Before you run this command, run the following commands to turn on debug log output and enable timestamps:</p> <pre>diagnose debug enable diagnose debug console timestamp enable</pre>
<code>diagnose debug application hasync-base 7</code>	<p>Configures the debug logs for HA synchronization for L7 persistence. L7 persistence is available only in Active-Passive mode.</p>

diagnose debug application hatalk 7	Configures the debug logs for HA heartbeat links to display messages about the heartbeat signal, HA failover, and the uptime of the members of the HA cluster..
diagnose debug application hamain 7	Configures the debug logs to display the interaction messages between hamain and hatalk (heartbeat), as well as other kernel or function modules that need HA support
diagnose debug application hahlck 7	Configures the debug logs for HA health check messages. HA health check is available only in Standard Active-Active mode.

4. Collect HA related logs:

- System Event log: **Log&Report > Log Access > Event**
- /var/log/gui\_upload/ha\_event\_log #Download from **System > Maintenance > Backup & Restore > GUI File Download/Upload** (will be archived in the debug log in future builds)

### Troubleshooting HA issues when FortiWeb nodes are deployed on Hypervisors - Extra configuration on ESXi for HA deployment

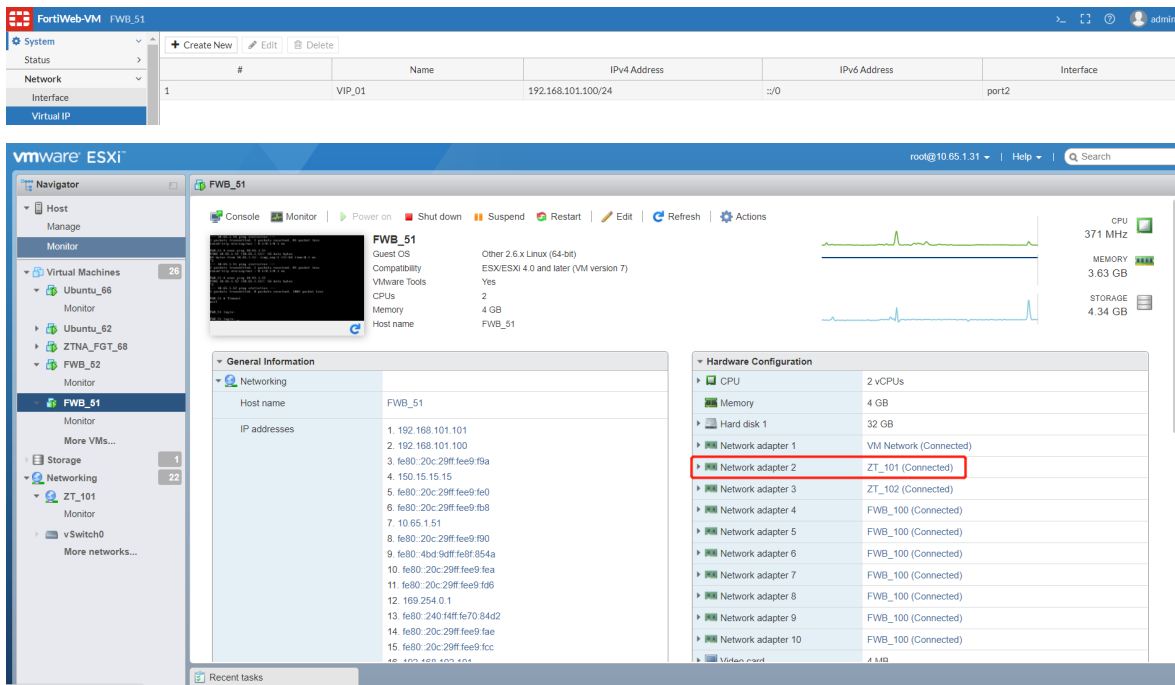
In most cases, traffic ports except the heartbeat and reserved-mgmt ones on FortiWeb will use a virtual MAC address, so in VM ESXi environment such as VMWare ESXi, if you want to visit the IP address or VIP, you'll need to enable the promiscuous mode on the traffic port. Actually you need to enable all three options for ESXi > Networking > Port-Groups > Edit settings > Security > Promiscuous mode, MAC address changes and Forged transmits.

The specific configuration is based on different HA modes:

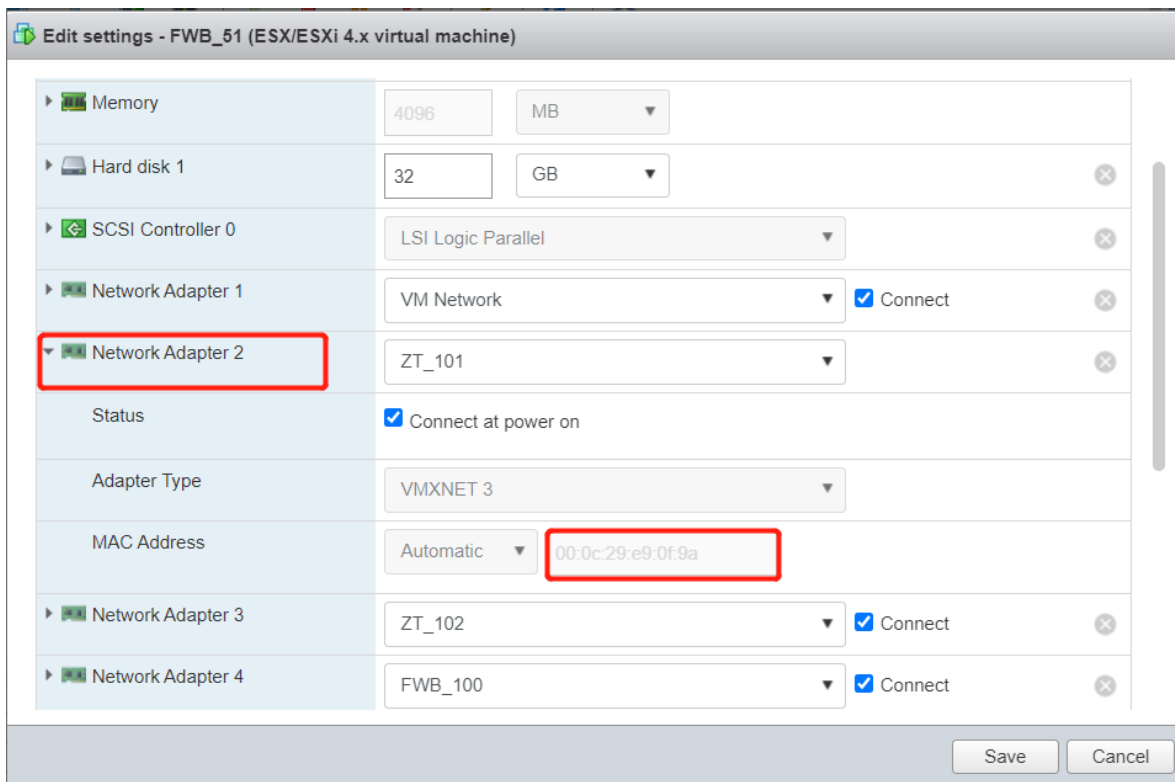
- Active-Passive mode: IP addresses on all traffic ports and VIPs on the primary node will use a virtual mac address formatted like "00:09:0F:A0:CC:02" to reply to a visit, so promiscuous needs to be enabled on all traffic ports. The secondary nodes will still use the real-mac until it switches to be the primary node.
- Active-Active-Standard mode: the same as Active-Passive mode.
- Active-Active-High-Volume mode: IP addresses on the physical ports will still use the original mac address, while VIPs will use virtual mac address, so if just the Interface IP is used as the Virtual Server in Server Policy, promiscuous can be disabled; but if VIPs are created and bound to Server Policy, promiscuous needs to be enabled on the traffic ports.

E.g. HA AS mode in ESXi platform:

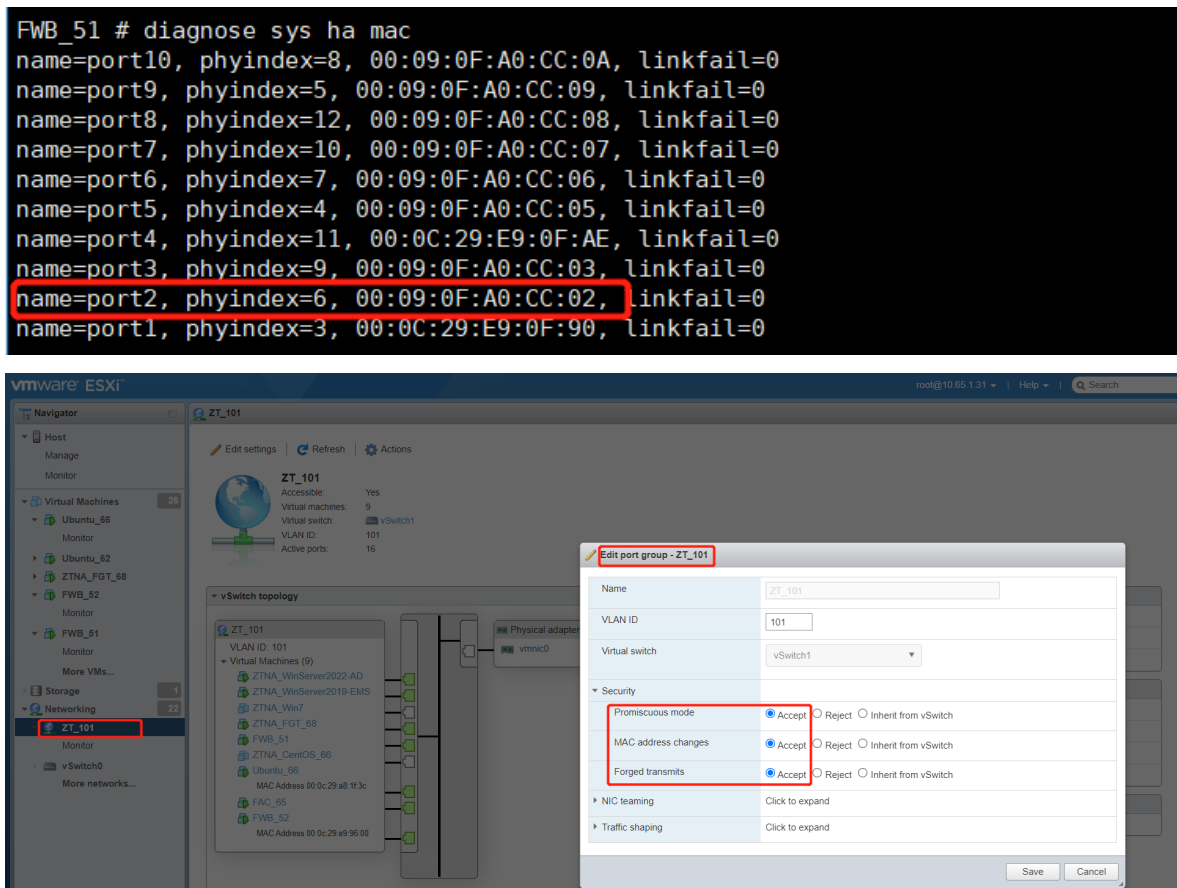
Name	Members	IPv4	IPv4 Access	Status	Link Status	Type	Ref
port11		10.65.1.51/24	HTTPS PING SSH SNMP HTTP FortiWeb Manager	Bring Down	OK	Physical	2
port2		192.168.101.101/24	HTTPS PING SSH SNMP HTTP FortiWeb Manager	HA Monitor	OK	Physical	2
port3		192.168.102.101/24	HTTPS PING SSH SNMP HTTP FortiWeb Manager	HA Monitor	OK	Physical	1
port4		0.0.0/0		HA Heartbeat	OK	Physical	2
port5		0.0.0/0		Bring Down	OK	Physical	0
port6		0.0.0/0		Bring Down	OK	Physical	0
port7		0.0.0/0		Bring Down	OK	Physical	0
port8		0.0.0/0		Bring Down	OK	Physical	0
port9		0.0.0/0		Bring Down	OK	Physical	0
port10		0.0.0/0		Bring Down	OK	Physical	0



By default, port2 (Network Adapter 2) only processes the original MAC address assigned by ESXi: 00:0c:29:e9:0f:9a:



But as HA-AAHV mode is enabled, IPs including the VIP on port2 uses a virtual MAC: 00:09:0f:a0:cc:02.



## HA Status issue 1 - All nodes are Primary

Regarding HA status issues, a typical issue is that both HA nodes are in the primary role.

Follow these steps to troubleshoot:

1. Verify the “4 Sames” HA configuration prerequisite:

The same Platform, same Firmware Version, same Group ID and same Override option.

2. Verify that heartbeat interfaces are configured correctly and properly.

Please refer to above section **HA Key Settings > Heartbeat** part for more details.

4. Test the cables and/or switches in the heartbeat link to verify that the link is functional.

5. Verify that the ports on Monitor Interface are linked up.

6. If the heartbeat link passes through switches and/or routers, you may need to adjust the time required after a reboot to assess network availability before electing the main appliance. To do this, use the command “`set boot-time <seconds_int>`”.

7. Check if CPU usage of HA members are extremely high.

It's rare but if the CPU usage of a certain HA appliance is extremely high, the system may fail to send or receive heartbeat packets, thus causing HA status abnormal too.

8. For debugging logs, use commands “diagnose system ha status” and “diagnose debug application hatakl 7” to check the heartbeat communication between the primary and secondary appliances.

The key point is to guarantee that HA member information for the peer node can be received and is correct.

E.g. the hbdev port10 gets disconnected, the peer HA member FVVM04TM21001050 leaves HA group.

```
FortiWeb # diagnose debug application hatakl 7
FortiWeb # diagnose debug enable
(2021-12-27 22:56:03 hb_port.c:324) Enter Fun : init_hb_ports, port port10, backup
(2021-12-27 22:56:03 hb_port.c:305) HB sockfd for interface (port10) = 9
(2021-12-27 22:56:03 hb.c:139) override old: 1 -> new: 1
(2021-12-27 22:56:03 hb.c:150) MyHB: gid 11, dpri 5, group name Group_AAS, sn
    FVVM08TM21000613
(2021-12-27 22:56:03 hb_timer.c:252) Member(FVVM04TM21001050) is too staleness, need
    to clean it from the ha group ()
(2021-12-27 22:56:03 hb_timer.c:266) Send ha member leave trap, sn:FVVM04TM21001050
(2021-12-27 22:56:03 hb_msg.c:62) Send ha member change, rv 0
(2021-12-27 22:56:03 hb_idx.c:160) Delete member id:FVVM04TM21001050
ha_reader:325 nstd rcv msg group:28
rcv msg from ha, msg_type:FREE          sn:FVVM04TM21001050 id:0
nstd rcv msg from ha, msg_type:3
```

## HA Status issue 2 - Unexpected switch over

When you found HA switchover happened but not sure about the reason, you can try to check the causes with following steps:

### 1. Check the HA primary role election rule

The primary HA role is elected according to these rules:

- If Override is disabled:  
Available ports number (Monitor) > Uptime > Priority > SN
- If Override is enabled:  
Available ports number (Monitor) > Priority > Uptime > SN

Serial numbers are sorted by comparing each character from left to right, where 9 and z are the greatest values, and result in highest placement in the sorted list. Since it's very rare that different nodes have the exact same uptime, SN is rarely compared.

### 2. Check if HA heartbeat links are normal and heartbeat packets can be sent and received normally.

### 3. Check if CPU usage of HA members are abnormal.

If the CPU usage of a HA appliance fluctuates and sometimes reaches 100%, the system may fail to send or receive heartbeat packets from time to time, thus causing HA status unstable.

In above cases, sometimes HA heartbeat packets may lose. One can try to increase the failure detection threshold if a failure is detected when none has actually occurred. For example, during peak traffic times, if the main appliance is very busy, it might not respond to heartbeat packets in time, and the standby appliance may assume that the main appliance has failed.

```
FortiWeb # sho full sys ha
config system ha
    set hb-interval 10      #heartbeat interval, range 1-20 (100ms)
    set hb-lost-threshold 3 #heartbeat threshold for failed, range 1-60
```

end

4. Check HA event logs to find the timeline and causes for HA failover:

Sometimes you may be not sure about the events and causes but just observed an unexpected HA failover, then you can check the HA failover events in these ways/logs.

- Check the Event logs, which include the reasons for HA status changes and can be filtered with “Action: HA-Switch” or other options as below:

**Log & Report > Log Access > Event > Action:** HA-Switch, HA-Synchronize, HA-member-left, HA-member-join, HA-monitor-port.

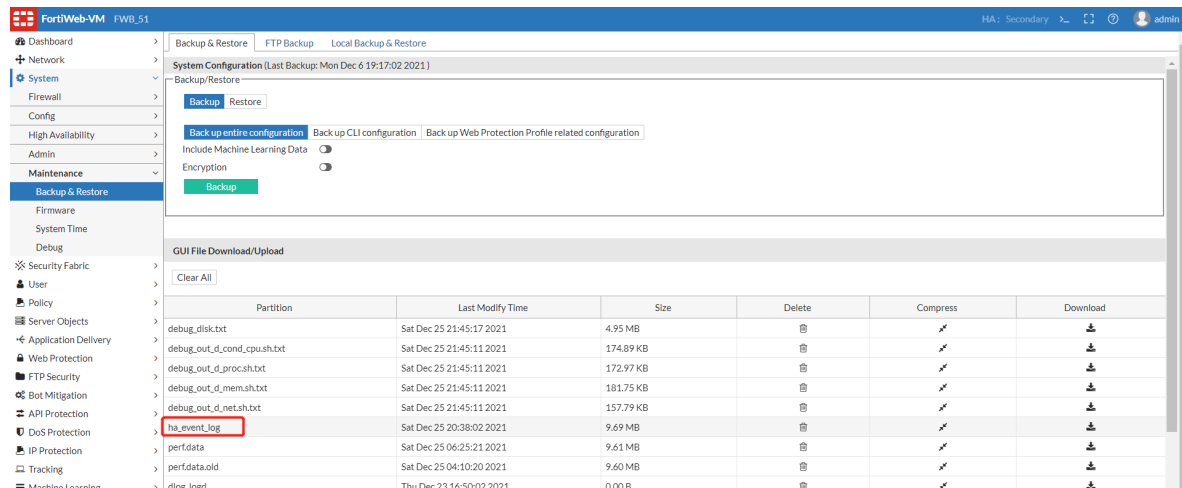
E.g. Below logs show different HA switch events caused by priority changes, monitor ports status changes and uptime comparison.

#	Date/Time	Level	User Inte...	Action	Message
1	2021/12/25 20:38:01	Warning	daemon	HA-Switch	HA switch from primary to secondary, the effective factor of the election is Priority .
2	2021/12/25 20:37:46	Warning	daemon	HA-Switch	HA switch from secondary to primary, the effective factor of the election is Monitor .
3	2021/12/23 16:49:40	Warning	daemon	HA-Switch	HA switch from primary to secondary, the effective factor of the election is Priority .
4	2021/12/23 16:46:30	Warning	daemon	HA-Switch	HA switch from secondary to primary, the effective factor of the election is Monitor .
5	2021/12/23 16:23:24	Warning	daemon	HA-Switch	HA switch from primary to secondary, the effective factor of the election is Priority .
6	2021/12/23 15:27:29	Warning	daemon	HA-Switch	HA switch from master to slave, the effective factor of the election is Age .

- Check more detailed HA file logs via diagnose command “diagnose system ha file-log show” or download the ha\_event\_log via /var/log/gui\_upload/:

E.g. Check HA switch events and causes:

```
FortiWeb # diagnose system ha file-log show | grep switch
2021-12-25 20:37:45 dbg-hamain ha_mode.c:62 Recv ha switch
2021-12-25 20:37:45 dbg-hataalk hb_msg.c:40 Send ha switch, rv 0
2021-12-25 20:37:46 dbg-hamain ha_mode.c:303 In ha mode process, old role
SECONDARY -> new role PRIMARY role changed: 1 switch reason: 1
2021-12-25 20:37:46 dbg-hamain ha_mode.c:315 switch SECONDARY -> PRIMARY
2021-12-25 20:37:46 dbg-hamain ha_mode.c:325 HA switch from secondary to primary,
the effective factor of the election is Monitor .2021-12-25 20:37:46 dbg-
hamain ha_mode.c:101 Send ha mode swith trap, reason:Monitor
2021-12-25 20:38:00 dbg-hamain ha_mode.c:62 Recv ha switch
2021-12-25 20:38:00 dbg-hataalk hb_msg.c:40 Send ha switch, rv 0
2021-12-25 20:38:01 dbg-hamain ha_mode.c:303 In ha mode process, old role PRIMARY
-> new role SECONDARY role changed: 1 switch reason: 2
2021-12-25 20:38:01 dbg-hamain ha_mode.c:342 switch PRIMARY -> SECONDARY
2021-12-25 20:38:01 dbg-hamain ha_mode.c:351 HA switch from primary to secondary,
the effective factor of the election is Priority .2021-12-25 20:38:01 dbg-
hamain ha_mode.c:224 HA device into Secondary mode
```



FortiWeb backend Shell:

```
~# tail -100 /var/log/gui_upload/ha_event_log | grep switch
2021-12-25 20:37:45 dbg-hamain ha_mode.c:62 Recv ha switch
2021-12-25 20:37:45 dbg-hataalk hb_msg.c:40 Send ha switch, rv 0
2021-12-25 20:37:46 dbg-hamain ha_mode.c:303 In ha mode process, old role
SECONDARY -> new role PRIMARY role changed: 1 switch reason: 1
2021-12-25 20:37:46 dbg-hamain ha_mode.c:315 switch SECONDARY -> PRIMARY
2021-12-25 20:37:46 dbg-hamain ha_mode.c:325 HA switch from secondary to primary,
the effective factor of the election is Monitor .2021-12-25 20:37:46 dbg-
hamain ha_mode.c:101 Send ha mode swith trap, reason:Monitor
2021-12-25 20:38:00 dbg-hamain ha_mode.c:62 Recv ha switch
2021-12-25 20:38:00 dbg-hataalk hb_msg.c:40 Send ha switch, rv 0
2021-12-25 20:38:01 dbg-hamain ha_mode.c:303 In ha mode process, old role PRIMARY
-> new role SECONDARY role changed: 1 switch reason: 2
2021-12-25 20:38:01 dbg-hamain ha_mode.c:342 switch PRIMARY -> SECONDARY
2021-12-25 20:38:01 dbg-hamain ha_mode.c:351 HA switch from primary to secondary,
the effective factor of the election is Priority .2021-12-25 20:38:01 dbg-
hamain ha_mode.c:224 HA device into Secondary mode
```

## Traffic drops down in HA environment

Follow below steps to troubleshoot if the application traffic drops down after in HA environment or HA failover takes place:

1. Verify that HA status on both/all members are correct after failover:

- Verify there is only one primary role
- Verify that all HA members have the correct and stable new status  
Referring to the above troubleshooting steps in "Unexpected switch over".

2. Verify that the configuration has been synchronized completely

- Verify that the md5 for SYS & CLI on the primary & secondary nodes via "execute ha md5sum" or "diagnose sys ha confd\_status" on the primary node to see if the configuration are identical

```
FortiWeb # execute ha md5sum
FVVM04TM21001050<Primary>
  SYS: D075A17ADDD372423263F4B31ACB8C7F
  CLI: 2D1DE97C0C1F1968FB4BFCE530E52A1B
FVVM08TM21000613<Secondary>
```

```
SYS: D075A17ADDD372423263F4B31ACB8C7F
CLI: 2D1DE97C0C1F1968FB4BFCE530E52A1B
```

- Verify that the Sync status on GUI top menu is “In Sync” (after 6.4 builds)

### 3. Verify that the requests are received by the new primary (former secondary) appliance:

- Verify that monitor ports on the former primary and the new primary appliance are configured and connected symmetrically
- Verify that the route entries on upstream routers are configured correctly so that VIPs on FortiWeb are reachable for the clients initiating the request
  - Check if PING can be successful or ICMP request can be captured on the new primary FortiWeb or the upstream router
  - Check if TCP 3-way handshakes can be successfully between the client and the new primary FortiWeb
  - Check if HTTP/HTTPS request can be captured on the new primary FortiWeb or the upstream router
  - If HTTP/HTTPS requests can be received by the new primary FortiWeb, check if the responses are forwarded back to the upstream router or other intermediate network nodes
- If it's HA-AAHV mode, check in the same way to confirm if requests are received by the node to which the VIP is distributed.

**Notes:** Node Allocation and Traffic Distribution are necessary for HA-AAHV mode on non-cloud platforms. VIPs used by server policies must be added into Traffic Distribution accordingly.

Node Allocation and Traffic Distribution are not supported on cloud platforms such as AWS, Azure and GCP, so GUI tabs are not available.

### 4. Verify the traffic distribution for Standard Active-Active (AAS) mode:

In AAS mode, the primary appliance distributes the traffic to all the HA members (including itself) according to the load-balancing algorithm. The primary node starts distributing traffic to other nodes from the TCP handshake stage, and will only maintain a distribution table to guarantee the following traffic in the same connection is distributed to the same node, but not maintain sessions between the clients and the primary node itself.

So in this situation, if traffic is distributed to a secondary node, troubleshooting needs to be performed on both the primary node&distributed secondary nodes:

- Capture packets to check if TCP SYN from client is received by the secondary node;
- Capture packets to check if TCP SYN ACK from the secondary node is received by the primary node;
- Capture packets to check if TCP SYN ACK from the secondary node is forwarded out to client by the primary node;
- Capture packets to check if SSL/TLS session can be established between the client and the secondary node in the same way;
- Capture packets to check if HTTP traffic is processed by the secondary node in the same way.

The below steps are the detailed troubleshooting methods for some of the above typical network problem after switch over:

### 5. Check if the VIP address is bound to the corresponding interface on the primary FortiWeb node

```
~# ip addr show port2
6: port2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq qlen 1000
   link/ether 00:09:0f:a0:2c:02 brd ff:ff:ff:ff:ff:ff
   inet 192.168.101.101/24 brd 192.168.101.255 scope global port2
       valid_lft forever preferred_lft forever
   inet 192.168.101.100/24 brd 192.168.101.255 scope global secondary port2
```

```

        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fee9:9600/64 scope link
        valid_lft forever preferred_lft forever
FortiWeb_52 # show system interface port2
config system interface
    edit "port2"
        set type physical
        set ip 192.168.101.101/24
        set allowaccess ping ssh snmp HTTP HTTPS FortiWeb-manager
    config secondaryip
    end
    config classless_static_route
    end
next
end

FortiWeb_52 # show system vip
config system vip
    edit "VIP_01"
        set vip 192.168.101.100/24
        set interface port2
        set index 1
    next
end

```

6. Verify that after switch over, the upstream router has its ARP table (or the switch refreshed its MAC table) refreshed via gratuitous ARP sent out by the new primary FortiWeb node.

Both IP addresses on ports and VIPs will send gratuitous ARP. It's better to check the ARP table on the upstream router, or the MAC table on the upstream switch.

7. Verify that network cables are working with the correct speed & duplex on the new primary FortiWeb node.

You can check the interfaces on FortiWeb with the below backend command or on the peer router/switch with corresponding diagnose commands.

```

~# ethtool port1
Settings for port1:
  Supported ports: [ TP ]
  Supported link modes:   1000baseT/Full
                        10000baseT/Full
  Supported pause frame use: No
  Supports auto-negotiation: No
  Supported FEC modes: Not reported
  Advertised link modes:  Not reported
  Advertised pause frame use: No
  Advertised auto-negotiation: No
  Advertised FEC modes: Not reported
  Speed: 10000Mb/s
  Duplex: Full
  Port: Twisted Pair
  PHYAD: 0
  Transceiver: internal
  Auto-negotiation: off
  MDI-X: Unknown
Cannot get wake-on-lan settings: Operation not permitted
Link detected: yes

```

8. If it's VM FortiWebs running in virtual environment, please check the extra configuration on hypervisors according to above section "HA Key Settings > Extra configuration on hypervisors in VM environment"

9. If the issue still cannot be resolved, you can try to:

- Disable HA on the FortiWeb node and check if it can be visited with standalone configuration
- Troubleshoot the issue in standalone mode

## HA Synchronization issues

When you are using the HA function for two or more than two FortiWeb devices and the configurations are different between the devices, the elected Primary device will synchronize almost all the configurations (except the hostname, HA priority, etc.) and some system files to other Secondary devices. Normally, the devices will get into the same HA group, and keep in sync, so the HA devices will work as what you want.

The basic synchronization principles:

- HA group uses the heartbeat link to automatically synchronize most of their configuration and occurs immediately when an appliance joins the group
- During the synchronization process after an appliance just joins HA, its HA status will be INIT. If the first sync fails, the primary will attempt to sync again for another 3 times (total 4 times). If the appliance stays in the INIT status for a long time, it mostly indicates a synchronization failure. After the first complete & successful sync, further configuration sync will be executed in every 30 seconds and just based on configuration diffs.
- After HA is established, each HA member will generate a MD5 for SYS files and CLI config files. These two MD5 will be identical if the configuration & data are synchronized successfully between the primary and secondary appliances. The secondary appliance will receive both the synchronized configuration/data and the primary device's two MD5 values; after it loads the synchronized configuration, it will calculate its own MD5 values and compare with the primary node's, then judge if the synchronization is successful and complete
- Configuration synchronization uses TCP on port number 6011 and a reserved IP address (169.254.0.0/16)
- Synchronization includes: (show in "diagnose sys ha sync-stat" and "diagnose system ha file-stat")
  - Core CLI-style configuration file (/migadmin/etc/cli\_syntax.xml -> ha\_not\_sync="2" will not sync)
  - X.509 certificates, certificate request files (CSR), and private keys
  - HTTP error pages
  - FortiGuard IP Reputation Service database
  - FortiGuard Security Service files (attack signatures, predefined data types & suspicious URLs, known web crawlers & content scrapers, global allow list, vulnerability scan signatures)
  - FortiGuard Antivirus signatures
  - Geography-to-IP database
- Configuration settings that are not synchronized:
  - Network interface (IP addresses on interfaces in Active-Active-High-Volume mode, and IP address on the reserved-mgmt-interface in Active-Passive & Active-Active-Standard modes are NOT synchronized)
  - V-zone (Configured in Transparent Proxy & Transparent Inspection modes)
  - Firewall (Configured in Active-Active-High-Volume mode)
  - Static/Policy route (Configured in Active-Active-High-Volume mode)
  - HA static/policy route (Configured in Active-Passive and standard Active-Active modes)

- RAID level
- HA active status and priority
- Data that is not synchronized: (Please check the Admin Guide for details)
  - HTTP sessions (In Active-Active-Standard mode, session pickup can be enabled)
  - HTTPS sessions
  - Log messages
  - Generated reports
  - Machine Learning data: will not be synchronized in Active-Active-Standard & Active-Active-High-Volume mode; but will be synchronized in Active-Passive mode in every 10 minutes)

However, some errors could happen and the devices could not be in sync status at some times.

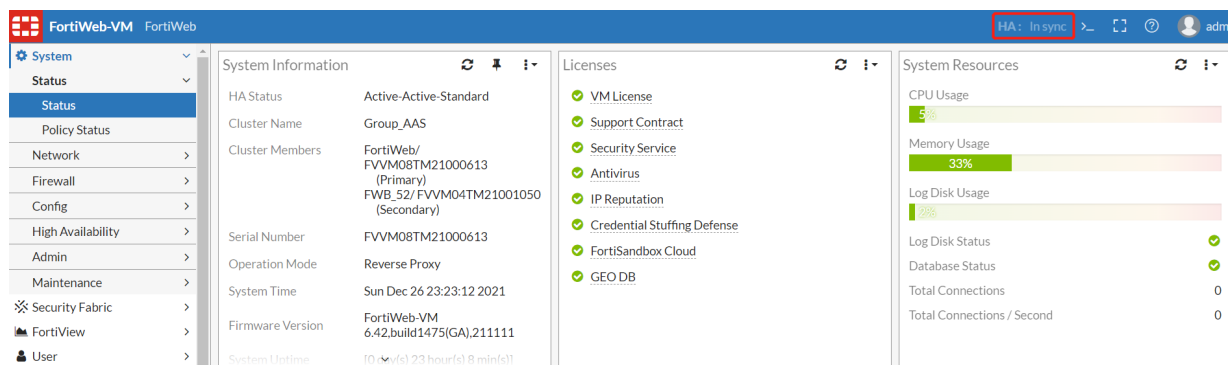
FortiWeb provides several methods to troubleshoot the HA configuration synchronization issues:

1. Verify that the heartbeat packet Ethertype is correctly configured and allowed by intermediate switches via which if the heartbeat interfaces of HA members are connected.

- HA uses Ethertype 0x8893 to synchronize HA configuration, so the switches used to connect heartbeat interfaces require a configuration that allows them.
- The Ethertype for level2 frames can be configured between 0x8890 and 0x8893.
- You can use “diagnose network sniffer <hbdev>” to capture packets and see if such packets are sent & received from both HA nodes

2. Use the HA Diff Toolbar to check the HA status and configuration Diff on GUI.

On 6.4.1 and later releases, FortiWeb adds a new toolbar to show the HA sync status in the toolbar. If the HA devices are not synchronized, the menu will be clickable. After you click the ‘Not sync’ menu, it will prompt one slide page on the right and show the HA differences between the Primary and first different Secondary device. In other words, if you have more than one Secondary devices which are all not synchronized with the Primary device, this new tool will only show the first Secondary difference. After you fix the first Secondary difference, it will show the next difference.



Please note that this HA Diff Tool is only effective on the Primary device.

HA Sync Status on GUI:

Status	Description	Clickable
Standalone	No HA mode enabled and Standalone mode now	No

Status	Description	Clickable
Wait to sync	Found the Secondary device, not sure about the sync status, please wait some minutes to check the sync status	No
In sync	All the HA devices are in sync status	No
Not sync	At least one or more Secondary devices are not sync with the Primary node. You can click this menu and show the differences between Primary device and first different Secondary device	Yes
Secondary	Current HA device is a secondary node	No
INIT	Available on the secondary device when the device just joins HA group and during synchronizing configuration from the primary node	No

**Note:** When the Secondary device joins a HA cluster for the first time, HA status may show as 'Not sync'. You may not get a difference report when clicking 'Not sync' at this time because the secondary device is converting the configuration received from the primary node.

Depending on the size of configuration files, it'll take several minutes to complete converting the configuration.

#### **Example 1: Configurations not sync**

In the figure below, the Virtual IP configurations are different between the two HA devices. You can modify or remove the differences in the Primary device. Otherwise, you need to backup the entire configurations respectively and contact us.

HA: Not sync ⚠ >\_ [?] admin

HA Diff

Context Lines  Range: 1-500

Apply Refresh

Files changed (1)

[/tmp/hadir/ha\\_compare/{ha\\_conf\\_local -> ha\\_conf\\_peer}](#) +2 -2

[/tmp/hadir/ha\\_compare/{ha\\_conf\\_local -> ha\\_conf\\_peer}](#) RENAMED

@@ -283,22 +283,22 @@	
283 set vip 16.8.3.22/24	283 set vip 16.8.3.22/24
284 set interface port7	284 set interface port7
285 set index 1	285 set index 1
286 next	286 next
287 edit "vip3"	287 edit "vip3"
288 set vip 36.33.33.33/24	288 set vip 36.33.33.33/24
289 set interface port7	289 set interface port7
290 set index 2	290 set index 2
291 next	291 next
292 edit "myvip3"	292 edit "myvip3"
293 - set vip 10.10.10.10/24	293 + set vip 10.10.10.11/24
294 - set interface port4	294 + set interface port5
295 set index 3	295 set index 3
296 next	296 next

Return

### Example 2: System files not sync

In the figure below, the files '/data/etc/ssh/mytest' are different between the two HA devices

HA: Not sync ⚠ >\_ [?] admin

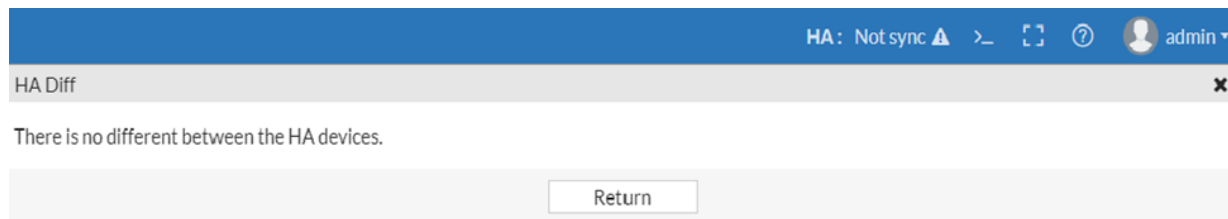
HA Diff

303 set override enable	303 set override enable
304 set hbdev port2	304 set hbdev port2
@@ -5306,21 +5306,21 @@	
5306 filename:/data/etc/m-learning/svm2/svm-xss-gene	5306 filename:/data/etc/m-learning/svm2/svm-xss-gene
5307 filename:/data/etc/m-learning/svm2/svm-xss-gene	5307 filename:/data/etc/m-learning/svm2/svm-xss-gene
5308 filename:/data/etc/saml/shibboleth/service_provider	5308 filename:/data/etc/saml/shibboleth/service_provider
5309 filename:/data/etc/saml/shibboleth/service_prov	5309 filename:/data/etc/saml/shibboleth/service_prov
5310 filename:/data/etc/wvs/profile/	5310 filename:/data/etc/wvs/profile/
5311 filename:/var/log/maxminddb/	5311 filename:/var/log/maxminddb/
5312 filename:/var/log/maxminddb/GeoIPv4_country.mmc	5312 filename:/var/log/maxminddb/GeoIPv4_country.mmc
5313 filename:/var/log/maxminddb/GeoIPv6_country.mmc	5313 filename:/var/log/maxminddb/GeoIPv6_country.mmc
5314 filename:/var/log/logo/	5314 filename:/var/log/logo/
5315 filename:/data/etc/ssh/	5315 filename:/data/etc/ssh/
5316 - filename:/data/etc/ssh/mytest	5316 + filename:/data/etc/ssh/mytest
5317 filename:/data/etc/ssh/ssh_host_dsa_key	5317 filename:/data/etc/ssh/ssh_host_dsa_key
5318 filename:/data/etc/ssh/ssh_host_dsa_key.pub	5318 filename:/data/etc/ssh/ssh_host_dsa_key.pub
5319 filename:/data/etc/ssh/ssh_host_rsa_key	5319 filename:/data/etc/ssh/ssh_host_rsa_key
5320 filename:/data/etc/ssh/ssh_host_rsa_key.pub	5320 filename:/data/etc/ssh/ssh_host_rsa_key.pub
5321 filename:/data/etc/keytab/	5321 filename:/data/etc/keytab/
5322 filename:/data/etc/xml_schema/	5322 filename:/data/etc/xml_schema/
5323 filename:/data/etc/json_schema/	5323 filename:/data/etc/json_schema/
5324 filename:/data/etc/json_schema/json_schema/READ	5324 filename:/data/etc/json_schema/json_schema/READ
5325 filename:/data/etc/xml_wsdl/	5325 filename:/data/etc/xml_wsdl/
5326 filename:/data/etc/cert/tslca/	5326 filename:/data/etc/cert/tslca/

Return

### Example 3: Configurations not sync

In the figure below, although the menu show “Not sync”, when you click it the HA diff page shows “There is no difference between the HA devices.”



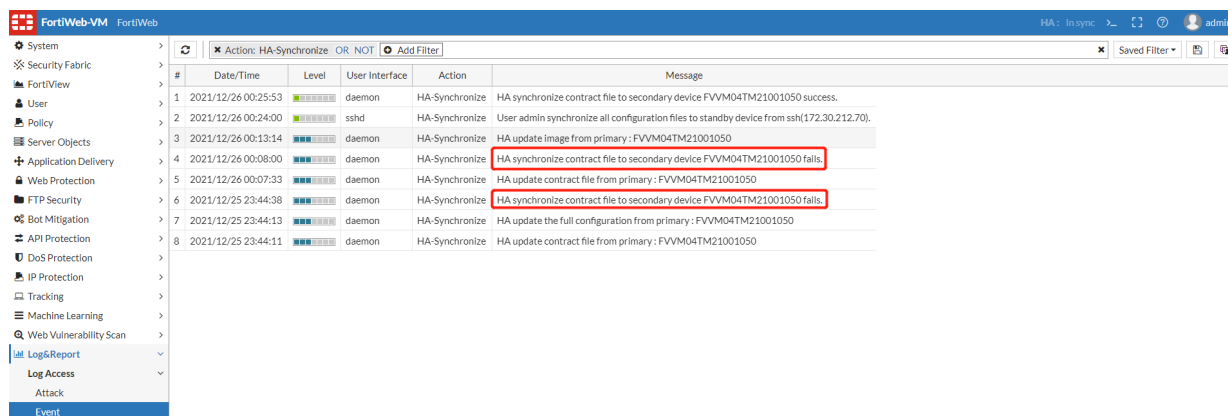
This is because when the Primary device gets the Secondary device not sync status, the Primary device will synchronize the full configurations and some system files to the Secondary, then the Secondary node will receive these files and apply them. This process will also take some time. After the full synchronization, the HA devices are in sync status. Wait a minute, the HA difference menu will show 'In sync' status.

If there are lots of differences between the two HA devices, it could take long time to show the differences. Please wait patiently. If you always fail to get the difference for the not sync status or some errors happen when using the HA difference tool, you have other options to check the HA differences.

3. Check the Event log to confirm that HA synchronization failure events and the cause.

**Log & Report > Log Access > Event > Action: HA-Synchronize.**

E.g. Logs will show synchronization fails as below:



4. Use diagnose commands to check the HA sync status and detailed sync data/files on nodes.

If sync failure occurs, the MD5 values on different nodes might be different, and the `cfg_state` will not be In sync; also, “diagnose system ha sync-stat” will show detailed data or file sync failures.

```
FortiWeb # diagnose system ha confd_status
HA information
Model=FortiWeb-VM 7.00,build0044(Interim),211223, Mode=active-active-standard
Group=11
```

```
HA group member information: is_manage_master=1. cfg_state:In sync
LocalSN: FVVM04TM21001050 confd
member cnt: 2
msg_queue:0 file_queue:0 md5_rep_ignore:0 do_md5sum:39
FVVM04TM21001050: Primary
pending:0 update:0 time:0 sync:0 cfg_state:In sync
SYS: D075A17ADDD372423263F4B31ACB8C7F
CLI: 2D1DE97C0C1F1968FB4BFCE530E52A1B
FVVM08TM21000613: Secondary
pending:198485 update:198486 time:198486 sync:0 cfg_state:In sync
SYS: D075A17ADDD372423263F4B31ACB8C7F
CLI: 2D1DE97C0C1F1968FB4BFCE530E52A1B
```

**Notes:** The MD5 values of both SYS and CLI are the same on the primary and secondary nodes, so both system files and configuration are synchronized successfully.

```
FortiWeb # diagnose system ha sync-config get-status
The sync config status is enable.
```

```
FortiWeb # diagnose system ha file-stat
FortiWeb Security Service:
2022-11-30
Last Update Time: 2021-12-25 Method: Scheduled
Signature Build Number-0.00308
FortiWeb Antivirus Service:
2022-11-30
Last Update Time: 2021-12-25 Method: Scheduled
Regular Virus Database Version-89.08105
Extended Virus Database Version-89.07977
FortiWeb IP Reputation Service:
2022-11-30
Last Update Time: 2021-12-25 Method: Scheduled
Signature Build Number-4.00727
FortiWeb Geodb Service:
Last Update Time: 2021-12-25 Method: Scheduled
GEO Dabase Build Number-Fortiweb-Country-Build0107 2021-12-03
FortiWeb Credential Stuffing Defense Service:
2022-11-30
Last Update Time: 2021-12-25 Method: Scheduled
Signature Build Number-1.00351
System files MD5SUM: D075A17ADDD372423263F4B31ACB8C7F
CLI files MD5SUM: 2D1DE97C0C1F1968FB4BFCE530E52A1B
```

```
FortiWeb # diagnose system ha sync-stat
Image INIT
Config INIT
System INIT
CLI INIT
Signature SUCCESS
```

```
GeoDB          SUCCESS
AV             SUCCESS
IpReputation   SUCCESS
HarvestCredentials SUCCESS
```

HA sync-stat showed above:

Status	Description
INIT	Last synchronization completed; system is ready and waiting for next synchronization.
SENDING	Synchronization is in process; data is sending.
SUCCESS	Success in data sending; synchronization is complete.
SEND_TIMEOUT	Data sending timeout; synchronization is incomplete.

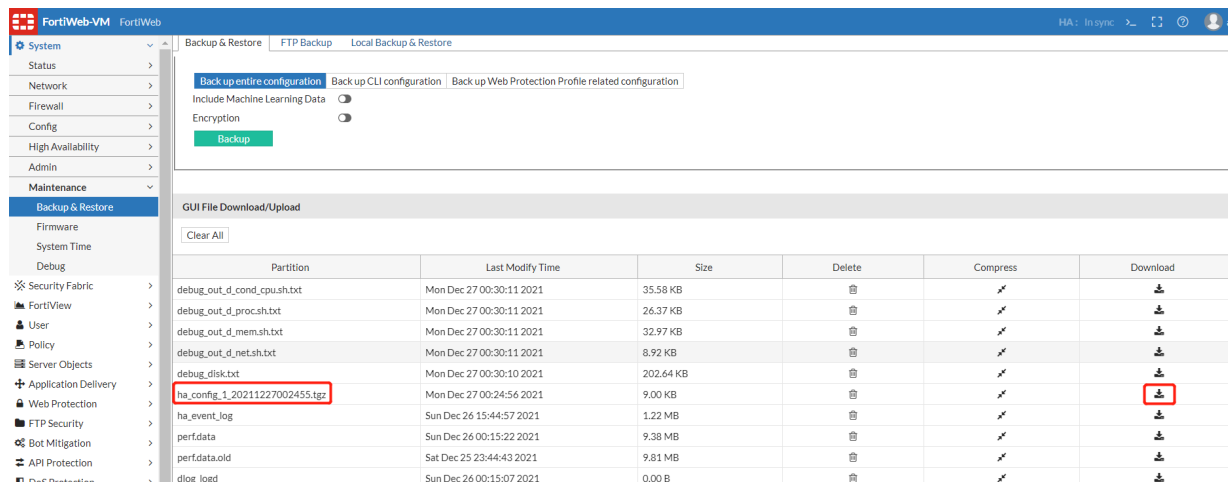
5. Use “diagnose system ha backup-config” to check the synchronized configuration

Use this command to export the configuration file of the HA nodes. It only backs up the configurations synchronized between HA nodes. You can use this command to compare the configuration files between the HA nodes and check which part of the configuration is not synchronized as expected.

```
FortiWeb # diagnose system ha backup-config
<id> please input peer box index.
<1>  Subsidiary unit FVVM08TM21000613
<2>  Subsidiary unit FVVM04TM21001050
FortiWeb # diagnose system ha backup-config 1
Config file /var/log/gui_upload/ha_config_1_20211227002455.tgz has been backed up.
Please download it from System->Maintenance->Backup&Restore by GUI.
```

```
FortiWeb # diagnose system ha backup-config 2
FortiWeb #
```

Then you can check the **System > Maintenance > Backup & Restore** page, and you will see the GUI file Download/Upload part. Please download the files as the below, it will be very helpful for locating the issue.



6. Download the backup configuration files and compare them manually.

When configuration not sync occurs, the primary system will archive the current configuration files & the md5 for each domain. You can check and compare them for details.

Depending on the cause of difference (SYS files or CLI configuration), the archive files will be named as “ha\_config\_cli\_xxx” or “ha\_config\_sys\_xxx”.

Partition	Last Modify Time	Download
ha_config_cli_48C67FB6ACD95A86C53C58E15858A415_1630523297_2_20210901110819.tgz	Wed Sep 1 19:08:21 2021	
ha_config_cli_4411C8285E309E2C6D5ADB3C42673CBE_1630523297_1_20210901110817.tgz	Wed Sep 1 19:08:19 2021	

Partition	Last Modify Time	Download
ha_config_sys_19327B246BE682964D42C4E87E5D018B_1630523819_2_20210901111701.tgz	Wed Sep 1 19:17:04 2021	
ha_config_sys_6162844003160AFFD01446F98CD0D918_1630523819_1_20210901111659.tgz	Wed Sep 1 19:17:01 2021	

As above, "ha\_config\_cli\_\*\_1\_\*.tgz" and "ha\_config\_sys\_\*\_1\_\*.tgz" are SYS files and CLI configuration from the primary node; "ha\_config\_cli\_\*\_2\_\*.tgz" and "ha\_config\_sys\_\*\_2\_\*.tgz" are those from the secondary node. You can download and compare them from the primary node, instead of downloading them respectively from two or more HA nodes.

### 7. Manually execute ha synchronize.

When you find HA sync failures, you can try to execute ha synchronization manually and see if the problem can be resolved.

```
FortiWeb # execute ha synchronize
cli          CLI configurations
sys          System configurations
all          CLI & System configurations
avupd        antivirus definition,scan engine and proxy update
geodb        GEO db file
scanner      scanner_integration file
```

```
FortiWeb # execute ha synchronize cli
starting synchronize with HA primary...
```

The secondary appliance will log the synchronization process:

#	Date/Time	Level	User Interface	Action	Message
6	2021/12/27 00:47:55	system	system	import	Imported machine learning data successfully
7	2021/12/27 00:47:48	daemon	sshd	purge	The cache flush is enabled, flush cache at intervals.
8	2021/12/27 00:47:48	system	system	start	Backup daemon started
9	2021/12/27 00:47:48	system	system	import	Start importing machine learning data
10	2021/12/27 00:47:48	system	system	restore	Restored the configuration success.
11	2021/12/27 00:47:32	daemon	GUI	HA-Synchronize	HA update the cli configuration from primary: FVVM08TM21000613
12	2021/12/27 00:00:21	daemon	HA-Synchronize	HA-Synchronize	HA update virus engine and virus database from primary: FVVM08TM21000613
13	2021/12/27 00:00:10	daemon	HA-Synchronize	HA-Synchronize	HA update contract file from primary: FVVM08TM21000613
14	2021/12/26 23:41:59	daemon	sshd	edit	Command failed: 'Return code -90: CLI parsing error.
15	2021/12/26 23:41:57	daemon	sshd	login	User admin logged in successfully from ssh(172.30.212.73)
16	2021/12/26 23:41:56	daemon	sshd	login	User admin logged in successfully from ssh(172.30.212.73)
17	2021/12/26 23:23:24	daemon	GUI	login	User admin logged in successfully from GUI->HTTPS(172.30.212.73)
18	2021/12/26 22:01:13	daemon	HA-Synchronize	HA-Synchronize	HA update virus engine and virus database from primary: FVVM08TM21000613
19	2021/12/26 22:00:11	daemon	HA-Synchronize	HA-Synchronize	HA update contract file from primary: FVVM08TM21000613
20	2021/12/26 20:00:21	daemon	HA-Synchronize	HA-Synchronize	HA update virus engine and virus database from primary: FVVM08TM21000613
21	2021/12/26 20:00:07	daemon	HA-Synchronize	HA-Synchronize	HA update contract file from primary: FVVM08TM21000613

## Log&Report issues

- Common troubleshooting methods for issues that Logs cannot be displayed on GUI on page 216
- Step-by-step troubleshooting for log display on FortiWeb GUI failures on page 222
- Logs cannot be displayed on FortiAnalyzer on page 224

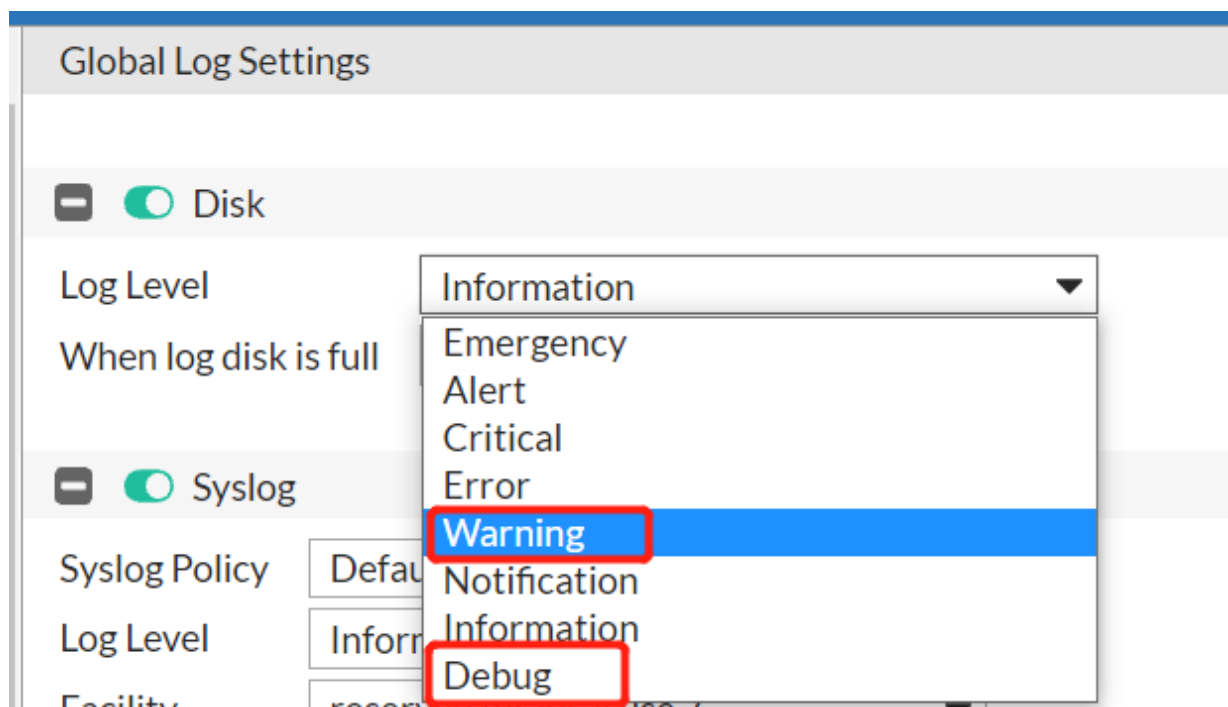
### Common troubleshooting methods for issues that Logs cannot be displayed on GUI

This section summarizes the common troubleshooting methods for log related issues such as Attack/Traffic/Event logs not generated or displayed on GUI. The following sections will use these methods to actually locate specific issues step by step.

1. Check if the security level in log disk is configured properly on CLI or GUI.

Take below configuration for example, only the log messages with a severity of Warning or higher will be recorded.

```
FortiWeb # show full-configuration log disk
config log disk
    set status enable
    set severity warning
    set diskfull overwrite
end
```



Please note: Log level of traffic log is Notification and log level of attack log is Alert.

## 2. Double check if log options are enabled correctly:

- Make sure global log options are enabled via GUI or CLI as below:

```
FortiWeb # show full log event-log
config log event-log
    set status enable
end
FortiWeb # show full log traffic-log
config log traffic-log
    set status enable
end
FortiWeb # show full log attack-log
config log attack-log
    set status enable
end
```

- On 6.4.16, 7.0.0 and later releases, traffic log is disabled by default and can be enabled or disabled per server-policy policy via CLI:

```
FortiWeb # show full-configuration server-policy policy
config server-policy policy
    edit "SP_01"
        set tlog enable
    next
```

## 3. Check if logd, indexd and mysqld work normally in backend:

Sometimes logs fail to be displayed are caused by log related daemons instability such as coredump.

There are several ways to judge if these three daemons every restarted abnormally:

- Check the PID number of related daemons. The PID of logd and mysqld are usually a small 4-digit one like below, so if the PID becomes a big number, it may indicate the daemon ever restarted.
- Check the PID of the 3 daemons several times to make sure they are stable (PID is not changing). If the PID of the daemons is changing, it indicates the daemon ever restarted or the administrator ever executed "execute db rebuild".

```
# ps | grep logd
1479 root      4508 S    /bin/syslogd -n -b 99 -s 500
1480 root      4508 S    /bin/klogd -n
1502 root      308m S    /bin/logd    #1502 is the PID of logd
1729 shell     4508 R    grep logd
# ps | grep indexd
2133 shell     4508 S    grep indexd
18411 root     55840 S    /bin/indexd  #18411 is PID of indexd
# ps | grep mysqld
1584 root      773m S    /bin/mysqld --defaults-file=/data/etc/mysql/my-
    fortiweb.cnf --skip-grant-tables --user=root    #1584 is PID of mysqld
2139 root          0 Z    [mysqld_monitor.]
2328 shell     4508 S    grep mysqld
```

- Another way is to check .NMON files. The PID of daemons are recorded in each .NMON file > TOP. Please refer to [Retrieving system logs in backend system](#) to see how to analyze .NMON files.

Time	PID	%CPU	%User	%Sys	Size	ResSet	ResText	ResData	ShdLib	MinorFault	MajorFault	Command	Threads	IOWaitTime	Interval	CP	WSet
3697	8:27:37	15142	0.24	0.04	0.19	823256	13788	64	131028	9720	6	0	monitor	11	0	0.01	131,092
3698	8:32:37	15142	0.23	0.04	0.19	823256	13788	64	131028	9720	6	0	monitor	11	0	0.01	131,092
3699	8:37:37	15142	0.24	0.05	0.19	823256	13788	64	131028	9720	6	0	monitor	11	0	0.01	131,092
3700	8:42:37	15142	0.24	0.05	0.19	823256	13788	64	131028	9720	6	0	monitor	11	0	0.01	131,092
3701	8:47:37	15142	0.24	0.05	0.2	823256	13788	64	131028	9720	6	0	monitor	11	0	0.01	131,092
3702	8:52:37	5031	4.12	3.02	1.1	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3703	9:02:37	5031	4.1	3	1.1	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3704	9:07:37	5031	3.98	3.02	0.96	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3705	9:12:37	5031	4.06	3.07	0.99	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3706	9:17:37	5031	4.01	2.96	1.05	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3707	9:22:37	5031	4.05	2.99	1.05	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3708	9:27:37	5031	4.02	2.94	1.08	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3709	9:32:37	5031	4.04	2.97	1.07	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3710	9:37:37	5031	4.04	2.96	1.08	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3711	9:42:37	5031	4.1	3	1.09	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3712	9:47:37	5031	4.05	2.95	1.08	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3713	9:52:37	5031	4.06	2.99	1.07	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3714	9:57:37	5031	4.08	2.97	1.11	3730272	1420388	19056	1752736	8736	0	0	mysqld	37	0	0.10	1,771,792
3715	10:02:37	5031	5.56	4.46	1.1	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.14	1,772,512
3716	10:07:38	5031	4.08	3	1.08	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3717	10:12:38	5031	4.09	3.01	1.08	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3718	10:17:38	5031	4.03	2.99	1.04	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3719	10:22:38	5031	4.11	3	1.12	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3720	10:27:37	5031	4.12	2.97	1.14	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3721	10:32:37	5031	4.06	2.98	1.08	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3722	10:37:37	5031	4.01	2.95	1.06	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3723	10:42:37	5031	4.13	3.02	1.11	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.10	1,772,512
3724	10:47:37	5031	5.68	4.54	1.14	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.14	1,772,512
3725	10:52:37	5031	4.42	3.23	1.19	3730272	1421180	19056	1753456	8736	0	0	mysqld	37	0	0.11	1,772,512

- If you find logd daemon of kernel coredump files, please download them and deliver to R&D for further investigation. Another way is to check.  
Please note: logd coredump need to be enabled with the following command in backend shell: (please refer to "Run backend shell commands" in this guide)  

```

/# touch /var/log/debug/logrpt_core_flag
    
```

Please refer to "Customize & Download debug logs" in this guide to see how to download coredump files.

4. Use diagnose commands to check logds outputs:

"diagnose debug application logd" is very useful to help find the cause for log related issues.

Hereby we'll provide several specific case/examples:

- When no useful log is printed out when diagnose is enabled, it usually means no logs are sent to logd by other function modules.

```

FortiWeb # diagnose debug application logd 7
FortiWeb # diagnose debug timestamp enable
FortiWeb # diagnose debug enable

##When either the global traffic-log or per server-policy traffic log option
is disabled, there will be no useful diagnose information:
VM_01 # [Logd][11-22-16:29:12][INFO][_log_try_push][436]: log try push 10
times

##If traffic log is enabled, there will be diagnose info like below:
VM_01 # [Logd][11-22-16:39:27][INFO][_log_process][383]: ##### Recv a traffic
log
[Logd][11-22-16:39:27][INFO][log_format_local_msg][512]: log_id=30001000, msg_
id=000000001063, subtype=HTTPS, url=/
[Logd][11-22-16:39:27][INFO][log_format_local_msg][578]: Local Detail =
v011xxxxdate=2021-11-22 time=16:39:27 log_id=30001000 msg_id=000000001063
device_id=FVVM04TM21000715 vd="root" timezone="(GMT-7:00)Mountain Time
(US&Canada)" timezone_dayst="GMTb+7" type=traffic subtype="HTTPS"
pri=notice proto=tcp service=HTTPS/tls1.2 status=success reason=none
policy="SP_02_RS_SSL" original_src=172.30.213.248 src=172.30.213.248 src_
port=3067 dst=10.159.37.11 dst_port=443 HTTP_request_time=0 HTTP_
response_time=0 HTTP_request_bytes=82 HTTP_response_bytes=927 HTTP_
    
```

```

method=get HTTP_url="/" HTTP_agent="curl/7.78.0" HTTP_retcode=200
msg="HTTPS get request from 172.30.213.248:3067 to 10.159.37.11:443"
original_srccountry="Reserved" srccountry="Reserved" content_switch_
name="none" server_pool_name="Pool_HTTPS" HTTP_host="test.vm02.com:8002"
user_name="Unknown" HTTP_refer="none" HTTP_version="1.x" dev_
id=B039BB143F81FCEBE2C39ACC361EE9411534 cipher_suite="TLS_ECDHE_RSA_WITH_
AES_256_GCM_SHA384"
[Logd] [11-22-16:39:27] [WARNING!] [log_format_msg] [1718]: No srv need to send
[Logd] [11-22-16:39:27] [INFO] [_log_process] [403]: Begin to write disk.
[Logd] [11-22-16:39:27] [INFO] [_log_process] [409]: Begin to write packet.
[Logd] [11-22-16:39:27] [INFO] [_log_add_pkt] [545]: packet log cache 1 logs
stored
[Logd] [11-22-16:39:27] [INFO] [_log_process] [412]: Process done.
[Logd] [11-22-16:39:27] [INFO] [log_disk_push] [988]: push tlog 915
[Logd] [11-22-16:39:27] [INFO] [_log_write_disk] [622]: Open existing log file
'/var/log/fwlog/root/disklog/tlog(2021-11-22-16:39:27).log' with link
[Logd] [11-22-16:39:27] [INFO] [write_cache_to_file] [277]: cur cnt: 3 start pos =
1744, len = 915, currnet len = 2659
[Logd] [11-22-16:39:27] [INFO] [write_cache_to_file] [337]: Write log item Traffic
log 1 msg_id 000000001063 start offset : 2659 length : 915
[Logd] [11-22-16:39:27] [INFO] [write_cache_to_file] [347]: cur_log_cnt : 4, cache
type = Traffic log cache count : 1

```

- Sometimes one may be not sure about the severity of specific attack/traffic logs, you can use the diagnose commands to debug:

```

FortiWeb # diagnose debug application logd 7
FortiWeb # diagnose debug timestamp enable
FortiWeb # diagnose debug enable

```

#### Sample diagnose output:

```

[Logd] [10-18-12:47:02] [WARNING!] [log_disk_write] [921]: Disk log rejected! t:2,
s:1, 4 < 5? h->category : 2

```

**[Cause]** The traffic log level is notification but disk log severity is set as Warning, so logs are not recorded to local disk.

**[Explanation]** Both t:2 & h->category : 2 mean traffic log; s:1 means log is enabled to write to disk; 4 < 5 means current severity level is 5 (Notification), while the current log severity is 4 (Warning).

#### 5. Check backend logs:

Usually diagnose output will show most useful debug information, while sometimes we need to double check or find the root cause via more detailed backend logs or counters.

- /var/log/dlog\_indexd

We can use realtime output with “tail -f” or “grep” with keywords such as “can't connect”, “error” or “mysqld segment fault” to check if there are any obvious defaults in dlog\_indexd.

#### Example 1:

```

"MySQL server has gone away" means mysql server used by logd cannot be connected,
so logs cannot be recorded successfully.
/# tail -f /var/log/dlog_indexd
/var/log/fwlog/root/disklog/alog(2021-11-15-14:01:53).log has no mapping entry
11-16-16:48:28.157212! 2818: dlog_indexer.c(3569)@__mapping_get_tname:
mysqlerr 2 0: MySQL server has gone away
11-16-16:48:28.157218! 2818: dlog_indexer.c(3508)@__mapping_get_maxid:
mysqlerr 1 8: MySQL server has gone away
11-16-16:48:28.157228! 2818: dlog_indexer.c(2210)@_create_log_tab

```

**Example 2:**

```

/# cat /var/log/dlog_indexd | grep mysql
cannot connect mysql, try walk around (ret:0), mysqlerr 1:Can't connect to
local MySQL server through socket '/tmp/mysql.sock' (2)
cannot connect mysql, try walk around (ret:0), mysqlerr 1:Can't connect to
local MySQL server through socket '/tmp/mysql.sock' (2)
cannot connect mysql, try walk around (ret:0), mysqlerr 1:Can't connect to
local MySQL server through socket '/tmp/mysql.sock' (2)

```

- **/var/log/mysql/error.log**

Similarly, we can also check if there is any fault in this log file:

```

/# cat /var/log/dlog_indexd | grep mysql
cannot connect mysql, try walk around (ret:0), mysqlerr 1:Can't connect to
local MySQL server through socket '/tmp/mysql.sock' (2)
cannot connect mysql, try walk around (ret:0), mysqlerr 1:Can't connect to
local MySQL server through socket '/tmp/mysql.sock' (2)
cannot connect mysql, try walk around (ret:0), mysqlerr 1:Can't connect to
local MySQL server through socket '/tmp/mysql.sock' (2)

```

- **/var/log/fwlog/root/disklog**

All attack/event/traffic logs will be written to harddisk after logd received and handled logs sent by other modules. Outputs in this file will help to check if logs have been written to the local disk successfully.

```

/var/log/fwlog/root/disklog# ls -l
-rw-r--r-- 1 root 0 417601 Nov 22 22:27 alog(2021-11-22-
22:26:09).log
lrwxrwxrwx 1 root 0 57 Nov 22 22:26 alog.log ->
/var/log/fwlog/root/disklog/alog(2021-11-22-22:26:09).log
-rw-r--r-- 1 root 0 459145 Nov 23 10:27 elog(2021-11-22-
14:34:23).log
lrwxrwxrwx 1 root 0 57 Nov 22 14:34 elog.log ->
/var/log/fwlog/root/disklog/elog(2021-11-22-14:34:23).log
-rw-r--r-- 1 root 0 46946294 Nov 22 23:13 tlog(2021-11-22-
15:59:23).log
-rw-r--r-- 1 root 0 45953552 Nov 22 23:55 tlog(2021-11-22-
23:13:38).log
lrwxrwxrwx 1 root 0 57 Nov 22 23:13 tlog.log ->
/var/log/fwlog/root/disklog/tlog(2021-11-22-23:13:38).log
#One can just check the soft link for the latest logs.

```

```

/var/log/fwlog/root/disklog# tail -f tlog.log
v011xxxxdate=2021-11-23 time=10:37:11 log_id=30001000 msg_id=000000102564 device_
id=FVVM04TM21000715 vd="root" timezone="(GMT-7:00)Mountain Time(US&Canada)"
timezone_dayst="GMTb+7" type=traffic subtype="HTTPS" pri=notice proto=tcp
service=HTTPS/tls1.2 status=success reason=none policy="SP_01" original_
src=172.30.213.98 src=172.30.213.98 src_port=1941 dst=10.159.26.123 dst_
port=80 HTTP_request_time=0 HTTP_response_time=0 HTTP_request_bytes=82 HTTP_
response_bytes=923 HTTP_method=get HTTP_url="/" HTTP_agent="curl/7.78.0"
HTTP_retcode=200 msg="HTTPS get request from 172.30.213.98:1941 to
10.159.26.123:80" original_srccountry="Reserved" srccountry="Reserved"
content_switch_name="none" server_pool_name="Pool_Single" HTTP_
host="test.vm01.com:7002" user_name="Unknow" HTTP_refer="none" HTTP_
version="1.x" dev_id=03AFBEAE2124AE47968CB4271208410FF9A8 cipher_suite="TLS_
ECDHE_RSA_WITH_AES_256_GCM_SHA384"

```

## 6. Check log related backend counters:

Logd will receive, handle, index and display logs sent by the system processes or specific function modules on GUI, while in abnormal situations it fails to do so. Then it's useful to double check with two backend counters for attack/event/traffic logs.

```

/# cd /proc/miglog/
/proc/miglog# ls
alog dlog elog tlog
/proc/miglog# ls alog/
brief          queue_max_len
/proc/miglog# ls elog/
brief          queue_max_len
/proc/miglog# ls tlog/
brief          queue_max_len
/proc/miglog# ls dlog/      #dlog is for debug only; just ignore it
brief          queue_max_len

/proc/miglog/tlog# cat queue_max_len
163840          #The log queue length; usually fixed
/proc/miglog/tlog# cat brief
total 4
enqueued 4      #New logs are sent from other process/module; one new HTTP/HTTPS
                session usually increase this count by 1
dequeued 4      #New logs received are processed by logd; should be the same as enq
overflow 0      #Not 0 means log overflows caused by too many logs generated; one
                may need check current CPS or disable traffic logs
error 0         #kernel errors that cause logging failures

```

#### 7. Use “execute db rebuild” to rebuild log database :

Use this command to rebuild the FortiWeb appliance's internal database that it uses to store log messages. Please note there are some behavior differences between 6.x and later releases:

- On 6.x builds, db rebuild also erases databases for ML, while on 7.0.0 and later builds, this operation will only clean and rebuild databases for disklog; you can execute redis rebuild to clean ML databases.
- Historical traffic/attack/eventlogs will not be cleared, while one needs to wait several minutes for log index rebuilding - the time is based on log amount;
- In HA mode, executing db rebuild on primary appliance will take effect on all secondary appliances simultaneously on 6.x builds, whereas on 7.0.0 and later builds, rebuilding just impacts local box instead of the whole HA groups.
- With 6.x builds, executing this command will trigger FortiWeb system reboot, while with 7.0.0 and later, this command will not lead to system reboot.

##### 6.x old builds: (Reboot system)

```

FortiWeb# exec db rebuild
This operation will clean and rebuild database for disklog, and will clean
database for ML and Client Management, and it will reboot the system!
Do you want to continue? (y/n)y
rebuilding the database.....

FortiWeb# Connection closing...Socket close.
FortiWeb starts to reboot...

```

##### 6.3.16, 7.0.0 and later: (Not reboot system)

```

FortiWeb # execute db rebuild
This operation will clean and rebuild database for disklog.
Do you want to continue? (y/n)y

```

```
rebuilding the database.....
```

```
FortiWeb #
```

For some cases, it would take a long time to complete database rebuild (depending on how many logs there are existing). While the database is rebuilding, new generated logs are postponed to be written to the database so that the newly generated logs are not available immediately on GUI. The logs are all saved in log files. No log would be lost.

8. Use “**execute formatlogdisk**” to clear the logs from the FortiWeb appliance’s hard disk and reformat the disk.

This operation is more dangerous than “execute db rebuild” because it formats the whole log disk /var/log, so all logs and databases used by varied modules stored on this disk will be cleared.

One point here is, signatures will be cleared so they will be downloaded again after system reboot. (proxyc restart will re-create the signature database)

```
FortiWeb # execute formatlogdisk
```

```
This operation will clear all logs on the Hard Disk and take a few minutes depending
on the disk size!!
```

```
Please backup system configuration and restore it after format operation, otherwise
openapi data will be lost!
```

```
Do you want to continue? (y/n)y
```

```
/# df -h
Filesystem          Size      Used Available Use% Mounted on
/dev/root            472.5M    355.6M   117.0M    75% /
none                 1.1G      176.0K    1.1G     0% /tmp
none                 3.8G       2.9M     3.8G     0% /dev/shm
/dev/sda2            362.4M    270.0M    72.8M    79% /data
/dev/sda3             90.6M     56.0K    85.6M     0% /home
/dev/sda4            30.5G     604.4M   28.4G     2% /var/log
```

## Step-by-step troubleshooting for log display on FortiWeb GUI failures

### Logs could be displayed before but now it’s empty on GUI

Please follow these steps to check the issue:

1. Check if logs files (/var/log/fwlog/root/disklog) are still there.  
If no, check if someone executed formatlogdisk command or deleted log files by mistake; if yes, go next step.
2. Check if mysqld still works:
  - Check “ps | grep mysqld” to verify the daemon is still running and without keep restarting
  - Check error.log & check dlog\_indexd to see if there are error messages; referring to above section 8.1
  - Download error.log & check dlog\_indexd for further investigation
  - You can also try to reboot FortiWeb to see if the log issue may disappear
3. Execute db rebuild. if it still does not work, go to the next step.
4. Diagnose hardware check to see if HD is ok. If no, then go RMA; if yes, keep the debug info and contact support.

## Old logs are available on GUI but no new logs displayed

Some possible causes:

**HA-AA mode:** In this mode, all the FortiWebs are active and requests are distributed over them. Every FortiWeb in this mode processes its own requests and keeps its own logs. If you do not see logs on one FortiWeb, check the logs on the other FortiWebs.

**Database is rebuilding:** Database is rebuilding: For some cases, it would take a long time to complete database rebuild (depending on how many logs there are existing). While the database is rebuilding, newly generated logs are postponed to be written to the database so that the newly generated logs are not available immediately on GUI. The logs are all saved in log files. No log would be lost. Please wait 1 or 2 days to see if there are new logs being generated.

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

**Daemons issues:** try DB rebuild

For other causes, please follow these steps to check the issue:

1. Verify the configuration.
2. Verify that logd and indexd are working normally and stably.
3. Check “diagnose debug application logd” to see if logd is receiving logs.
  - if no, it indicates that FortiWeb function/daemons does not send logs to logd. You need to check the issue of corresponding daemons.
  - if yes, go to the next step.
4. Check “diagnose debug application logd” output to see if logs have been saved to log files, or you can double check log files (tail -f /var/log/fwlog/root/disk/tlog.log, or elog.log/alog.log).
  - if no, check if the log disk is full:  

```
df -h
```
  - Execute hardware health check to see if hard disk is normal.  
if yes, go to next step
5. Check dlog\_indexd to see if logs are processed and delivered to the log database.
6. Collect results of above diagnose steps and download error.log & check dlog\_indexd for further investigation.

## New logs displayed on GUI with delay

1. Check if system cpu usage is very high.  
If CPU usage is very high, logs may not be able to be delivered to logd or written to disk, thus cannot be displayed immediately.
2. Check if database is rebuilding or log version is transferring because of image upgrade (see details above). You could also check dlog\_indexd file in backend shell to see if running `db rebuild` or other daemons occupies resource and delays the new logs.

## Logs cannot be displayed on FortiAnalyzer

Besides being restored in local disk, Attack/Traffic/Event logs can also be delivered to FortiAnalyzer. This section provides troubleshooting methods when Attack/Traffic/Event logs failed to be displayed on FortiAnalyzer (abbreviated as FortiAnalyzer in below section).

The possible causes usually include:

- FortiAnalyzer certificate issue
- TCP connection issue with FortiAnalyzer

### FortiAnalyzer certificate issue

Certificates 'fortinet-subca2001' and 'fortinet-ca2' are necessary on FortiAnalyzer for establishing SSL connection with FortiWeb. If these certs are lost on FortiAnalyzer, FortiWeb will fail to establish connection with FortiAnalyzer and thus fail to send logs to FortiAnalyzer.

#### 1. Basic check

Check if there are 2 certificates 'Fortinet\_SUBCA' & 'Fortinet\_CA' on the FortiAnalyzer (**System Settings > Certificates > CA Certificates**).

If they are not there, download these two certificates from another FortiAnalyzer and import them to the current FortiAnalyzer.

#### 2. Use diagnose commands to check and analyze certificate issues.

##### On FortiWeb

```
diagnose debug application offtp 7
diagnose debug enable
```

The following errors indicates failing to establish SSL connection between FortiWeb and FortiAnalyzer:

```
[OFTP][DEBUG](oftp_async.c:386): oftp_auth_send: auth send done fd=14...
[OFTP][DEBUG](oftp_async.c:420): oftp_auth_rcv: fd=14, buf_pos=0,buf_len=12
[OFTP][DEBUG](oftp_async.c:429): oftp_auth_rcv: read again : errno=Resource
temporarily unavailable
```

##### On FortiAnalyzer

```
# diagnose debug application offtpd 8
# diagnose debug enable
```

The following message indicates FortiAnalyzer certificate verification failed because the necessary CA cert (CN=fortinet-ca2) is not available on the FortiAnalyzer.

FortiWeb sends its cert (CN = FortiWeb) to FortiAnalyzer for auth. This cert is signed by an intermediate CA (fortinet-subca2001) and the root CA (fortinet-ca2). FortiAnalyzer needs the 2 CA certs to verify the received cert.

```
[__verify_callback:475] VERIFY ERROR: depth=2, error=self signed certificate in
certificate chain: /C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Certificate
Authority/CN=fortinet-ca2/emailAddress=support@fortinet.com
[__SSL_info_callback:310] SSL Alert write: fatal unknown CA
[__SSL_info_callback:320] error
[__SSL_info_callback:334] Error error:1417C086:SSL routines:tls_process_client_
certificate:certificate verify failed
```

```
[OFTP_try_accept_SSL_connection:1686 192.168.14.20] SSL accept failed
```

The solution is to download these two CA certificates (CA\_Cert\_1 & CA\_Cert\_2) and import them to the FortiAnalyzer (**System Setting > Certificates > CA Certificates**).

## TCP connection issue with FortiAnalyzer

Long time after FortiWeb sends logs to FortiAnalyzer, sometimes we may encounter the issue that FortiAnalyzer cannot receive new logs from FortiWeb.

1. Use diagnose commands on FortiWeb to analyze:

```
diagnose debug application oftp 7
diagnose debug enable
```

Logs are not sent out and the queue is full if seeing the following:

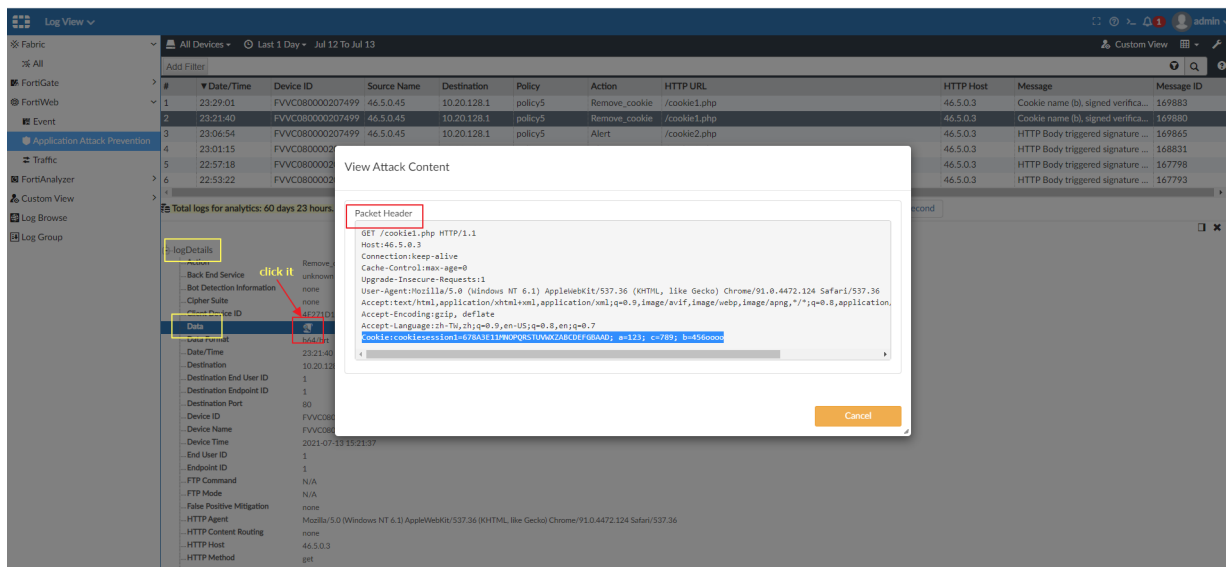
```
[OFTP][WARN](log_oftp.c:1006): queue[IP_ADDRESS] full: fd=14, discard oldest one!
```

2. Capture packets on FortiWeb corresponding interface (the interface connecting to FortiAnalyzer), and in the packets there might be.
  - Many [TCP ZeroWindow] (Win=0) tagged to TCP ACK packets sent from FortiAnalyzer to FortiWeb. It means FortiAnalyzer is informing FortiWeb to stop sending data because full cache (Win=0) on FortiAnalyzer.
  - Many TCP Dup Ack from FortiAnalyzer and TCP Retransmission from FortiWeb after FortiWeb sent TLS application data to FortiAnalyzer. It means FortiWeb sent the logs but received no ACK from FortiAnalyzer. Suggest to reboot FortiAnalyzer to re-establish new connection between FortiWeb and FortiAnalyzer.

## Packet log of attacks is enabled on FortiWeb but they are not displayed on FortiAnalyzer

When a feature is enabled in FortiWeb' GUI **Log&Report > Log Config > Other Log Settings > Retain Packet Payload For**, the attack packet's payload that buffered and parsed by HTTP parser will be displayed in attack logs and sent to FortiAnalyzer.

It's an unobvious place on FortiAnalyzer to see such packet payload. Please check **FortiAnalyzer > Log View > FortiWeb > Application Attack Prevention > log detail of an attack log**. Packet headers and raw data are available by clicking the Data icon.



## Replacement message

- How does Support AJAX Requests in Replacement Message work? on page 226
- Can we add an exception for Replacement Message > Support JAX Requests? on page 227

## FAQ

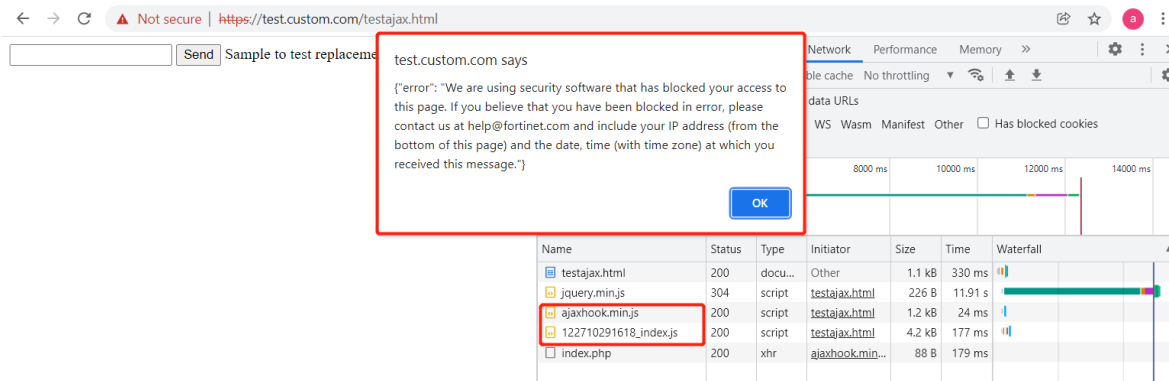
### How does Support AJAX Requests in Replacement Message work?

You can enable Replacement Message for AJAX requests to respond to a AJAX request, and configure the AJAX block page message. You must enable it by going to **System > Config > Feature Visibility** first.

The replacement message for AJAX requests is different from the other replacement messages:

- If **Support AJAX Requests** is enabled and the response Content-Type is text/html and also the response status code is 200, when FortiWeb receives responses from the backend server, it will insert two .js scripts into the HTML response:
  - ajaxhook.min.js
  - 122710291618\_index.js
- Once the clients call AJAX functions open() and send(), “122710291618\_index.js” will hood the request and insert “X-FortiWeb-AJAX-BLOCK” into the request header;
- When FortiWeb gets the request with the “X-FortiWeb-AJAX-BLOCK” header, it will record this, and then remove the “X-FortiWeb-AJAX-BLOCK” header from the request and forward the request to backend servers;
- If both requests and responses comply with all rules on FortiWeb, there’s nothing to do and everything works fine. But if either requests or responses violate any one rule, and also FortiWeb needs to return an error page to clients, FortiWeb will insert an HTTP “X-FortiWeb-AJAX-REPONSE” header into the returned error page.

- When clients receive AJAX responses, "122710291618\_index.js" will hood the responses and check them. If there's "X-FortiWeb-AJAX-REPONSE" in the header, the error page message will be alerted in GUI. On the contrary, no "X-FortiWeb-AJAX-REPONSE" in the header means normal response.



So, actually even if "Support AJAX Requests" is disabled, the "AJAX block" function still works. The only problem is that it is no longer so user-friendly. That means there would be no conspicuous GUI prompt when the AJAX requests are blocked.

### Can we add an exception for Replacement Message > Support JAX Requests?

There have been customer issues reporting that the target URL cannot be visited due to conflict between our injected .js scripts and the customer's source code of the webpage. Sometimes it's hard to locate the root cause from these customer pages or 3rd-party code.

The latest build 7.0.0 provides an enhancement that one can add a URL Access Rule or IP List to bypass the injection of such .js scripts. In this case, the AJAX block function still works, while the two .js scripts will not be injected by FortiWeb, thus the client browser will not prompt a warning message even if the AJAX request is blocked.

# Diagnose hardware issues

---

<b>Using diagnose commands</b> .....	<b>228</b>
<b>Diagnosing Power Supply issues</b> .....	<b>229</b>
<b>Diagnosing hard disk issues</b> .....	<b>229</b>
<b>Diagnosing SSL Card issues</b> .....	<b>231</b>
<b>Diagnosing NIC issues</b> .....	<b>234</b>

## Using diagnose commands

Use diagnose commands to check and analyze hardware related issues:

```
FortiWeb # diagnose hardware
bypass      bypass
check       check
cpld        cpld
cpu         cpu
fail-open   fail-open
harddisk    harddisk
interrupts  interrupts
logdisk     logdisk
mem         mem
nic         nic
raid        raid
raid-card   raid-card
sysinfo     sysinfo
```

```
FortiWeb # diagnose hardware check all
*****
CPU check      Pass
core-number    Pass      4
cpu-number     Pass      1
frequence      Pass     3564
cache-size     Pass     6144
model-name     Pass     Intel(R) Core(TM) i3-8100 CPU @ 3.60GHz

*****
*****
Memory check   Fail
Total-size    Fail     8097512
frequence      Pass     1600
*****
*****
logdisk check  Pass
size           Pass     468
```

```

disk-number    Pass    1
*****
*****
NIC check      Pass
num            Pass    8
Giga nic num   Pass    8
10G nic num    Pass    0
*****

```

## Diagnosing Power Supply issues

Use these tools to check and diagnose possible power supply issues:

Check hard disk status

```

FortiWeb # execute sensors-list

===== Power Module 1 =====
Power Module Status: power up

===== Power Module 2 =====
Power Module Status: power down

```

## Diagnosing hard disk issues

### How do I set up RAID for a replacement hard disk?

The procedures applies to all models except 100D, 400B, 400C, and 400D.

1. Power off the FortiWeb.
2. Remove the hard disk from FortiWeb and install the new hard disk.
3. Power on the FortiWeb.
4. Use the following command to initialize RAID:

```
execute create-raid level raid1
```

5. Enter y to confirm the initialization.

FortiWeb reboots and starts the RAID initialization. The process can take a few hours to complete.

6. Use the following command to check the RAID status:

```
diagnose hardware raid list
```

If the process is successful, a message similar to the following is displayed:

```

FortiWeb # diagnose hardware raid list
level  size(M)  disk-number
raid1  1876242   0 (OK),1 (OK)

```



**5. Check filesystem mount status:**

```
FortiWeb # diagnose system mount list
Filesystem          1M-blocks      Used Available Use% Mounted on
/dev/ram0            473            310      162    65% /
none                1164           31       1132    2% /tmp
none                3880           3        3877    0% /dev/shm
/dev/sdb1           362            254       89    74% /data
/dev/sdb3           91             0         86    0% /home
/dev/sda1          449651         7771     418971  1% /var/log
```

## Diagnosing SSL Card issues

Collect below information for further analysis:

**1. Diagnose commands for hardware SSL card:**

```
FortiWeb# diagnose hardware check sslcard
  Ssl card intel check    Pass      #intel card
FortiWeb # diagnose hardware check sslcard
  Ssl card cp9 check     Pass      #cp9 card

##After v5.85, ssl card status can be shown with:
FortiWeb# diagnose debug sslhardwarestatus show
proxyd using cp9 engine      #cp9 card works
Or
FortiWeb# diagnose debug sslhardwarestatus show
proxyd not using engine      #cp9 card does not work well

FortiWeb # diagnose hardware cavium3 status
Or
FortiWeb # diagnose hardware cp9 status
Tue Jan 18 22:07:53 2022
kxp[0]:{0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:}
kxp[1]:{0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:}
vpn[0]:{0:0:0:0:}
vpn[1]:{0:0:0:0:}

##Below commands are available but might be removed soon
FortiWeb # diagnose hardware cp9 test 1
cp_uio: Detect KXP device[0]
cp_uio: Detect KXP device[1]
cp_uio: Detect VPN device[0]
cp_uio: Detect VPN device[1]
Testing kxpvpn memory...
  num 1          alloc 1 done
Done
Testing RNG interface(bytes: 4080)...
Done
Testing BN_mod_exp interface...
  Testing BN_mod_exp mod 1K
  Done
  Testing BN_mod_exp mod 2K
  Done
  Testing BN_mod_exp mod 3K
  Done
```

```
Testing BN_mod_exp mod 4K
    1.0 ops/s   0.0 MB/s
Done
Done
Testing RSA_mod_exp interface...
Testing RSA_mod_exp mod 1k
Done
Testing RSA_mod_exp mod 2k
Done
Testing RSA_mod_exp mod 3k
Done
Testing RSA_mod_exp mod 4k
Done
Done
Testing ssl3_generate_master_secret...
Done
Testing ssl3_setup_key_block...
    1.0 ops/s   0.0 MB/s
Done
Testing tls_generate_master_secret...
Done
Testing tls_setup_key_block...
Done
Testing ECSKEY(NID:415, prime256v1)...
Done
Testing ECSKEY(NID:715, secp384r1)...
Done
Testing ECSKEY(NID:716, secp521r1)...
    1.0 ops/s   0.0 MB/s
Done
Testing ECSIGN(NID:415, prime256v1)...
Testing ECSIGN(NID:715, secp384r1)...
Testing ECSIGN(NID:716, secp521r1)...
Testing ECVERIFY(NID:415, prime256v1)...
Testing ECVERIFY(NID:715, secp384r1)...
    1.0 ops/s   0.0 MB/s
Testing ECVERIFY(NID:716, secp521r1)...
Testing AES interface...
Done
Testing DES interface...
Done
Testing 3DES interface...
Done

>>>> System Memory <<<<
block[128]:    2048/2048
block[256]:    2048/2048
block[512]:    2048/2048
block[1024]:   10240/10240
block[2048]:   10240/10240
block[4096]:   10240/10240
block[8192]:   8192/8192
block[16384]:  2048/2048
block[32768]:  2048/2048
Size:         237312 Mbytes

>>>> Status <<<<
```

```

kxp[0]:{0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:}
kxp[1]:{0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:}
vpn[0]:{0:0:0:0:}
vpn[1]:{0:0:0:0:}
RNG                1          0 0
SSL3_GENMS         1          0 0
SSL3_GENKM         1          0 0
TLS_GENMS          1          0 0
TLS_GENKM          1          0 0
PKCE_1024          1          0 0
PKCE_2048          1          0 0
PKCE_4096          2          0 0
CRT_PARAM_1024     1          0 0
CRT_PARAM_2048     1          0 0
CRT_PARAM_4096     2          0 0
CRT_1024           1          0 0
CRT_2048           1          0 0
CRT_4096           2          0 0
EC_SIGN            3          0 0
EC_VERIFY          3          0 0
ECSKEY             3          0 0
NID_aes_128_sha1   1          0 0
NID_des_ede3_cbc   1          0 0
NID_des_cbc        1          0 0

```

2. If you doubt that the hardware SSL card has some problem, you can disable it and try if the software SSL works well with below command:

```

##Enable high-compatibility-mode will turn off hardware SSL card
FortiWeb# dia de sslhardwarestatus show
proxyd using intel engine
FortiWeb # config server-policy setting
FortiWeb (setting) # set high-compatibility-mode enable
FortiWeb (setting) # end
high compatibility mode:This operation will restart proxyd and clear the current
connection!
Do you want to continue? (y/n)y
FortiWeb # show server-policy setting
config server-policy setting
    set high-compatibility-mode enable
end
FortiWeb # diagnose debug sslhardwarestatus show
proxyd not using engine

```

3. Check more detailed information in dmesg or /var/log/dmesg/kern.log:

```

[ 50.617068] Loading QAT CONTIG MEM Module ...
[ 50.893620] c6xx 0000:1a:00.0: qat_dev0 started 8 acceleration engines
[ 51.508620] c6xx 0000:1b:00.0: qat_dev1 started 8 acceleration engines
[ 51.859112] igb 0000:02:00.0 mgmt1: igb: mgmt1 NIC Link is Up 1000 Mbps Full
Duplex, Flow Control: RX
[ 51.862020] QAT: Stopping all acceleration devices.
[ 51.862029] c6xx 0000:1a:00.0: qat_dev0 stopped 8 acceleration engines
[ 51.862324] c6xx 0000:1a:00.0: Resetting device qat_dev0
[ 51.862325] c6xx 0000:1a:00.0: Function level reset
[ 51.965722] c6xx 0000:1b:00.0: qat_dev1 stopped 8 acceleration engines
[ 51.965811] IPv6: ADDRCONF(NETDEV_CHANGE): mgmt1: link becomes ready
[ 51.966034] c6xx 0000:1b:00.0: Resetting device qat_dev1
[ 51.966034] c6xx 0000:1b:00.0: Function level reset
[ 53.071493] c6xx 0000:1a:00.0: Starting acceleration device qat_dev0.

```

```
[ 53.334619] c6xx 0000:1a:00.0: qat_dev0 started 8 acceleration engines
[ 53.688343] c6xx 0000:1b:00.0: Starting acceleration device qat_dev1.
[ 53.951619] c6xx 0000:1b:00.0: qat_dev1 started 8 acceleration engines
```

## Diagnosing NIC issues

Sometimes diagnosing NIC issues is important, especially for hardware FortiWeb appliance.

### 1. Use diagnose command to check and analyze NIC related issues:

```
FortiWeb # diagnose hardware nic list port9
driver                igb
version              5.6.0-k
firmware-version     3.29, 0x8000021a
bus-info             0000:85:00.0

Supported ports:      [ TP ]
Supported link modes: 10baseT/Half 10baseT/Full
                    100baseT/Half 100baseT/Full
                    1000baseT/Full

Supported pause frame use: Symmetric
Supports auto-negotiation: Yes
Supported FEC modes:   Not reported
Advertised link modes: 10baseT/Half 10baseT/Full
                    100baseT/Half 100baseT/Full
                    1000baseT/Full

Advertised pause frame use: Symmetric
Advertised auto-negotiation: Yes
Advertised FEC modes:   Not reported

Speed:               1000Mb/s
Duplex:              Full
Port:                Twisted Pair
PHYAD:               1
Transceiver:         internal
Auto-negotiation:    on
MDI-X:               off (auto)
Supports Wake-on:    pumbg
Wake-on:              g
Current message level 0x00000007 (7)
Link detected        yes

Link encap           Ethernet
HWaddr              08:35:71:11:65:BB
INET addr            0.0.0.0
Bcast                10.52.255.255
Mask                 255.255.0.0
FLAG                 UP BROADCAST RUNNING MULTICAST
MTU                  1500
Metric               1
Outfill              538970656
Keepalive            538976266

Memory              fbd80000-fbdfffff
```

---

RX packets	1
RX errors	0
RX dropped	1
RX overruns	0
RX frame	0
TX packets	148
TX errors	0
TX dropped	0
TX overruns	0
TX carrier	0
TX collisions	0
TX queuelen	1000
RX bytes	60 (60.0 b)
TX bytes	10360 (10.1 Kb)
Adaptive RX	off
Adaptive TX	off
stats-block-usecs	0
sample-interval	0
pkt-rate-low	0
pkt-rate-high	0
rx-usecs	3
rx-frames	0
rx-usecs-irq	0
rx-frames-irq	0
tx-usecs	0
tx-frames	0
tx-usecs-irq	0
tx-frames-irq	0

## System tools & diagnose commands

To locate system and network issues, FortiWeb appliances provide several troubleshooting tools.

Troubleshooting methods and tips may use:

- The command line interface (CLI & Backend Shell)
  - Diagnostic commands
  - Execute commands
  - Backend Shell commands & tools
- The Web UI
- External third-party tools

Some CLI commands provide troubleshooting information not available through the web UI; third-party tools on external hosts can test connections from perspectives that cannot be achieved locally.

---

<b>Diagnostic Commands</b> .....	<b>236</b>
<b>Execute Commands</b> .....	<b>238</b>
<b>Ping &amp; Traceroute</b> .....	<b>238</b>
<b>Packet capture</b> .....	<b>239</b>
<b>Diff</b> .....	<b>245</b>
<b>Run backend-shell commands</b> .....	<b>246</b>
<b>Upload a file to or download a file from FortiWeb</b> .....	<b>248</b>

## Diagnostic Commands

Most diagnostic tools are in the CLI and are not available from the web UI. Many are used in the above sections. For more information on the diagnose command and other CLI commands, see the FortiWeb CLI Reference:

<https://docs.fortinet.com/product/fortiweb/>

The main diagnostic commands are listed as below:

### Diagnose debug

```
FortiWeb-AWS-M01 # diagnose debug
admin-HTTPS      admin-HTTPS
  application      set/get debug level for daemons
cli              debug cli
cloudinit        cloudinit
cmdb             debug cmdbsvr
comlog comlog
console          console
```

```

coredumplog      coredumplog
crashlog         crashlog
daemonlog       daemonlog
disable          disable debug output
dnsproxy        dnsproxy
dpdkpktinfo     dpdkpktinfo
emerglog        emerglog
enable          enable debug output
flow            flow
info            show active debug level settings
jemalloc         jemalloc
jemalloc-conf   jemalloc-conf
jemalloc-heap   jemalloc-heap
kernlog         kernlog
memory          dump internal memory usage
netstatlog      netstatlog
proxy           set/get debug for proxyd
reset           reset all debug level to default
serial(ttyS0)   serial(ttyS0)
sslhardwarestatus sslhardwarestatus
sysinit         sysinit
timestamp       timestamp
trace           trace
ttp             ttp
vm              vm
waf             waf
writedisk       writedisk

```

## Diagnose network

Show, add or delete IP address, ARP, TCP/UDP connection, route tables, etc.

```

FortiWeb # diagnose network
aggregate      802.3ad link aggregation
arp            arp
ip            ip
irq           read network irq
redundant     redundant interface
route         route
rtcache      rtcache
rule         rule
sniffer      sniffer network traffic
tcp          tcp
udp          udp
vip          vip

```

## Diagnose policy

Use this command to view the process ID, live sessions, and traffic statistics associated with a server policy.

```

FortiWeb # diagnose policy
awscloud-stats  awscloud-stats
conn-psec       conn-psec
detail-stats    detail-stats
period-blockip  period-blockip

```

```
back-end server      back-end server
quarant-ip           quarant-ip
server-pool          server-pool
session              session
total-conn-psec      total-conn-psec
total-detail-stats   total-detail-stats
total-session        total-session
total-traffic        total-traffic
traffic              traffic
vdom-session         vdom-session
vdom-traffic         vdom-traffic
worker-detail-stats  worker-detail-stats
```

## Execute Commands

The execute command has an immediate and decisive effect on your FortiWeb appliance and, for that reason, should be used with care. Unlike config commands, most execute commands do not result in any configuration change.

### Execute session-cleanup

Just note this command will clear all current sessions by restart proxyd.

```
FortiWeb # execute session-cleanup
This operation will clean up all the sessions!
Do you want to continue? (y/n)y
```

### Execute smart

Diagnose hard disk health status by using SMART tool

```
execute smart enable
execute smart self-test
execute smart test-process
execute smart test-result
```

## Ping & Traceroute

If your FortiWeb appliance cannot connect to other hosts, try using ICMP (ping and traceroute) to determine if the host is reachable or to locate the node of your network at which connectivity fails, such as when static routes are incorrectly configured. You can do this from the FortiWeb appliance using CLI commands.

For example, you might use ping to determine that 192.0.2.87 is reachable:

```
execute ping 192.0.2.87
PING 192.0.2.87 (192.0.2.87): 56 data bytes
64 bytes from 192.0.2.87: icmp_seq=0 ttl=64 time=2.4 ms
64 bytes from 192.0.2.87: icmp_seq=1 ttl=64 time=1.4 ms
```

```
64 bytes from 192.0.2.87: icmp_seq=2 ttl=64 time=1.4 ms
64 bytes from 192.0.2.87: icmp_seq=3 ttl=64 time=0.8 ms
64 bytes from 192.0.2.87: icmp_seq=4 ttl=64 time=1.4 ms
--- 192.0.2.87 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.8/1.4/2.4 ms
```

or that 192.168.1.10 is not reachable:

```
execute ping 192.0.2.55
PING 192.0.2.55 (192.0.2.55): 56 data bytes
Timeout ...
Timeout ...
Timeout ...
Timeout ...
Timeout ...
--- 192.0.2.55 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

If the host is not reachable, you can use traceroute to determine the router hop or host at which the connection fails:

```
execute traceroute 192.0.2.55
traceroute to 192.0.2.55 (192.0.2.55), 32 hops max, 72 byte packets
1  192.168.1.2 2 ms 0 ms 1 ms
2  * * *
```

For details about CLI commands, see the FortiWeb CLI Reference:

<https://docs.fortinet.com/product/fortiweb/>

For details about troubleshooting connectivity, see [Diagnosing Network Connectivity Issues](#).



Both ping and traceroute require that network nodes respond to ICMP. If you have disabled responses to ICMP on your network, hosts may appear to be unreachable to ping and traceroute, even if connections using other protocols can succeed.

---

## Packet capture

Packet capture, also known as sniffing or packet analysis, records some or all of the packets seen by a network interface (that is, the network interface is used in promiscuous mode). By recording packets, you can trace connection states to the exact point at which they fail, which may help you to diagnose some types of problems that are otherwise difficult to detect.

FortiWeb appliances have a built-in sniffer. Packet capture on FortiWeb appliances is similar to that of FortiGate appliances. You can perform the packet capture through CLI command or Web UI.

## Packet capture via CLI command

To use the built-in sniffer, connect to the CLI and enter the following command:

```
diagnose network sniffer [{any | <interface_name>} [{none | '<filter_str>'} [{1 | 2 | 3 | 4 | 5 | 6} [<count_int> <tsformat>]]]
```

where:

- <interface\_name> is either the name of a network interface, such as port1, or enter any for all interfaces.
- '<filter\_str>' is the sniffer filter that specifies which protocols and port numbers that you do or do not want to capture, such as 'tcp port 80', or enter none for no filters. Filters use tcpdump (<http://www.tcpdump.org>) syntax.
- {1 | 2 | 3} is an integer indicating whether to display the network interface names, packet headers, and/or payloads for each packet that the network interface sends, receives, or sees:
- 1—Display the packet capture timestamp, plus basic fields of the IP header: the source IP address, the destination IP address, protocol name, and destination port number.

Does **not** display all fields of the IP header; it omits:

- IP version number bits
- Internet header length (ihl)
- Type of service/differentiated services code point (tos)
- Explicit congestion notification
- Total packet or fragment length
- Packet ID
- IP header checksum
- Time to live (TTL)
- IP flag
- Fragment offset
- Options bits
- For example:

```
interfaces= [port2]
```

```
filters= [none]
```

```
0.655224 172.20.130.16.2264 -> 172.20.130.15.42574: udp 113
```

```
FWB # diagnose network sniffer port1 "tcp port 80" 1
filters=[tcp port 80]
3.586959 172.19.33.15.1082 -> 10.65.1.93.80: syn 370304845
3.586991 10.65.1.93.80 -> 172.19.33.15.1082: syn 2254261780 ack 370304846
3.587102 172.19.33.15.1082 -> 10.65.1.93.80: ack 2254261781
3.587158 172.19.33.15.1082 -> 10.65.1.93.80: psh 370304846 ack 2254261781
3.587167 10.65.1.93.80 -> 172.19.33.15.1082: ack 370304933
3.587669 10.65.1.93.80 -> 172.19.33.15.1082: psh 2254261781 ack 370304933
3.587765 172.19.33.15.1082 -> 10.65.1.93.80: ack 2254261994
3.614443 172.19.33.15.1082 -> 10.65.1.93.80: fin 370304933 ack 2254261994
3.614519 10.65.1.93.80 -> 172.19.33.15.1082: fin 2254261994 ack 370304934
3.614626 172.19.33.15.1082 -> 10.65.1.93.80: ack 2254261995
```

- 2—All of the output from 1, plus the packet payload in both hexadecimal and ASCII. For example:

```
FWB # diagnose network sniffer port1 "tcp port 80" 2
filters=[tcp port 80]
4.682601 172.19.33.15.1118 -> 10.65.1.93.80: syn 240953163
0x0000 4500 003c 1ad5 0000 3f06 8827 ac13 210f E..<....?...'!..
0x0010 0a41 015d 045e 0050 0e5c a74b 0000 0000 .A.]^P.\K....
0x0020 a002 3908 e0bb 0000 0204 05b4 0402 080a ..9.....
0x0030 080d 9316 0000 0000 0103 030a .....
```

- 3—All of the output from 2, plus the link layer (Ethernet) header. e.g.:

```
FWB # diagnose network sniffer port1 "tcp port 80" 3
filters=[tcp port 80]
5.896404 172.19.33.15.1160 -> 10.65.1.93.80: syn 1153539951
0x0000 0009 0fa0 9801 906c ac95 9f7e 0800 4500 .....l...~..E.
0x0010 003c 1adb 0000 3f06 8821 ac13 210f 0a41 .<....?...'!..A
0x0020 015d 0488 0050 44c1 9f6f 0000 0000 a002 .]...PD...o.....
0x0030 3908 a0c2 0000 0204 05b4 0402 080a 080d 9.....
0x0040 a45c 0000 0000 0103 030a .\.....
```

- 4—All of the output from 2, plus the ingress or egress interface.

```
FWB # diagnose network sniffer port1 "tcp port 80" 4
filters=[tcp port 80]

interface=[port1]
2.985197 172.19.33.15.1170 -> 10.65.1.93.80: syn 1339018934

interface=[port1]
2.985231 10.65.1.93.80 -> 172.19.33.15.1170: syn 4031884093 ack 1339018935
```

- 5—All of the output from 2, plus the ingress or egress interface.

```
FWB # diagnose network sniffer port1 "tcp port 80" 5
filters=[tcp port 80]
interface=[port1]
5.254139 172.19.33.15.1174 -> 10.65.1.93.80: syn 3018448609
0x0000 4500 003c 1ae7 0000 3f06 8815 ac13 210f E..<....?.....!.
0x0010 0a41 015d 0496 0050 b3e9 dee1 0000 0000 .A.]...P.....
0x0020 a002 3908 de09 0000 0204 05b4 0402 080a ..9.....
0x0030 080d b86c 0000 0000 0103 030a ...l.....
```

- 6—All of the output from 3, plus the ingress or egress interface.

```
FWB # diagnose network sniffer port1 "tcp port 80" 6
filters=[tcp port 80]
interface=[port1]
3.495456 172.19.33.15.1217 -> 10.65.1.93.80: syn 1799303857
0x0000 0009 0fa0 9801 906c ac95 9f7e 0800 4500 .....l...~..E.
0x0010 003c 1aed 0000 3f06 880f ac13 210f 0a41 .<....?.....!..A
0x0020 015d 04c1 0050 6b3f 32b1 0000 0000 a002 .]...Pk?2.....
0x0030 3908 c815 0000 0204 05b4 0402 080a 080d 9.....
0x0040 c310 0000 0000 0103 030a .....
```

- <count\_int> is the number of packets the sniffer reads before stopping. Packet capture output is printed to your CLI display until you stop it by pressing Ctrl+C, or until it reaches the number of packets that you

have specified to capture.



Packet capture can be very resource intensive. To minimize the performance impact on your FortiWeb appliance, use packet capture only during periods of minimal traffic, with a local console CLI connection rather than a Telnet or SSH CLI connection, and be sure to stop the command when you are finished.

For example, you might capture all TCP port 443 (typically HTTPS) traffic occurring through port1, regardless of its source or destination IP address. The capture uses a high level of verbosity (indicated by 3).

A specific number of packets to capture is not specified. As a result, the packet capture continues until the administrator presses Ctrl+C. The sniffer then confirms that five packets were seen by that network interface.

(Verbose output can be very long. As a result, output shown below is truncated after only one packet.)

- `<tsformat>` is the format of timestamp.
  - **a:** absolute UTC time, yyyy-mm-dd hh:mm:ss.ms
  - **otherwise:** relative to the start of sniffing, ss.ms

```
FortiWeb# FortiWeb# diagnose network sniffer port1 'tcp port 443' 3
interfaces=[port1]
filters=[tcp port 443]
10.651905 192.168.0.1.50242 -> 192.168.0.2.443: syn 761714898
0x0000 0009 0f09 0001 0009 0f89 2914 0800 4500 .....E.
0x0010 003c 73d1 4000 4006 3bc6 d157 fede ac16 .<s.@.@;..W....
0x0020 0ed8 c442 01bb 2d66 d8d2 0000 0000 a002 ...B..-f.....
0x0030 16d0 4f72 0000 0204 05b4 0402 080a 03ab ..Or.....
0x0040 86bb 0000 0000 0103 0303 .....
```

Instead of reading packet capture output directly in your CLI display, you usually should save the output to a plain text file using your CLI client. Saving the output provides several advantages. Packets can arrive more rapidly than you may be able to read them in the buffer of your CLI display, and many protocols transfer data using encodings other than US-ASCII. It is often, but not always, preferable to analyze the output by loading it into in a network protocol analyzer application such as Wireshark (<http://www.wireshark.org>).

For example, you could use PuTTY or Microsoft HyperTerminal to save the sniffer output to a file. Methods may vary. See the documentation for your CLI client.

## Requirements

- Terminal emulation software such as PuTTY (<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>)
- A plain text editor such as Notepad
- A Perl interpreter (<http://www.perl.org/get.html>)
- Network protocol analyzer software such as Wireshark (<http://www.wireshark.org>)

## To view packet capture output using PuTTY and Wireshark

1. On your management computer, start PuTTY.
2. Use PuTTY to connect to the FortiWeb appliance using either a local console, SSH, or Telnet connection. For details, see the *FortiWeb CLI Reference*: <https://docs.fortinet.com/product/fortiweb/>
3. Type the packet capture command, such as:

```
diagnose network sniffer port1 'tcp port 443' 3
```

but do **not** press Enter yet.

4. In the upper left corner of the window, click the PuTTY icon to open its drop-down menu, then select **Change Settings**. A dialog appears where you can configure PuTTY to save output to a plain text file.
5. In the **Category** tree on the left, go to **Session > Logging**.
6. In **Session logging**, select **Printable output**.
7. In **Log file name**, click the **Browse** button, then choose a directory path and file name such as `C:\Users\MyAccount\packet_capture.txt` to save the packet capture to a plain text file. (You do not need to save it with the `.log` file extension.)
8. Click **Apply**.
9. Press **Enter** to send the CLI command to the FortiWeb appliance, beginning packet capture.
10. If you have not specified a number of packets to capture, when you have captured all packets that you want to analyze, press `Ctrl + C` to stop the capture.
11. Close the PuTTY window.
12. Open the packet capture file using a plain text editor such as Notepad.
13. Delete the first and last lines, which look like this:

```

===== PuTTY log 4/22/2024.07.25 11:34:40
=====
FortiWeb-2000 #

```

These lines are a PuTTY timestamp and a command prompt, which are not part of the packet capture. If you do not delete them, they could interfere with the script in the next step.

14. Convert the plain text file to a format recognizable by your network protocol analyzer application. You can convert the plain text file to a format (`.pcap`) recognizable by Wireshark (formerly called Ethereal) using the `fgt2eth.pl` Perl script. To download `fgt2eth.pl`, see the Fortinet Knowledge Base article "Troubleshooting Tool: Using the FortiOS built-in packet sniffer" (<http://kb.fortinet.com/kb/documentLink.do?externalId=11186>).



The `fgt2eth.pl` script is provided as-is, without any implied warranty or technical support, and requires that you first install a Perl module compatible with your operating system.

---

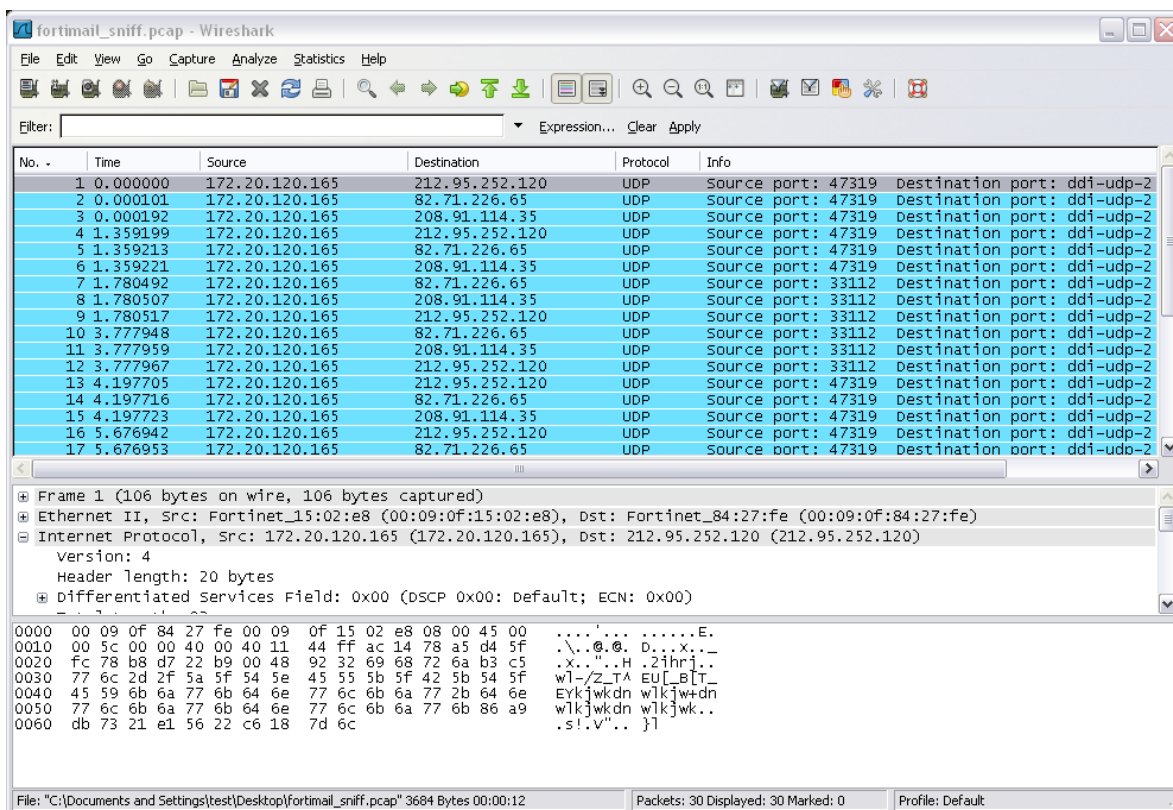
To use `fgt2eth.pl`, open a command prompt, then enter a command such as the following:

```
fgt2eth.pl -in packet_capture.txt -out packet_capture.pcap
```

where:

- `fgt2eth.pl` is the name of the conversion script; include the path relative to the current directory, which is indicated by the command prompt
  - `packet_capture.txt` is the name of the packet capture's output file; include the directory path relative to your current directory
  - `packet_capture.pcap` is the name of the conversion script's output file; include the directory path relative to your current directory where you want the converted output to be saved
15. Open the converted file in your network protocol analyzer application. For further instructions, see the documentation for that application.

## Viewing sniffer output in Wireshark



For additional information on packet capture, see the Fortinet Knowledge Base article "Troubleshooting Tool: Using the FortiOS built-in packet sniffer" (<http://kb.fortinet.com/kb/documentLink.do?externalId=11186>).

For more information on CLI commands, see the *FortiWeb CLI Reference*: <https://docs.fortinet.com/product/fortiweb/>

## Packet capture via Web UI

### To create a packet capture policy:

1. Go to **Network > Packet Capture**.
2. Click **Create New** to create a new packet capture policy.
3. Configure these settings:

<b>Interface</b>	Select the network interface on which you want to capture packets.
<b>Filter</b>	Specify which protocols and port numbers that you do or do not want to capture, such as 'tcp and port 80 and host IP1 and ( IP2 or IP3 )', or leave this field blank for no filters. <b>Note</b> that please use the same filter expression as <code>tcpdump</code> for this filter, you can refer to the Linux man page of <code>TCPDUMP</code> ( <a href="http://www.tcpdump.org/manpages/tcpdump.1.html">http://www.tcpdump.org/manpages/tcpdump.1.html</a> ).

**Maximum Packet Count** Specify the maximum packets you want to capture for the policy. Capture will stop automatically if the total captured packets hits the count.

4. Click **OK**.
5. Configure a packet capture policy from the policy table:

**Interface** The network interface on which the packet capture policy is applied.

**Filter** The protocols and port numbers that the packet capture policy do or do not want to capture.

**Packets** Current captured packet count. This value keeps increasing during the capture is running.

**Maximum Packet Count** The maximum packets count of the policy.

**Progress** Click the **Start** button aside **No Running** to start the capture.

During the capture processing, a progress bar is displayed to show the progress to the maximum packet count. Count of captured packets is displayed in **Packets** field.

Capture stops when hitting the maximum packet count, or you can click the **Stop** button to stop the capture anytime. Captured packets will be saved as a .pcap file.

Click the **Download** button to download the capture output file.

Click the **Restart** button to restart the capture.

**To view the packet capture data:**

1. Go to **Network > Packet Capture**.
2. Select the interface of which you want to view the packets data.
3. Click the **View** icon to view the details of the packets. You will see the details of the packet data.



4. You can also click the **Download** icon to download the .pcap file to your local directory.

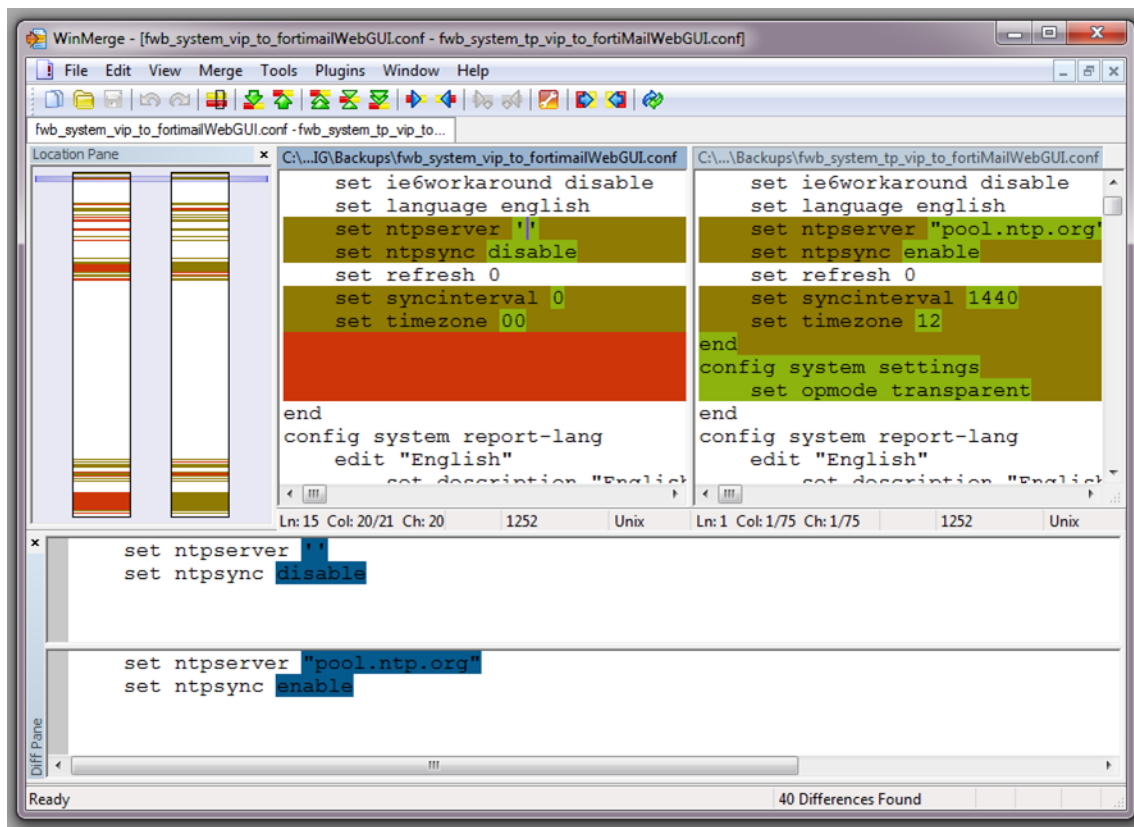
## Diff

You can compare backups of the core configuration file with your current configuration. This can be useful if, for example:

- A previously configured feature is no longer functioning, and you are not sure what in the configuration has changed.
- You want to recreate something configured previously, but do not remember what the settings were.

Difference programs can help you to quickly find all changes.

## Configuration differences highlighted in WinMerge



There are many such difference-finding programs, such as WinMerge (<http://sourceforge.net/projects/winmerge>) and the original diff (<http://www.gnu.org/s/diffutils>). They can compare your configurations, line by line, and highlight parts that are new, modified, or deleted.

For instructions, see your difference program's documentation.

## Run backend-shell commands



Shell-access is no longer possible on 7.4.1 and higher releases.

Sometimes we need to login to FortiWeb backend shell to check logs or collect some specific files. Though we expect all useful logs are collected or archived in the debug log file or can be downloaded from **System > Maintenance > Backup & Restore > GUI File Download**, some files especially logs for new features may not be included, so you may have to login to the backend shell to collect these logs or execute some commands, for example, executing curl to verify if the backend servers is reachable.

## Login to backend shell on 6.4 or 6.3 builds

It's simple but really dangerous. The admin user can login to the backend shell with the root permission just by executing "fn sh".

```
FWB # fn sh
/#
```

## Login to backend shell on 7.0.0 and later builds

To access the backend shell, you need to enable shell-access and create a temporary user/password through CLI first, then login via SSH.

```
config system global
  set shell-access enable
  set shell-username <user_name>
  set shell-password <password>
  set shell-timeout 1200 #The shell-access will be disabled in 1200 minutes
  set shell-history-size 1024 #Record 1024 operations
  set shell-trusthostv4 0.0.0.0/0 #soucre ip(ipv4) should in the trust-host address
  set shell-trusthostv6 ::/0 #soucre ip(ipv6) should in the trust-host address
end
```

Then you can login to the backend shell with a SSH client:

```
C:\>ssh shell@192.168.0.99
shell@192.168.0.99's password:
-- WARNING! All configurations should be done through CLI shell.
-- You now have full access.
/#
```

To check the shell access history, run:

```
diagnose debug shell-access history show
```

## Use "fnsysctl" in CLI to execute backend commands

To simplify, you can execute some commonly used backend commands directly in FortiWeb CLI, without enabling shell-access and adding username/password.

On 7.0.3 and previous builds, below commands are supported:

```
FortiWeb # fnsysctl
```

Below are the usable commands:

```
basename cat date df dmesg
du ifconfig netstat nslookup ping
sleep uname ps kill killall
lspci df fdisk mount free
lsusb insmod mknod smartctl MegaCli ssh dmidecode pstack
strace tcpdump gdb
```

```
FortiWeb # fnsysctl df -h
Filesystem          Size      Used Available Use% Mounted on
/dev/root            472.5M    358.2M    114.4M    76% /
none                 1.1G     44.3M     1.1G      4% /tmp
```

none	3.8G	3.0M	3.8G	0%	/dev/shm
/dev/sda2	362.4M	271.5M	71.3M	79%	/data
/dev/sda3	90.6M	56.0K	85.6M	0%	/home
/dev/sda4	30.5G	4.1G	24.9G	14%	/var/log

For security purpose, 7.0.4 and newer builds only support below commands:

```
FortiWeb # fnsysctl
Below are the usable commands:
basename date df dmesg ifconfig
netstat nslookup ping sleep uname
ps lspci free lsub traceroute
pidof smartctl dmidecode nmon
```

Please note that some commands such as “fn pstack” and “fn ssh” are not supported. To collect the pstack information, you need to configure shell-access and login into the backend shell first.

## Upload a file to or download a file from FortiWeb

The upload and download method has already been stated in [Customizing and downloading debug logs on page 86](#) and [Collecting core/coredump files and logs on page 93](#).



Copyright© 2024 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.