FORTINET

Release Notes

FortiADC 7.4.5

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

September 6, 2024
FortiADC 7.4.5 Release Notes

TABLE OF CONTENTS

Change Log

Date	Change Description
September 6, 2024	FortiADC 7.4.5 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.4.5, Build 0364.

To upgrade to FortiADC 7.4.5, see Upgrade notes.

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: https://docs.fortinet.com/product/fortiadc.

What's new

FortiADC 7.4.5 offers the following new features and enhancements:

Increased GSLB capacity

FortiADC now supports an increase in the number of Global Server Load Balancing (GSLB) objects. You can create up to 4,096 zones and Fully Qualified Domain Name (FQDN) hosts across all platforms, exceeding the previous limit of 256 GSLB hosts. Additionally, devices with four or more logical cores can utilize up to 1,024 GSLB policies, enhancing the flexibility and scalability of your load-balancing configurations.

Parameters	100F/120F/200F/220F	300D/400D/300F/320F/400F/420F/1000F/1200F/2000F/2200F	4000F/4200F/5000F
Zones	4096	4096	4096
FQDN hosts	4096	4096	4096
GLB policies	256	300D/300F/320F/400F: 256 420F/1000F/1200F/2000F/2200F: 1024	1024

Parameters	VM01	VM02	VM04	VM08	VM16
Zones	4096	4096	4096	4096	4096
FQDN hosts	4096	4096	4096	4096	4096
GLB policies	256	256	256	1024	1024

Enhanced SSL Forward Proxy Performance

Users can now optimize SSL Forward Proxy performance via CLI with two new configurations:

- Adjustable Certificate Key Length — Configure key lengths of 1024, 2048, or automatic, with 1024 as the default.
- Selectable Certificate Type — Select from RSA, ECDSA, or both to better suit performance and security needs.

```
config load-balance client-ssl-profile
...
  set forward-proxy enable
  set forward-proxy-resign-cert-by-sni enable
  set forward-proxy-resign-cert-type {both|rsa|ecdsa}
  set forward-proxy-resign-cert-rsa-key-size {auto|1024bit|2048bit}
  set forward-proxy-resign-cert-ecdsa-curve {auto|prime256v1|secp384r1|secp521r1}
end
```

`forward-proxy-resign-cert-type`	The **forward-proxy-resign-cert-type** option is available if **forward-proxy** is enabled.

	Select either of the following: • both — When the SSL Forward Proxy needs to resign the local/remote certificate, both RSA and ECDSA certificates are generated and loaded. • rsa — When the SSL Forward Proxy needs to resign the local/remote certificate, only generate and load the RSA certificate • ecdsa — When the SSL Forward Proxy needs to resign the local/remote certificate, only generate and load the ECDSA certificate.
`forward-proxy-resign-cert-rsa-key-size`	The **forward-proxy-resign-cert-rsa-key-size** option is available if **forward-proxy-resign-cert-type** is **both** or **rsa**. Select either of the following: • auto — The **auto** option will adapt its behavior based on the status of the **forward-proxy-resign-cert-by-sni** setting, performing different actions depending on whether this option is enabled or disabled. **When forward-proxy-resign-cert-by-sni is disabled:** • If the remote server uses **RSA certificates** — Use a 1024-bit RSA certificate if the remote server’s RSA certificate key size is 1024 or smaller. Otherwise, use a 2048-bit RSA certificate if the key size is larger. • If the remote server uses **ECDSA certificates** — Use a 2048-bit RSA certificate for all ECDSA certificates. • If the remote server uses **DSA certificates** — Use a 1024-bit RSA certificate if the remote server’s DSA certificate key size is 1024 or smaller. Otherwise, use a 2048-bit RSA certificate if the key size is larger. **When forward-proxy-resign-cert-by-sni is enabled**: • HTTPS Requests with SNI — The proxy will use the built-in "Factory" certificate, which is a 2048-bit RSA certificate. • HTTPS Requests without SNI — The behavior will follow the same rules as when the **forward-proxy-resign-cert-by-sni** option is **disabled**. • 1024bit — Only a 1024-bit RSA certificate will be generated and loaded. • 2048bit — Only a 2048-bit RSA certificate will be generated and loaded.
`forward-proxy-resign-cert-ecdsa-curve`	The **forward-proxy-resign-cert-ecdsa-curve** option is available if **forward-proxy-resign-cert-type** is **both** or **ecdsa**. Select either of the following: • auto — The **auto** option will adapt its behavior based on the status of the **forward-proxy-resign-cert-by-sni** setting, performing different actions depending on whether this option is enabled or disabled. **When forward-proxy-resign-cert-by-sni is disabled**: • If the remote server uses **RSA certificate**s — Use the prime256v1 ECDSA curve if the RSA key size is 2048 or smaller. Otherwise, use the secp384r1 ECDSA curve if the RSA key size is

	larger. • If the remote server uses **ECDSA certificates** — Use the prime256v1 ECDSA curve if the certificate does not specify a named curve. Otherwise, use the prime256v1 ECDSA curve if the curve ID is less than or equal to NID_X9_62_prime256v1. If the curve ID is greater than NID_X9_62_prime256v1 and less than or equal to NID_secp384r1, use the secp384r1 ECDSA curve. And for all other ECDSA certificates, use the secp521r1 ECDSA curve. • If the remote server uses **DSA certificates** — Use the prime256v1 ECDSA curve if the DSA key size is 2048 or smaller. Otherwise, use the secp384r1 ECDSA curve if the DSA key size is larger. **When forward-proxy-resign-cert-by-sni is enabled:** • HTTPS Requests with SNI — The proxy will use the built-in "Factory" certificate, which is a RSA_2048 certificate (in which case the prime256v1 curve will be used). • HTTPS Requests without SNI — The behavior will follow the same rules as when the **forward-proxy-resign-cert-by-sni** option is **disabled**. • prime256v1 — Only an ECDSA certificate using prime256v1 curve will be generated. • secp384r1 — Only an ECDSA certificate using secp384r1 curve will be generated. • secp521r1 — Only an ECDSA certificate using secp521r1 curve will be generated.

SSL Session ID persistency support in Layer 7 TCP via Lua scripting

FortiADC now supports SSL Session ID persistency without decrypting the traffic in Layer 7 TCP. This is implemented through the new Lua stream scripting function **LB:set_peer(ip, port)** which allows you to select a real server with a specific IP and port in STREAM_REQUEST_DATA events.

```
when STREAM_REQUEST_DATA {
    LB:set_peer("10.0.0.1","443")
}
```

Name	Description
ip	A real server IP address. **Note**: Only the IP address in a real server from the regular pool can be used here; it cannot use a real server from the schedule pool. If a real server is not specified, then FortiADC will select a real server by using the specified load-balancing method.
port	A real server port. **Note**: Only the port in a real server from the regular pool can be used here; it cannot use a real server from the schedule pool. If a real server is not specified, then FortiADC will select a real server by using the specified load-balancing.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.4.5. All supported platforms are 64-bit version of the system.

Supported Hardware:

- FortiADC 300D
- **FortiADC 400D**
- FortiADC 100F
- FortiADC 120F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 320F
- FortiADC 400F
- FortiADC 420F
- FortiADC 1000F
- FortiADC 1200F
- FortiADC 2000F
- FortiADC 2200F
- FortiADC 4000F
- FortiADC 4200F
- FortiADC 5000F

For more information on the supported hardware models, see FortiADC's Hardware Documents.

The FortiADC 400D will reach End of Support with version 7.4.6, which will be the final release for this model.

Supported hypervisor versions:

VM environment	Tested Versions
VMware	ESXi 3.5, 4.x, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0
Microsoft Hyper-V	Windows Server 2012 R2, 2016 and 2019
KVM	Linux version 3.19.0 qemu-img v2.0.0, qemu-img v2.2
Citrix Xen	XenServer 6.5.0
Xen Project Hypervisor	4.4.2, 4.5
OpenStack	Pike

VM environment	Tested Versions
Nutanix	AHV
Proxmox VE	6.4

Supported cloud platforms:

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

For more information on the supported cloud platforms, see the FortiADC Private Cloud and Public Cloud documents.

Supported web browsers:

- Mozilla Firefox version 109
- Google Chrome version 110

We strongly recommend you set either of the Web browsers as your default Web browser when working with FortiADC. You may also use other (versions of the) browsers, but you may encounter certain issues with FortiADC's Web GUI.

Resolved issues

The following issues have been resolved in FortiADC 7.4.5 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1069133	False positives for SQL/XSS Injection Detection are triggered by legitimate requests containing Arabic language characters.
1067899	Unable to edit real servers from the FortiView Local Topology.
1066100	Unable to assign a /31 subnet IP to the interface for a point-to-point connection.
1054660	When configuring a REST API Administrator, the API key cannot be generated if the setup is done through the Global configuration without access to the root VDOM.
1042724	A core dump was triggered due to a socket in the process of closing during the socket dump operation, causing the issue to occur.
1042085	Unable to delete a script — the error message states that the script is applied to a Layer 4 virtual server, which does not support scripting.
1039565	The Authentication Policy with Server Load Balancing is truncating "–" from usernames.
1036480	FortiADC unable to synchronize HA cluster due to WAF signature database upgrade.
1034384	Unable to log in to FortiADC appliance through GUI when /tmp folder reaches 90% capacity.
1034357	LDAPS negotiation failure with TLS 1.0 post upgrade from 7.4.0 to 7.4.3.
1031727	Httproxy crash related to OpenSSL issue — resolved by upgrading to OpenSSL version 3.1.5.
1030563	High latency issue caused by httproxy utilizing 100% CPU when the Exception List is enabled and the client unsuccessfully initiates the TLS handshake.
1015996	Newly imported certificate/private key is not being accepted.
1009204	Some virtual servers are not responding, with traffic logs showing 0 bytes sent or received.
1001089	VIP is not accessible on 400F port9 and port10 when packet capture is disabled.

Common Vulnerabilities and Exposures

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

Bug ID	Description
1051921	FortiADC 7.4.5 is no longer vulnerable to the following CVE-Reference: CVE-2024-6387.

Known issues

This section lists known issues in version FortiADC 7.4.5, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

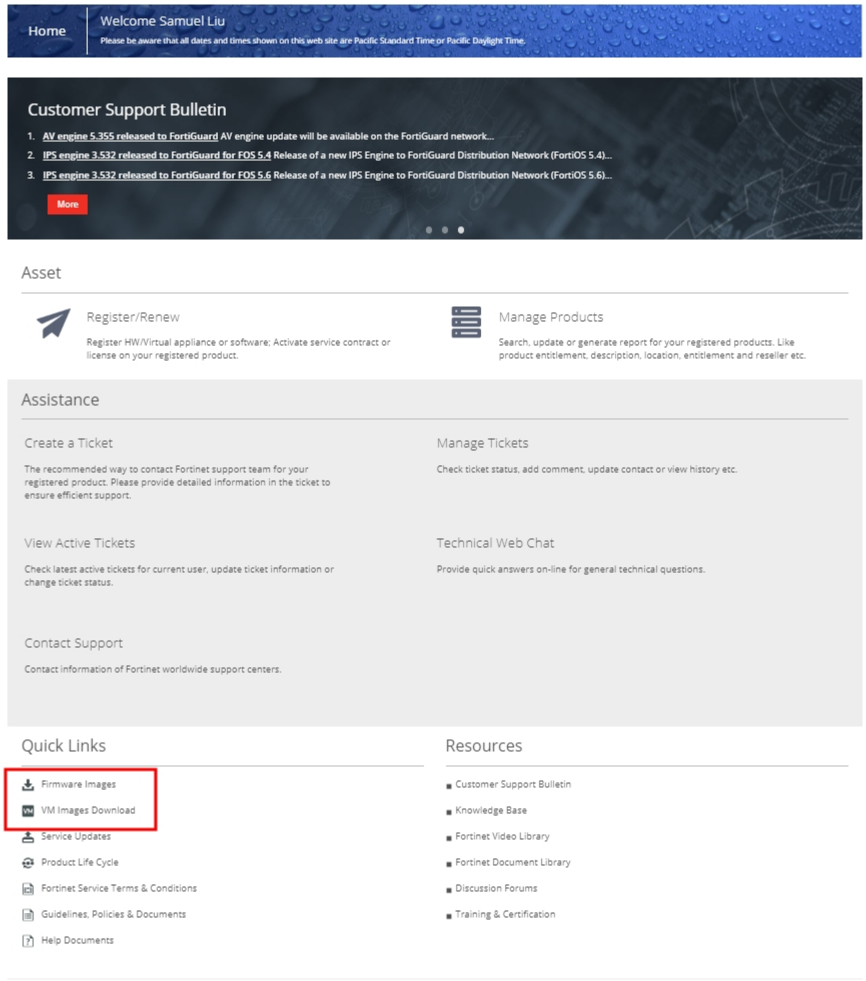
Bug ID	Description
1071500	In FortiView, unable to show GLB topology if the number of hosts is 4096 or more.

Image checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, click the Firmware Image Checksums button. (The button appears only if one or more of your devices has a current support contract.) In the File Name field, enter the firmware image file name including its extension, then click Get Checksum Code.

Customer Service & Support image checksum tool



Home

Welcome Samuel Liu

Please be aware that all dates and times shown on this web site are Pacific Standard Time or Pacific Daylight Time.

Customer Support Bulletin

1. AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...
2. IPS engine 3.532 released to FortiGuard for FOS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FOS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...

More

Asset

Register/Renew

Register HW/Virtual appliance or software; Activate service contract or license on your registered product.

Manage Products

Search, update or generate report for your registered products. Like product entitlement, description, location, entitlement and reseller etc.

Assistance

Create a Ticket

The recommended way to contact Fortinet support team for your registered product. Please provide detailed information in the ticket to ensure efficient support.

Manage Tickets

Check ticket status, add comment, update contact or view history etc.

View Active Tickets

Check latest active tickets for current user, update ticket information or change ticket status.

Technical Web Chat

Provide quick answers on-line for general technical questions.

Contact Support

Contact information of Fortinet worldwide support centers.

Quick Links

- Firmware Images
- VM Images Download
- Service Updates
- Product Life Cycle
- Fortinet Service Terms & Conditions
- Guidelines, Policies & Documents
- Help Documents

Resources

- Customer Support Bulletin
- Knowledge Base
- Fortinet Video Library
- Fortinet Document Library
- Discussion Forums
- Training & Certification

Upgrade notes

This section includes upgrade information about FortiADC 7.4.5.

Supported upgrade paths

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

If you are upgrading to a version that is in a higher version level, you will need to upgrade to the nearest branch of the major level incrementally until you reach the desired version. For example, to upgrade from 7.1.1 to 7.4.0, you will follow the upgrade path below:

7.1.1 → 7.1.x → 7.2.x → 7.4.0

(wherein "x" refers to the latest version of the branch)

7.2.x to 7.4.x

Direct upgrade via the web GUI or the Console.

7.1.x to 7.2.x

Direct upgrade via the web GUI or the Console.

7.0.x to 7.1.x

Direct upgrade via the web GUI or the Console.

6.2.x to 7.0.x

Direct upgrade via the web GUI or the Console.

6.1.x to 6.2.x

Direct upgrade via the web GUI or the Console.

6.0.x to 6.1.x

Direct upgrade via the web GUI or the Console.

5.4.x to 6.0.x

Direct upgrade via the web GUI or the Console.

5.3.x to 5.4.x

Direct upgrade via the web GUI or the Console.

5.2.x to 5.3.x

Direct upgrade via the web GUI or the Console.

For more information on upgrading from versions earlier than 5.2.x, please see the Upgrade Instructions document for that version.

Upgrading a stand-alone appliance

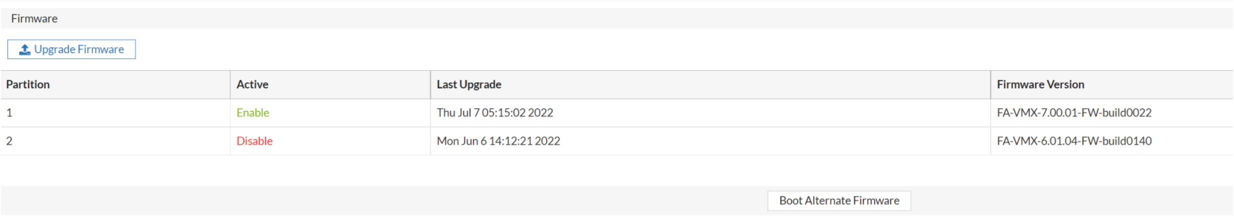
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- Updates the firmware on the inactive partition and then makes it the active partition.
- Copies the firmware on the active partition, upgrades it, and installs it in place of the configuration on the inactive partition.

For example, if partition 1 is active, and you perform the upgrade procedure:

- Partition 2 is upgraded and becomes the active partition; partition 1 becomes the alternate partition.
- The configuration on partition 1 remains in place; it is copied, upgraded, and installed in place of the configuration on partition 2.

This is designed to preserve the working system state in the event the upgrade fails or is aborted.



Partition	Active	Last Upgrade	Firmware Version
1	Enable	Thu Jul 7 05:15:02 2022	FA-VMX-7.00.01-FW-build0022
2	Disable	Mon Jun 6 14:12:21 2022	FA-VMX-6.01.04-FW-build0140

Before you begin:

- You must have super user permission (user admin) to upgrade firmware.
- Download the firmware file from the Fortinet Customer Service & Support website: https://support.fortinet.com/
- Back up your configuration before beginning this procedure. Reverting to an earlier firmware version could reset settings that are not compatible with the new firmware.
- You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

To update the firmware:

1. Go to **System > Settings**.
2. Click the **Maintenance** tab.

3. Scroll to the **Firmware** section.
4. Click **Upgrade Firmware** to locate and select the firmware file.
5. Click ⬆ to upload the firmware and reboot.
   The system replaces the firmware on the alternate partition and reboots. The alternate (upgraded) partition becomes the active, and the active becomes the alternate.
6. Clear the cache of your web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Upgrading an HA cluster

The upgrade page includes an option to upgrade the firmware on all nodes in an HA cluster from the primary node.

The following chain of events occur when you use this option:

1. The primary node pushes the firmware image to the member nodes.
2. The primary node notifies the member nodes of the upgrade, and takes on their user traffic during the upgrade.
3. The upgrade command is run on the member nodes, the systems are rebooted, and the member nodes send the primary node an acknowledgment that the upgrade has been completed.
4. The upgrade command is run on the primary node, and it reboots. While the primary node is rebooting, a member node assumes the primary node status, and traffic fails over from the former primary node to the new primary node.

After the upgrade process is completed, the system determines whether the original node becomes the primary node, according to the HA Override settings:

- If Override is enabled, the cluster considers the Device Priority setting. Both nodes usually make a second failover in order to resume their original roles.
- If Override is disabled, the cluster considers the uptime first. The original primary node will have a smaller uptime due to the order of reboots during the firmware upgrade. Therefore, it will not resume its active role. Instead, the node with the greatest uptime will remain the new primary node. A second failover will not occur.

Before you begin, do the following:

1. Make sure that you have super user permission (user admin) on the appliance whose firmware you want to upgrade.
2. Download the firmware file from the Fortinet Customer Service & Support website:
   https://support.fortinet.com/
3. Back up your configuration before beginning this procedure. Reverting to an earlier version of the firmware could reset the settings that are not compatible with the new firmware.
4. Verify that the cluster node members are powered on and available on all of the network interfaces that you have configured. (Note: If required ports are not available, HA port monitoring could inadvertently trigger an additional failover, resulting in traffic interruption during the firmware update.)
5. You upgrade the alternate partition. Decide which partition you want to upgrade. If necessary, click **Boot Alternate Firmware** to change the active/alternate partitions.

To update the firmware for an HA cluster:

1. Log into the web UI of the *primary* node as the `admin` administrator.
2. Go to **System > Settings**.
3. Click the **Maintenance** tab.
4. Scroll to the **Upgrade Firmware** button.
5. Click **Choose File** to locate and select the file.
6. Enable the **HA Cluster Upgrade**.
7. Click ⬆ to upload the firmware and start the upgrade process.

After the new firmware has been installed, the system reboots.

> When you update software, you are also updating the web UI. To ensure the web UI displays the updated pages correctly:
>
> - Clear your browser cache.
> - Refresh the page.
>
> In most environments, press Ctrl+F5 to force the browser to get a new copy of the content from the web application. See the Wikipedia article on browser caching issues for a summary of tips for many environments: https://en.wikipedia.org/wiki/Wikipedia:Bypass_your_cache.

Special notes and suggestions

7.2.3

- The real server auto-populate feature is currently supported only in FortiADC version 7.2.3. Upgrading from version 7.2.3 to 7.4.0/7.4.1 will cause auto-populated real server related configuration loss, and may cause other unexpected behavior.
  Support for real server auto-population will be extended to later versions in the next release.

7.0.2/7.1.x

- After upgrading to 7.0.2/7.1.x, in Virtual Machine HA environments where both nodes have been installed with certificate embedded licenses you must reinstall those licenses. As some backend certificate files would have been synchronized and overwritten by the HA Peer (due to an existing bug), the certificate file would not be recoverable. Reinstalling the certificate embedded licenses is required to ensure they would work properly where they are needed, such as in ZTNA or FortiSandbox Cloud.

7.0.0

- When deploying the new GSLB based on FortiADC 7.0.0, the verify-CA function will be enabled by default.

6.2.2

- To use the SRIOV feature, users must deploy a new VM.

6.2.0

- In version 6.2.0, the default mode of QAT SSL has been changed to polling.

6.1.4

- Before downgrading from 6.1.4, ensure the new L7 TCP or L7 UDP application profiles are deleted or changed to a profile type that is supported in the downgrade version. Otherwise, this will cause the cmdb to crash.

5.2.0-5.2.4/5.3.0-5.3.1

- The backup configuration file in versions 5.2.0-5.2.4/5.3.0-5.3.1 containing the certificate configuration might not be restored properly (causing the configuration to be lost). After upgrading, please discard the old 5.2.x/5.3.x configuration file and back up the configuration file in the upgraded version again.

FORTINET®

www.fortinet.com