FORTINET

Release Notes

FortiADC 7.6.0

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

July 17, 2024
FortiADC 7.6.0 Release Notes

TABLE OF CONTENTS

Change Log **4**
Introduction **5**
What's new **6**
Hardware, VM, cloud platform, and browser support **8**
Resolved issues **10**
Known issues **13**
Image checksums **14**
Upgrade notes **15**
Supported upgrade paths 15
Upgrading a stand-alone appliance 16
Upgrading an HA cluster 17
Special notes and suggestions 18

Change Log

Date	Change Description
July 17, 2024	FortiADC 7.6.0 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.6.0, Build 0422.

To upgrade to FortiADC 7.6.0, 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 7.6.0 offers the following new features and enhancements. For detailed descriptions, see the New Features document.

Web Application Firewall

- WAF Adaptive Learning
- Bot Detection enhancement

Security Fabric

- FortiGate Security Fabric Connector

FortiView

- OWASP Top 10 Compliance

System

Certificate

- ACME TLS-ALPN-01 Enhancements

High Availability

- HA cluster supports maximum 8 member nodes
- HA management interface network options via CLI
- Virtual MAC address option as interface in Active-Passive HA via CLI
- New and enhanced CLI commands to force HA nodes into standby mode

Settings

- Administrator lockout controls in CLI
- Direct VDOM Access for Administrators

Server Load Balance

- Waiting Room for virtual queuing through HTTP scripting
- AWS autoscaling group discovery
- New health check down options
- HTTP3 support for HTTP to HTTPS Redirection

Global Load Balance

- Multiple Global DNS Policy support in FQDN zones
- DNS forwarding support at zone level with no matching hostname
- DNS forwarding log debug in CLI

Link Load Balance

- SLB local traffic support

Platform

- FortiFlex support for cloud-init in Proxmox (KVM)

Troubleshooting

- Health Check debug log enhancement in CLI

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.6.0. 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.

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, Octavia 2023.2
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 7.6.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
1023569	`fib_stat` memory is not released due to a reference count leak caused by a connection tracking entry being attached to multiple SKBs.
1042724	Coredump caused by processing sockets.
1042085	Unable to delete script and error message indicates that the script is applied to a Layer 4 virtual server that should not support scripting.
1039565	Authentication Policy with Server Load Balance is cutting '–' off of usernames.
1036480	FortiADC unable to synchronize HA cluster due to WAF signature database upgrade.
1034357	LDAPS negotiation failure with TLS 1.0 after upgrading from 7.4.0 to 7.4.3.
1034347	High CPU utilization due to timer system issues, and httproxy-SSL crashes caused by crash in the WAF module.
1031466	Unable to pass TLS-APLN-01 challenge with HTTP2 VS.
1029446	Unclear event log message: The index table elog.0000000013 of log file is broken and rebuild it.
1028025	ICMP Timestamp Request Remote Date Disclosure (CVE-1999-0524) remediation support.
1027026	FD (file descriptor) leak for Health Check, leading to partial VS down in the VDOM.
1025346	In GLB, the error "GLB FQDN A/AAAA hosts are duplicated" message occurs when adding more than two A records into a policy.
1025087	FortiADC stops processing DNS queries with the zone type defined as fqdn-generate.
1024031	High CPU usage occurs after upgrading device from 7.4.1 to 7.4.3.
1022505	GSLB does not work as expected after upgrading to 7.2.4.
1020498	Alertd crashes when HA synchronizes configurations.
1015996	FortiADC did not accept new certificate/private key due to failed certificate import.
1011313	Layer 4 virtual server traffic incorrectly matches when the VM is restarted or in the event of fail-over.
1009305	The Sync List functionality is unable to properly synchronize certificates.

Bug ID	Description
1009229	VMware clone of FortiADC image retains the MAC addresses of the original image when new MAC addresses should be assigned.
1007062	Httproxy crash caused by hidden field length limit in WAF input validation function.
1005919	The FortiADC becomes stuck on 1M connections on the dashboard concurrent sessions as a result of a timer system issue.
1005767	Unable to manage the FortiADC if logged in as LDAP user due to exceeding the maximum DN (Distinguished Name) length of 127 characters.
1005261	Request to allow HTTP:persist() script function to be used in the HTTP_RESPONSE event.
1003220	FortiADC-VM memory leak caused by the incorrect return of ha_tun_rcv.
1002301	DLP dictionaries incorrectly includes PK dictionaries.
1001137	Httproxy-ssl crash caused by connection release delay.
1001089	VIP is not accessible on 400F port9 and port10 when packet capture is disabled.
1000632	Memory leak in fcnacd daemon.
1000626	Server health check scripts fail to work after upgrade to FortiADC 7.4.1.
0999904	Httproxy-SSL crashed related to the WAF module crash.
0999197	License upload page is outdated, still using GUI from version 5.x.
0997325	Timezone delay due to outdated zonefile.
0996826	Hidden Field Input Validation is not working due to the HTML form action "#" being appended to the POST URL.
0982605	Configuring L7 Content Routing affects L4 Virtual Server with Content Routing enabled.
0979813	Web-category-test display issues.
0973378	SLBL7 FTPS fails sometimes.
0956991	Misspelled Trap OIDs.
0857626	FortiADC network becomes unresponsive at random in Redhat Openstack environment.

Common Vulnerabilities and Exposures

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

Bug ID	Description
0985993	FortiADC 7.6.0 is no longer vulnerable to the following CVE-Reference: CVE-2023-48795.

Known issues

This section lists known issues in version FortiADC 7.6.0, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

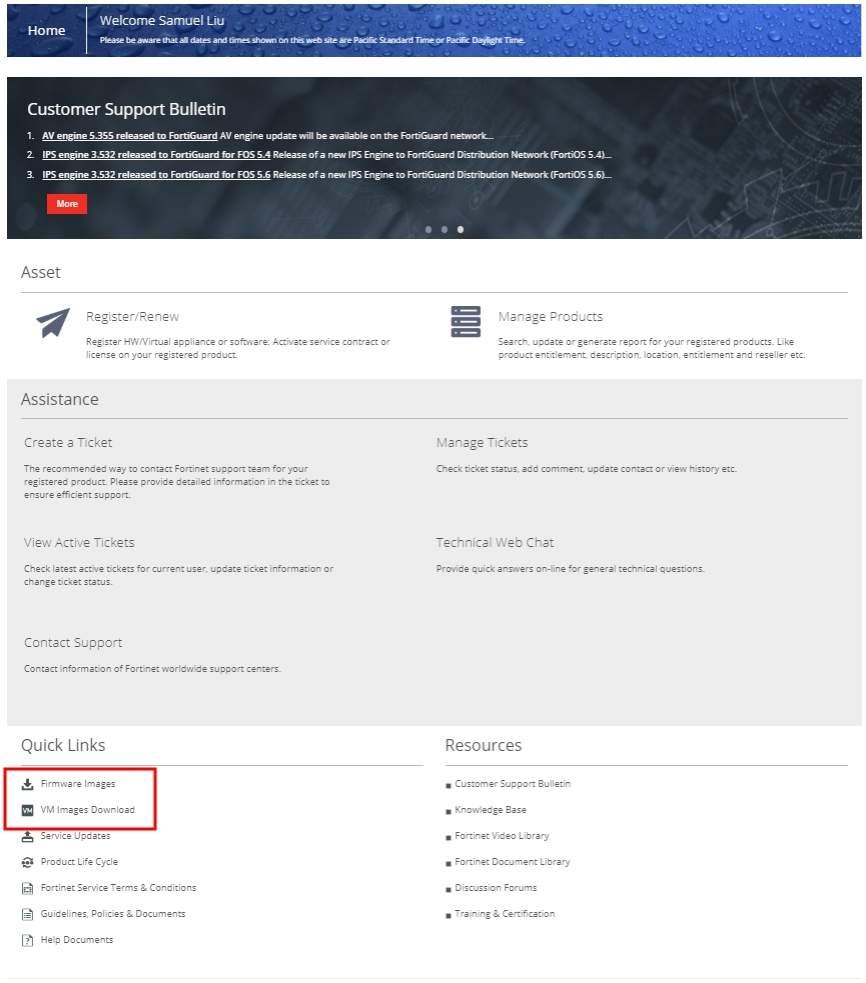
Bug ID	Description
1046923	Adaptive Learning does not support the same parameter or hidden field in different URLs under the same Virtual Server.
0992554	Threat Analytic does not support AWS BYOL.

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



Upgrade notes

This section includes upgrade information about FortiADC 7.6.0.

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 7.2.1 to 7.6.0, you will follow the upgrade path below:

7.2.1 → 7.2.x → 7.4.x → 7.6.0

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

7.4.x to 7.6.x

Direct upgrade via the web GUI or the Console.

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.

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.)

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.

www.fortinet.com