FortiADC - Release Notes

Version 7.0.0

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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

January 28, 2022
FortiADC 7.0.0 Release Notes
01-544-677187-20201112

TABLE OF CONTENTS

Change Log

Date	Change Description
January 28, 2022	FortiADC 7.0.0 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.0.0, Build 0014.

To upgrade to FortiADC 7.0.0, see Special notes.

FortiADC provides load balancing, both locally and globally, and application delivery control. For more information, visit: http://docs.fortinet.com/fortiadc-d-series/.

What's new

FortiADC 7.0.0 offers the following new features:

Load Balance

FTPS virtual server support

FortiADC now supports FTPS (File Transfer Protocol Secure) for virtual servers through the new Security Mode options for the FTP application profile type.

Increased secure communication between GSLB and SLB to prevent MITM attacks

To protect against MITM attacks, communication between GSLB and SLB can now be further secured by implementing root CA verification so that only the same set of certification and CA may pass.

Share IP address with SNAT and virtual servers

You can now enable the SNAT across the firewall, L4 VS and L7 VS to use the same IP address, while maintaining different port ranges.

SAML enhancements

- SAML Service Providers metadata can now be exported through the Web UI.
- You can now use the AuthNRequest algorithm to allow FortiADC to sign the SAML authentication request.
- The Assertion Require Sign configuration object has been added to support Sign SAML Assertion.
- The Single Logout Binding Type now supports “redirect”.

Layer 4 virtual server debug support

The new `diagnose debug flow` commands allows you to get the debug information of specific Layer 4 virtual servers.

Security

WAF exceptions enhancement

New WAF exception rule types have been added: HTTP Method, HTTP Header, Cookie, and Parameter.

IP Reputation now includes ISDB IPs

The FortiADC IP Reputation will now use Internet Services DB (ISDB) which is dependent on the FortiGuard IP Reputation service.

System

FortiGuard delta package download support

FortiADC now supports delta package downloads mode for AV DB from FortiGuard.

HSM FIPS support

You can now enable FIPS support in the HSM server to use a FIPS-certification HSM.

Automated Certificate Management Environment (ACME) support

The ACME protocol is a communications protocol for automating interactions between certificate authorities and their users' web servers. FortiADC will support the ACME protocol to get SSL certificates through certificate authorities like Let's Encrypt.

Unicast HA support for FortiADC-VM KVM image

FortiADC now supports HA VRRP Unicast mode in KVM.

GUI

Login navigation page enhancement

The Login navigation page will now guide users to set up the readable hostname and change the default password in their initial login.

GUI enhancements

The following enhancements are made in the GUI:

- In the Dashboard, the hover tooltip will show completely when the graph is on the first row.
- "No Data" is displayed when there is no available data for a chart.
- Graphs now dynamically scale according to the window size.
- In the FortiView Security Aggregate Log, graph titles have been added.
- In the FortiView System Automation page, table list items will show 25 entries per page as the default option.
- For Security Fabric objects, a check mark will be visible when hovering over a selection.

Product hardware, integration and support

This section lists the hardware models, hypervisor versions, cloud platforms, web browsers and Fortinet products supported by FortiADC 7.0.0. All supported platforms are 64-bit version of the system.

Supported Hardware:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- FortiADC 120F
- FortiADC 200F
- FortiADC 220F
- FortiADC 300F
- FortiADC 400F
- 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
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
Nutanix	AHV

Supported cloud platforms:

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

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

Supported web browsers:

- Mozilla Firefox version 59
- Google Chrome version 65

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.

Supported Fortinet products:

Resolved issues

The following issues have been resolved in FortiADC 7.0.0 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0774662	WAF signature details page displaying overlapping text.
0774607	CPU spikes occurring in both of the paired FortiADC units due to the DNSPod multi-thread daemon accessing null schedule data when the DNS request is very high.
0770880	WAF unable to detect the expected attack when the requests contain Non-US-ASCII characters.
0770832	Debug producing junk output.
0770608	Unable to register in FortiCare from AWS with FortiADC PAYG instance.
0769906	CLI returning wrong system status information despite GUI displaying correct license information for the IPS related service.
0769717	GUI does not allow the comment field to be empty for the local certificate configuration.
0769573	Telnet and SNMP are enabled by default on port1.
0768416	Unable to unset mail server address.
0768119	HA device repeatedly asking for license.
0766854	Cookie-security WAF rule causing VS-persistence to fail.
0766502	Ntpdate crash.
0766441	Unable to configure the WAF exception rules via GUI.
0765729	Spelling error: L3 Trasnparent Proxy → L3 Transparent Proxy.
0761550	FortiADC may reboot multiple times during upgrade when not using HA sync upgrade in HA environment.
0756750	Health check via GUI is not working properly for VDOM.
0754313	WAF Parameter Validation does not work when forming an action with no path.
0753788	There is no length restriction for NAT Pool name in GUI.
0751900	Spelling error: vitrual → virtual.
0751761	FortiADC administrator users are limited to control no more than 8 VDOMs per user.

Known issues

This section lists known issues in version FortiADC7.0.0, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

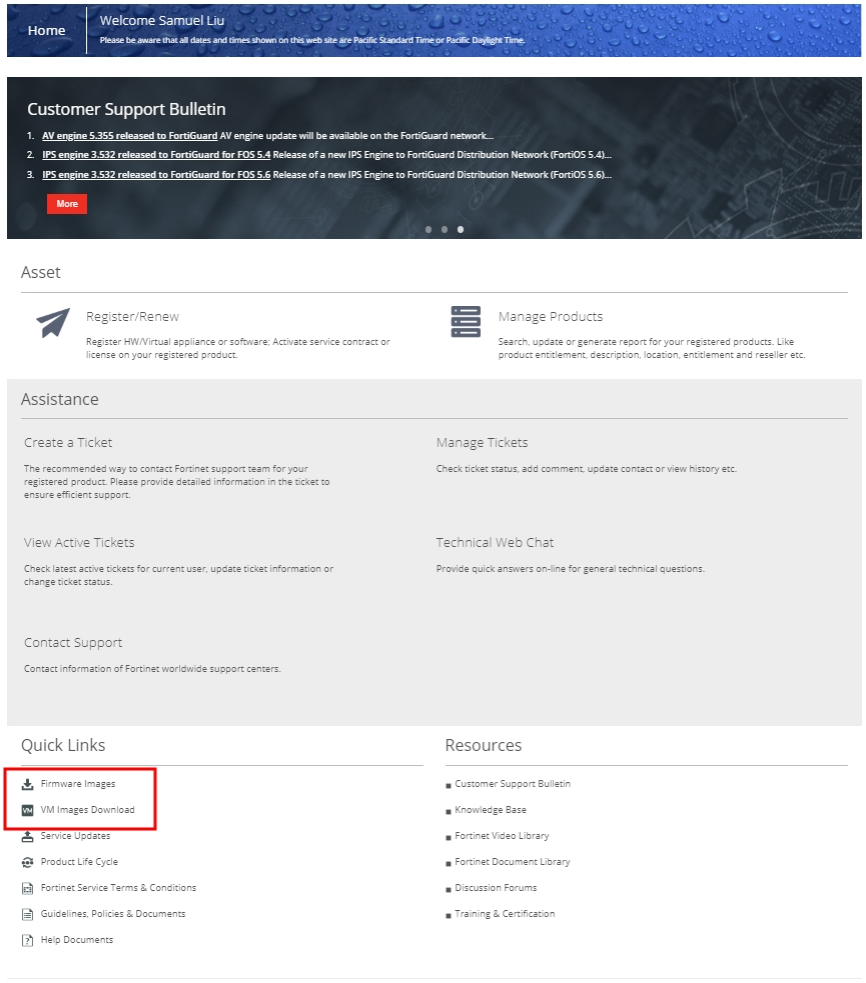
Bug ID	Description
0777422	In FortiADC deployed in AWS, DNS is resolving fails for SDN connectors (AWS, K8s, etc.).
0777345	FortiView page has a code injection risk in Referrer chart.
0777188	GLB is unable to connect to SLB and shows licd has failed to bind in SLB.
0777062	The aging problem on the Web Anti-Defacement page.
0776212	Traffic triggers A6-CORS protection but the log detail and Dashboard cannot display A6 information because currently there is no WAF Signature to support it.
0775632	FW NAT indication message "Out interface must be set" is incorrect; the message should indicate "Egress interface" instead of "Out interface".
0775509	FortiView OWASP Top10 - A1: 2017 Injection - 1Day - pop-up in the GUI.
0774277	GLB VS may respond to DNS query even when gw is down in HA VRRP mode.
0773648	In the HA Remote IP Monitor List, the GUI only shows the interfaces under root options, but the non-root interface is shown and can be assigned as a remote IP monitor interface in the CLI.
0772424	Duplicated listen port error warning when changing HA mgmt IP.
0769454	The SLB L4 debug has no output when the traffic coming from the IP belongs to the geo blocklist.
0768852	FortiADC does not withdraw BGP routes when the schedule pool is unavailable.
0697575	IPS adds signature check signature with api/fortiguard_proxy/fos file with no response.

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



Special notes

Suggestions

- HSM doesn't support TLS v1.3. If the HSM certificate is used in VS, the TLS v1.3 handshake will fail. **Workaround:** Uncheck the TLSv1.3 in the SSL profile if you're using the HSM certificate to avoid potential handshake failure.
- To use the SRIOV feature, users must deploy a new VM.
- When deploying the new GSLB based on FortiADC 7.0.0, the verify-CA function will be enabled by default.