FortiADC - Release Notes

Version 6.1.4

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

September 20, 2021
FortiADC 6.1.4 Release Notes
01-544-677187-20201112

TABLE OF CONTENTS

Change Log

Date	Change Description
September 20, 2021	FortiADC 6.1.4 Release Notes initial release.

Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 6.1.4, Build 0140.

To upgrade to FortiADC 6.1.4, see Upgrade 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 6.1.4 offers the following new features:

New Application Profile Type for L7

FortiADC now supports TCP/UDP profiles for L7 with the new application profile types, L7 TCP and L7 UDP. The existing TCP/ UDP application profile types will now apply to L4 only.

Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 6.1.4.

Supported Hardware:

- FortiADC 200D
- FortiADC 300D
- FortiADC 400D
- FortiADC 700D
- FortiADC 1500D
- FortiADC 2000D
- FortiADC 4000D
- FortiADC 100F
- 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
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.

Known issues

This section lists known issues in version 6.1.4, but may not be a complete list. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0752290	SAML fails to function after upgrade to FortiADC 6.1.4/6.2.0/6.2.1.
0746479	When enable ip_commands script and script log in L7TCP, the log message is not stable. It will show correctly after a few seconds.

Resolved issues

The following issues have been resolved in FortiADC 6.1.4 release. For inquiries about particular bugs, please contact Fortinet Customer Service & Support.

Bug ID	Description
0745311	Incorrect status output for unicast HA hb-type.
0744870	NTP diag log is incorrect.
0743690	VS stops forwarding traffic due to the fnginxctld and httproxy crashes.
0743252	GLB virtual server status is not correct after upgrade to 6.1.3. Resolved by optimizing the performance on licd and gicd communication.
0740912	Token parse error due to /tmp is full.
0740780	Data center unable to show if use country region.
0736799	No log name for the SNAT log.
0736358	Traffic logs not showing for L7 VS using TCP profile.
0735937	DNS response TTL is not correct if it has the same IP from different server.
0735008	LACP status is not correct when there is only one member.
0731909	DNSD crashes when a new real server with FQDN type is added or modifying an existing one.
0731622	Support SLB port 0 as wildcard of 1-65535.
0730683	System interface link status change to unknown when physical interface becomes member of aggr or softswitc.
0730183	Web UI issue after creating a WVS policy.
0729079	Not able to show completely for HA slave device for FortiGSLB status.
0728582	httproxy crashed with content-rewrite match with `.*` and http traffic url included `//`.
0728411	High CPU consumption and crashes due to httproxy.
0728103	Content route matching IP 0.0.0.0 takes precedence which overwrites other content route matching on different IP.
0726385	Sync-list auth fail in FortiADC Azure.
0728077	SNMP retrieves the wrong status for Real Server.
0725481	SLB-L7 SMTP returns 502 response when setting `disable-command-status` to `disable`.
0724897	Incorrect affinity settings in 100F.

Bug ID	Description
0724091	High memory consumption after upgrading to 6.1.2 due to the AV function.
0689373	GLB server gw is not correct in FortiView.
0644119	CPU gets stuck due to the fib_cache issue.

Common Vulnerabilities and Exposures

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

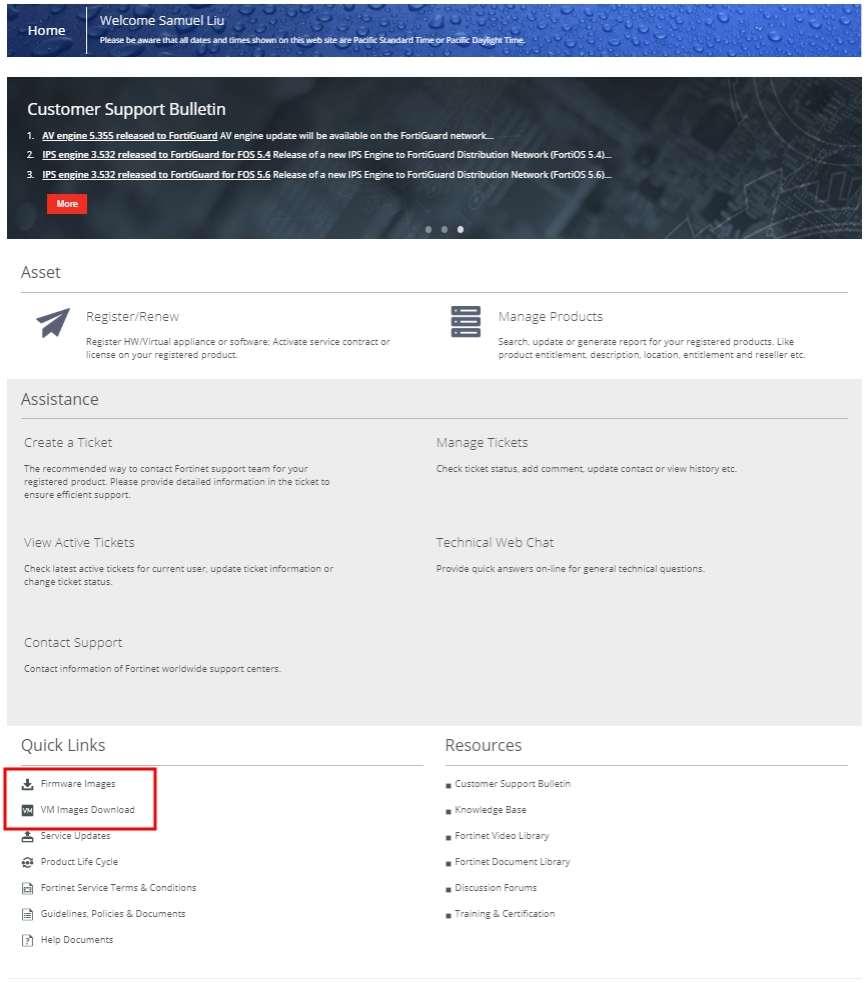
Bug ID	CVE reference
0729724	FortiADC 6.1.4 is no longer vulnerable to the following CVE-Reference: CWE-325: Missing Cryptographic Step.
0708219	FortiADC 6.1.4 is no longer vulnerable to the following CVE-Reference: CVE-2021-3450 and CVE-2021-3449.

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 6.1.4.

Do not upgrade to FortiADC 6.1.4/6.2.0/6.2.1 if you are currently using SAML. Once upgraded, SAML will fail to function. A solution to this issue is currently in development and will be available in the next release.

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.

Supported upgrade paths

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

Note:

If you are upgrading to the next major version level, you will need to upgrade to the nearest major versions first. For example, if you are updating from 4.8.4 to 5.2.0, then you will need to upgrade to 5.0.0, 5.1.0, and then to 5.2.0.

For upgrading to minor versions in a higher version level, you may skip the nearest major version to update directly to the minor version. For example, if you are updating from 4.8.4 to 5.1.2, then you will need to first upgrade to 5.0.0 then upgrade directly to 5.1.2.

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.

5.1.x to 5.2.x

Direct upgrade via the web GUI or the Console.

5.0.4 to 5.1.x

Direct upgrade via the web GUI or the Console.

Note: allow-ssl-version

There is an old SSL version in the allow-ssl-version config that is not recommend; but the client may have configured it before. This is removed when you upgrade from 5.0.x to 5.1.x/5.2.x. The client may need to add it back manually for compatibility.

5.0.0 to 5.0.4

Direct upgrade via the web GUI or the Console

4.8.x to 5.0.0

Direct upgrade via the web GUI or the Console.

GUI

Due to GUI changes and enhancements, we strongly recommend refreshing (Ctrl +F5) your web browser when access the FortiADC web GUI after the upgrade.

Authentication

This upgrade addresses the compatibility with other devices. Therefore, you must download the new FortiADC SAML SP and upload it to the SAML IDP peer. You do not need to modify the FortiADC SP file anymore.

System

It will take more time to upgrade to 5.0.0 because FortiADC has to create quarantine partition for the AV feature.

GEO IP

You will lose your existing GEO IP protection region configurations when upgrading from 4.7.x to 5.0.0.

4.8.4 to 4.8.4

Direct upgrade via the web GUI or the Console.

4.8.2 to 4.8.3

Direct upgrade via the web GUI or the Console.

4.8.1 to 4.8.2

Direct upgrade via the web GUI or the Console.

4.8.0 to 4.8.1

Direct upgrade via the web GUI or the Console.

GUI

- Due to GUI changes, be sure to refresh your web browser when the upgrade is completed (Ctrl + F5).
- FortiADC 60F supports Google Chrome only.

HA

- To synchronize system image upgrade in HA mode, make sure that all the devices in the HA cluster use exactly the same version of the image.
- Use the management interface in HA mode instead of a dedicated interface.

Platform

- Upgrade your VM01 to 4 GB of memory in virtual platform.

4.7.x to 4.8.0

Direct upgrade via the web GUI or the Console.

- GUI—Due to GUI changes, be sure to refresh (CTRL+F5) your web browser when access FortiADC upon upgrade.
- HA—(For physical devices) Upon upgrade, wait for a few minutes for the HA state to stabilize and the configuration to sync.
- Service—When upgrading to 4.8.x from 4.7.x or lower, FortiADC will add 28 predefined services. If you have old services with the same names as those of the predefined services, FortiADC will rename those "old" services to "`oldname_upgrade`".

- Global Load Balance—If there was a virtual server pool that was not referenced by any GLB Host in the 4.7.x configuration, the Default Feedback IP configuration in this virtual server pool will be lost upon upgrade. To keep this Default Feedback IP, you MUST reference this virtual server pool in the GLB Host before upgrading the system.

4.6.x to 4.7.x

Direct upgrade via the web UI or the CLI.

- GUI—Due to GUI changes, refresh (CTRL+F5) your web browser when access FortiADC upon upgrade.
- HA—(For physical devices) Upon upgrade, wait for a few minutes for the HA state to stabilize and the configuration to sync.
- Service—When upgrading to 4.7.x from 4.6.x or lower, FortiADC will add 28 predefined services. If you have old services with the same names as those of the predefined services, FortiADC will rename those "old" services to "`oldname_upgrade`".
- Global Load Balance—If there was a virtual server pool that was not referenced by any GLB Host in 4.7.x configuration, the Default Feedback IP configuration in this virtual server pool will be lost upon upgrade. To keep this Default Feedback IP, you MUST reference this virtual server pool in the GLB Host before upgrading the system.

4.6.1 to 4.6.2

Direct upgrade via the web UI or CLI.

4.5.x to 4.6.x

Direct upgrade to FortiADC 4.6.0 from any version prior to 4.5.x is NOT supported via the GUI. The best way to upgrade is via the CLI using the `restore image` command. If you prefer to upgrade via the GUI, you MUST first upgrade the image to 4.5.x and then to 4.6.x.

- GUI — Due to GUI changes in 4.6.x, be sure to refresh your browser when accessing the new FortiADC web GUI.
- Global Load Balance — If your existing configuration contains the ISP feature, reconfigure it. This is because the ISP option has been moved.
- HA —Update the firmware if HA Sync is enabled. The process normally takes about 10 minutes to complete.

4.4.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.3.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.2.x to 4.5.x

Direct upgrade via the web UI or the CLI.

4.1.x to 4.5.x

You can upgrade from FortiADC 4.1.x using the CLI. Direct upgrade from 4.1.x to 4.5.x is not supported from the web UI. See the FortiADC Handbook for instructions on upgrading with the CLI.

4.0.x to 4.5.x

Direct upgrade from 4.0.x and earlier is not supported. You must first upgrade to FortiADC 4.1.x, and the system must be in an operable state.

Upgrading a stand-alone appliance from 4.2.x or later

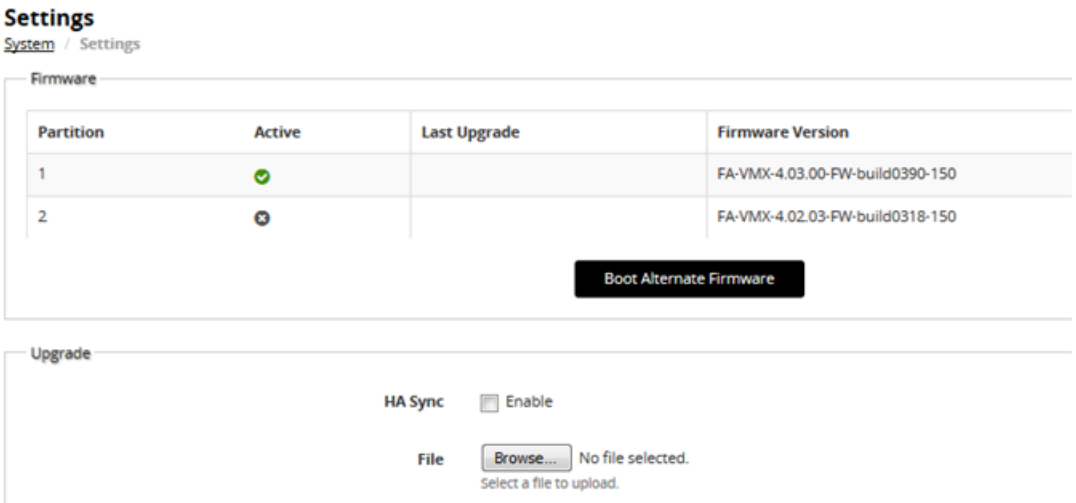
The following figure shows the user interface for managing firmware (either upgrades or downgrades). Firmware can be loaded on two disk partitions: the active partition and the alternate partition. The upgrade procedure:

- 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 firmware:

1. Go to System > Settings.
2. Click the **Maintenance** tab.
3. Scroll to the Upgrade section.
4. Click **Browse** to locate and select the 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 from 4.3.x or later

The upgrade page for Release 4.3.0 and later includes an option to upgrade the firmware on all nodes in an HA cluster from the primary node.

The following chain of events occurs 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 section.
5. Click **Browse** to locate and select the file.
6. Enable the **HA Sync** option.
7. Click  to upload the firmware and start the upgrade process.
8. Wait for the system to reboot and log you out to complete the upgrade.
9. Clear the cache of your Web browser and restart it to ensure that it reloads the web UI and correctly displays all interface changes.

Note: Normally, it takes approximately up to 10 minutes to upgrade with HA Sync.

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.
- The backup config file in versions 5.2.0-5.2.4/5.3.0-5.3.1 containing certificate config might not be restored properly (causing config to be lost). After upgrading to version 6.1.4, please discard the old 5.2.x/5.3.x config file and back up the config file in 6.1.4 again.
- Keep the old SSL version predefined config to ensure a smooth upgrade.
- HSM does not support TLSv1.3. If the HSM certificate is used in VS, the TLSv1.3 handshake will fail. **Workaround**: Uncheck the TLSv1.3 in the SSL profile if you are using the HSM certificate to avoid potential handshake failure.
- Since the v4.7.x release, FortiADC has introduced a parameter called `config-priotity` for HA configuration. It allows you to determine which configuration the system uses when synchronizing the configuration between the HA nodes. Therefore, upon upgrading to FortiADC 4.7.x or higher, we strongly recommend that you use this option to manually set different HA configuration priority values on the HA nodes. Otherwise, you'll have no control over the system's primary-secondary configuration sync

behavior.

When the configuration priority values are identical on both nodes (whether by default or by configuration), the system uses the configuration of the appliance with the larger serial number to override that of the appliance with the smaller serial number. When the configuration priority values on the nodes are different, the configuration of the appliance with the lower configuration priority will prevail.

The request-body-detection in the WAF web-attack-signature profile will be changed from "disable" to "enable" automatically after upgrading to FortiADC 5.4.0.