



# FortiADC - Release Notes

Version 7.1.0

**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](mailto:techdoc@fortinet.com)



July 29, 2022

FortiADC 7.1.0 Release Notes

01-544-677187-20220729

# TABLE OF CONTENTS

<b>Change Log</b>	<b>4</b>
<b>Introduction</b>	<b>5</b>
<b>What's new</b>	<b>6</b>
<b>Hardware, VM, cloud platform, and browser support</b>	<b>13</b>
<b>Resolved issues</b>	<b>15</b>
<b>Known issues</b>	<b>17</b>
<b>Image checksums</b>	<b>19</b>
<b>Upgrade notes</b>	<b>20</b>
Supported upgrade paths	20
Upgrading a stand-alone appliance	21
Upgrading an HA cluster	22
Special notes and suggestions	23

## Change Log

Date	Change Description
July 29, 2022	FortiADC 7.1.0 Release Notes initial release.

# Introduction

This *Release Notes* covers the new features, enhancements, known issues, and resolved issues of FortiADC™ version 7.1.0, Build 0111.

To upgrade to FortiADC 7.1.0, 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>.

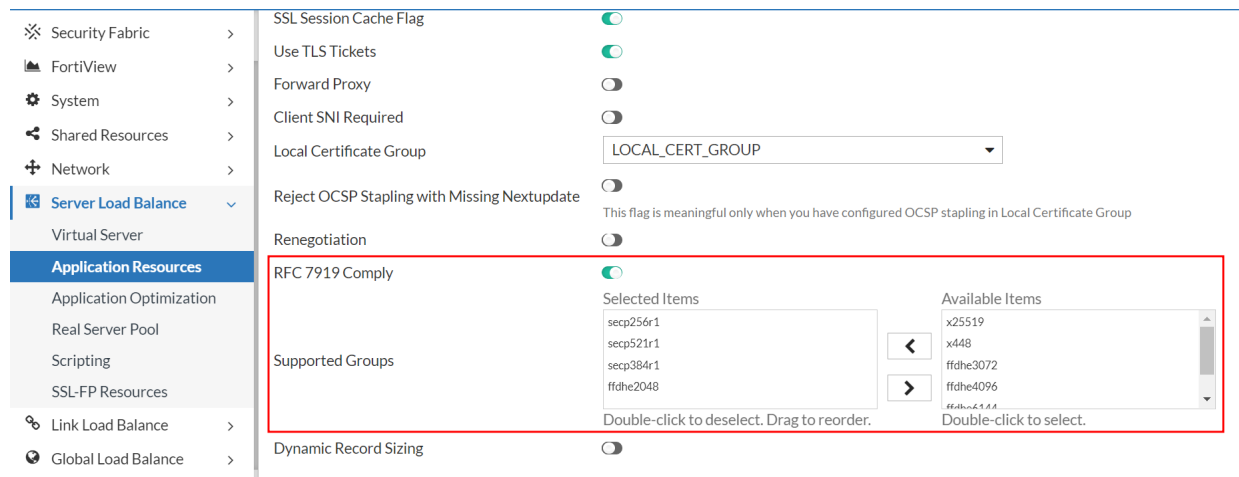
# What's new

FortiADC 7.1.0 offers the following new features:

## Server Load Balance

### RFC 7919 compliance support

You can now enable/disable [RFC 7919](#) compliance in your client SSL and real server SSL profile configurations.



### Enhancements to Cookie Hash and Insert persistence types

The Cookie Hash and Insert Cookie persistence rule types have been enhanced to allow more granular specifications for persistence.

- **Cookie Hash** — The persistence can now be based on a field of the cookie instead of the entire cookie.
- **Insert Cookie** — You can now set the domain value on the inserted cookie to allow it to be used cross-site as a wildcard.

### IPv6 support for Layer 2 TCP/UDP/IP virtual servers

FortiADC now supports IPv6 for Layer 2 server load balancing in TCP, UDP, and IP profiles.

### Error page enhancement

FortiADC has enhanced the error pages to include a new WAF deny page. In response to a WAF deny action, the error page will show the Message ID, Signature ID, and Client IP of the attack in the detailed message as recorded in the attack log.

## Real server pool and pool member availability enhancement

The Health Check backend workflow has been improved to allow more accurate diagnosis of the real server pool and pool member availability by accounting for status conditions that influence availability.

- **New real server pool member availability status "INIT"** — This status indicates that 1) the real server status is enabled, 2) the health check status is enabled for the pool member, and 3) the real server pool is not associated with a virtual server (which means the real server pool is either not used in a virtual server or it is used in a disabled virtual server).
- **How real server pool member availability influences the real server pool availability** — When the real server pool is associated with the virtual server, the real server pool availability can be influenced by the real server pool member availability if the real server pool member contains multiple availability statuses. For example, if the real server pool member availability is both "Healthy" and "Unhealthy" then the real server pool availability will be "Unhealthy".

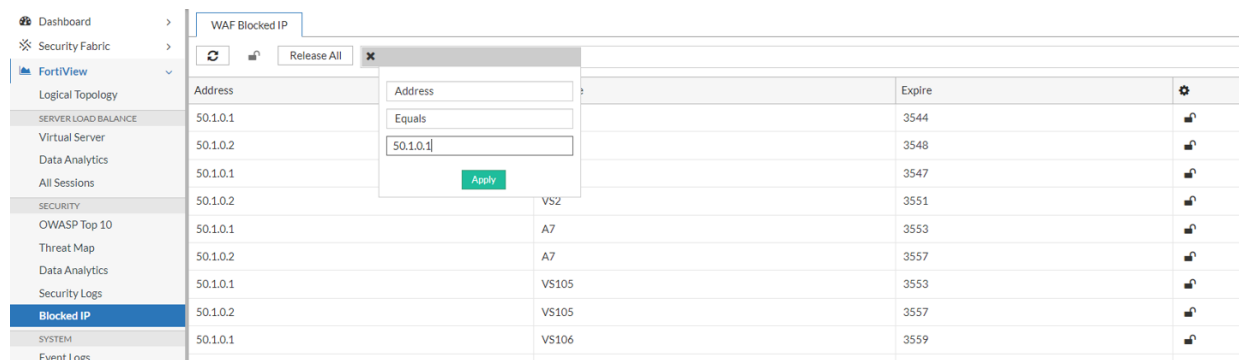
## BIND 9.18.0 upgrade

FortiADC has upgraded the BIND version to 9.18.0. As BIND 9.18.0 supports DNSSEC by default in Global Load Balancing, the option to manually enable/disable DNSSEC has been removed from the General Settings and Global DNS Policy.

## Security

### View and release WAF blocked IPs

You can now view and release any IP addresses that have been blocked by the WAF module through FortiView.




Address	Expire	
50.1.0.1	3544	
50.1.0.2	3548	
50.1.0.1	3547	
50.1.0.2	3551	VSZ
50.1.0.1	3553	A7
50.1.0.2	3557	A7
50.1.0.1	3553	VS105
50.1.0.2	3557	VS105
50.1.0.1	3559	VS106

### External IP list for firewall policies

The new IP Address external connector has been added to the FortiADC Security Fabric. You can now import external IP lists stored on an HTTP/HTTPS server and apply these IPs as an "External Source" for the Source Type/Destination Type address for IPv4 and IPv6 firewall policies.

Global ▾  
Dashboard >  
Security Fabric ▾  
Fabric Connectors  
External Connectors  
System >  
Network >  
Log & Report >

Thread Feeds

  
IP Address

Connector Settings

Name

Required config name. No spaces.

URI of External Resource

Required. Specify the resource URI.  
Example: http(s)://www.example.com/file.txt

HTTP Basic Authentication ☒

Username

Required. Specify the username.

Password

Required. Specify the password.

Refresh Rate

5  
Default: 5. Range: 1-43200 minutes

Comments

Specify the comments.

Status

☒

## OWASP Top 10 2021 update

The OWASP Top 10 list has been updated to the latest 2021 version. The OWASP Top 10 Wizard is automatically updated to the 2021 list, and the OWASP Top 10 2021 log data will be displayed through FortiView.

**Note:** Log data from OWASP Top 10 2017 can still be accessed through the Security log.



Server Load Balance >

Link Load Balance >

Global Load Balance >

Web Application Firewall >

OWASP TOP10 Wizard

WAF Profile

Known Web Attacks

Common Attacks Detection

Sensitive Data Protection

Input Validation

Access Protection

CORS Protection

API PROTECTION

JSON Protection

XML Protection

OpenAPI Validation

API Gateway

OWASP TOP10 Wizard

1 OWASP TOP10

2 Security Level

3 Add Profile

OWASP Top10

A1:2021-Broken Access Control

A2:2021-Cryptographic Failures

A3:2021-Injection

A4:2021-Insecure Design

A5:2021-Security Misconfiguration

A6:2021-Vulnerable and Outdated Components

A7:2021-Identification and Authentication Failures

A8:2021-Software and Data Integrity Failures

A9:2021-Security Logging and Monitoring Failures

A10:2021-Server-Side Request Forgery

root

Dashboard >

Security Fabric >

FortiView >

Logical Topology

SERVER LOAD BALANCE

Virtual Server

Data Analytics

All Sessions

SECURITY

OWASP Top 10

Threat Map

Data Analytics

Security Logs

Blocked IP

SYSTEM

Event Logs

Summary of

Threat Number 403

Action (Block/Monitor/Captcha) 403 (163/240/0)

Service (HTTP/HTTPS) 403 (396/7)

Time Period Last 1 Week

OWASP Top 10 Threats Log

Threats

Action (Block/Monitor/Captcha)

Service (HTTP/HTTPS)

A10:2021-Server-Side Request Forgery 40 0/40/0 40/0

A1:2021-Broken Access Control 115 76/39/0 112/3

A2:2021-Cryptographic Failures 157 76/81/0 154/3

A3:2021-Injection 40 0/40/0 40/0

A6:2021-Vulnerable and Outdated Components 41 1/40/0 40/1

1 Week

5/1/2022 5/2/2022 5/3/2022 5/4/2022 5/5/2022 5/6/2022 5/7/2022 5/8/2022

Block Monitor Captcha

## New SAP signature type

FortiADC has added the new SAP web server signature type to the Signature Creation Wizard to protect web applications against SAP vulnerabilities.

**Note:** The SAP signature is only supported in WAF Signature Database versions 0034 or later.

## Log & Reporting

### Status check for FortiAnalyzer OFTP connectivity

You can now view and test the OFTP connectivity when configuring FortiAnalyzer.

## System

### New Declarative REST APIs

New declarative REST APIs allow users to configure system operations by using a single REST API (/api/declarative) with the essential declaration instead of requiring multiple REST APIs for system deployments and configurations.

- POST /api/declarative — sends the declarative API request.
- GET /api/declarative?id=xxxxxxx — gets the declarative API processing status.
- GET /api/declarative/sample — gets the current system configuration by declarative API format.

Example: Delete one user with declarative API

1. Deploy the declarative API request.

```
{
  "async": "True", ← Operation is async or not
  "Config": { ← All config starts from this block
    "root": { ← Config for VDOM "root"
      "mySysAdmin1": { ← User defined variable name
        "class": "systemAdmin", ← Operation type
        "comments": "aa",
        "is-system-admin": "yes",
        "name": "admin",
        "profile": "super_admin_prof",
        "trusted-host": "",
        "vdom": "root"
      },
      "mySysAdmin2": {
        "class": "systemAdmin",
        "comments": "bb",
        "is-system-admin": "yes",
        "name": "op1",
        "profile": "super_admin_prof",
        "trusted-host": "",
        "vdom": "root"
      }
    },
    "vdom1": { ← Config for VDOM "vdom1"
      "mySysAdmin1": {
        "class": "systemAdmin",
        "comments": "aa",
        "is-system-admin": "yes",
        "name": "op2",
        "profile": "super_admin_prof",
        "trusted-host": "",
        "vdom": "root"
      }
    }
  }
  ... (configuration of other classes)
}
```

2. To delete user **op1**, edit the declaration to remove user **op1**.

3. POST the updated declaration which no longer contain the entry for **op1** to the server.

```
{
  "async": "True",
  "Config": {
    "root": {
      "mySysAdmin1": {
        "class": "systemAdmin",
        "comments": "aa",
        "is-system-admin": "yes",
        "name": "admin",
        "profile": "super_admin_prof",
        "trusted-host": "",
        "vdom": "root"
      }
    },
    "vdom1": {
      "mySysAdmin1": {
        "class": "systemAdmin",
        "comments": "aa",
        "is-system-admin": "yes",
        "name": "op2",
        "profile": "super_admin_prof",
        "trusted-host": "",
        "vdom": "root"
      }
    }
  }
  ...(configuration of other classes)
}
```

### ACME enhancement

The FortiADC ACME feature now supports automatic certificate renewal through TLS-ALPN-01 challenge. When importing automated local certificates you can now select the Challenge Type between DNS-01 and TLS-ALPN-01. The new TLS-ALPN-01 Challenge Type allows you to specify a Renew Window to automatically renew the certificate before it expires.

Global ▾	Local Certificate	
Dashboard >	Type	Automated ▾
Security Fabric >	Certificate Name	Required config name. No spaces.
System ▾	Domain Name	Required. Specify the FQDN. <small>Example: example.com.</small>
Settings	Email	Required. Specify the email address.
Virtual Domain	Key Type	RSA ▾
High Availability	Key Size	2048 bit ▾
Administrator	Password	Specify the password if necessary.
SNMP	CA Group	Click to select. ▾
Replacement Messages	ACME Service	Let's Encrypt Other
FortiGuard	Challenge Type	TLS-ALPN-01 DNS-01
Debug	Renew Window	Required. Specify the renew window before cert expiration <small>Range: 0-43200 minutes; 0 means disable renew</small>
CERTIFICATE		
Manage Certificates		
Verify		

## GUI

### Child configuration enhancement

The process of creating a parent and child configuration has been simplified to allow the child configuration to be created on the same page after creating the parent configuration. The initial implementation phase covers most modules that can support the simplified workflow. For now, modules that have more complex backend relationships between the parent-child configurations, such as Virtual Domain configurations, will remain unchanged.

# Hardware, VM, cloud platform, and browser support

This section lists the hardware models, hypervisor versions, cloud platforms, and web browsers supported by FortiADC 7.1.0. 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)
- Alibaba Cloud

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.

## Resolved issues

The following issues have been resolved in FortiADC 7.1.0 release. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0823553	Dashboard is not displaying data.
0819097	Error message "merge warning" triggers when synchronizing GSLB through Sync List.
0818711	Following a successful request, some WAF modules are not scanning subsequent requests within the same session. Affected WAF modules: Brute Force Attack Detection, Cookie Security, JSON Detection, OpenAPI Validation, and XML Detection.
0818663	Cloned IPS signatures cannot be modified.
0818128	Cannot edit JSON schema entry.
0817934	JSON schema import failing.
0816794	Requests are incorrectly blocked when the Cookie Security is in "Signed" mode.
0816089	FortiSandbox Fabric Connector cannot connect type FSA.
0815454	Client timeout settings limited to 3600 seconds or less.
0814475	Google OAuth authentication code verification fails with "Malformed auth code" and "match scope failed".
0810998	Local and remote administrative users unable to log in through GUI.
0810275	In an HA environment, the certificate embedded license is being synchronized to the peer device. The license should not be synchronized to the peer because each device requires a unique license.
0808086	FortiADC does not process some requests when using the WAF profile.
0807522	Cannot add system admin using default Ansible playbook.
0806865	False positives triggered in DOS HTTP request flood protection due to inaccurate request count caused by timer being too busy.
0806321	Email alerts is being sent in TLS 1.0, but since TLS versions 1.2 or lower has been deprecated, connections lower than TLS 1.2 is not being accepted.
0805167	User access issue on VDOM permission due to REST API return error.
0804514	HA status incorrectly show as "Not Sync".
0804489	L7 VS accepts only one SSH session.

Bug ID	Description
0795719	GSLB Cloud Connector and CLI commands not working.
0793892	DNS cannot resolve when there are many addresses for one FQDN.
0783548	FortiADC resets MySQL connection when concurrent connections are set for MySQL service in L7 VS.
0779734	If a FortiADC device is deleted from FortiAnalyzer as an authorized device, there is no indication on the FortiADC side that the channel has been disconnected.
0730266	Misleading server pool statuses.

### Common Vulnerabilities and Exposures

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

Bug ID	Description
0822315	FortiADC 7.1.0 is no longer vulnerable to the following CVE-Reference: CWE-228: Improper Handling of Syntactically Invalid Structure.



## Known issues

This section lists known issues in version FortiADC 7.1.0, but may not be a complete list. For inquiries about particular bugs, please contact [Fortinet Customer Service & Support](#).

Bug ID	Description
0829750	fnginxctld crash based on issue with longer loading time for websites going through FortiADC.
0828572	200D/100F/200F/1000F/2000F/4000F incorrectly uses FortiADC-VM as the CN (Common Name) for the default certificate Subject, which may cause FortiSandbox Cloud connection issues. This is expected to be fixed in the next release.
0827447	miglogd crash related to FortiAnalyzer.
0826540	<p>In the GUI, failed to append child list when configuring Automation. This results when an alert type has reached the maximum entry capacity. The current maximum is 256 entries for each alert type, as categorized in the backend CLI:</p> <ul style="list-style-type: none"> <li>• <code>config system alert-policy</code></li> <li>• <code>config system alert-action</code></li> <li>• <code>config system alert</code></li> <li>• <code>config system alert-email</code></li> <li>• <code>config system alert-snmp-trap</code></li> <li>• <code>config system alert-script</code></li> <li>• <code>config system alert-webhook</code></li> <li>• <code>config system alert-fortigate-ip-ban</code></li> <li>• <code>config system alert-syslog</code></li> </ul> <p><code>config system alert-policy</code> configurations are often composed of multiple <code>config system alert</code> entries, making the <code>config system alert</code> most likely to exceed the entry capacity. Please use <code>show full-configuration system alert</code> for details in the CLI.</p> <p><b>Workaround:</b> After figuring out which alert type has exceeded the 256 entry capacity from the backend CLI, remove any unused automation alerts from the GUI.</p>
0824203	There are some defects with the Country and phone number on the local user page and system Administrator page.
0823021	Timeout issue when creating a 2FA-local user and 2FA Administrator.
0822565	CLI and GUI response is not the same when creating a 2FA-local user.
0822356	New mysqld (MariaDB 10.6.7) will crash when it meets a corrupted database table. This behavior did not occur in the previous version because the corrupted database table would have been ignored.

Bug ID	Description
	<b>Workaround:</b> Run the CLI command <code>execute log rebuild</code> to rebuild the Database.
0820293	FortiADC shows "bind failed(30002372)" warning during automation test.
0819547	When importing the automated local certificate through GUI, if the internet connection is down or too slow, it will cause the certificate generation to fail due to server timeout. It may take several seconds to receive the timeout error, during which the GUI will be non-responsive.
0816798	<p>In an HA environment, if you are using a predefined automation configuration, resetting the configuration through the GUI (using the reset button) or unsetting comments through CLI will cause the HA synchronization to fail whenever a device reboots and rejoins the cluster. Using the GUI reset button resets the predefined configuration values to the predefined default values, all except the comments value which is set to the default value on the backend. For example, if using the HA predefined configuration, the reset will result in <code>set comments HA</code> → <code>set comments comments</code>. When a new device (or a rebooted device) joins the HA cluster, the synchronization will fail due to the mismatched <code>set comments</code> value between the device that has the predefined default value (<code>set comments HA</code>) and the reset device that has the default value (<code>set comments comments</code>).</p> <p>In the CLI, if <code>set comments</code> in the predefined configuration has been unset and is the default value <code>set comments comments</code>, then the same HA synchronization issue will occur.</p> <p><b>Workaround:</b> In the CLI, edit <code>set comments</code> to ensure it is <b>not</b> the default value (<code>set comments comments</code>) and it matches the value of the predefined configuration (for example, <code>set comments HA</code>).</p>
0811061	When using CLI command <code>conf-sync</code> to get a configuration file more than 10 MB, the operation may get stuck showing only "auth access", unable to retrieve the file.
0798862	Health Check does not support RFC 7919 yet.
0782143	From the GUI, if the FortiAnalyzer is cloned, the OFTP connection of the original configuration will disconnect, with debug showing it has stopped the connection to the FortiAnalyzer server.

# 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

The screenshot shows the Fortinet Customer Service & Support website. At the top, a blue banner displays 'Home' and 'Welcome Samuel Liu' with a note about time zones. Below this is a 'Customer Support Bulletin' section with three items: 'AV engine 5.355 released to FortiGuard AV engine update will be available on the FortiGuard network...', 'IPS engine 3.532 released to FortiGuard for FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...', and 'IPS engine 3.532 released to FortiGuard for FDS 5.6 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.6)...'. A 'More' button is present. The main content area is divided into 'Asset' and 'Assistance' sections. 'Asset' includes 'Register/Renew' and 'Manage Products'. 'Assistance' includes 'Create a Ticket', 'Manage Tickets', 'View Active Tickets', 'Technical Web Chat', and 'Contact Support'. At the bottom, there are 'Quick Links' and 'Resources' sections. In the 'Quick Links' section, 'Firmware Images' and 'VM Images Download' are highlighted with a red box. The 'Resources' section lists various support resources like 'Customer Support Bulletin', 'Knowledge Base', 'Fortinet Video Library', 'Fortinet Document Library', 'Discussion Forums', and 'Training & Certification'.

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 FDS 5.4 Release of a new IPS Engine to FortiGuard Distribution Network (FortiOS 5.4)...
3. IPS engine 3.532 released to FortiGuard for FDS 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 7.1.0.

## 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 5.3.5 to 6.1.5, you will follow the upgrade path below:

5.3.5 → 5.4.x → 6.0.x → 6.1.5

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

### 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.


Firmware			
<a href="#">Upgrade Firmware</a>			
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
<a href="#">Boot Alternate Firmware</a>			

### 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](https://en.wikipedia.org/wiki/Wikipedia:Bypass_your_cache).

---

## Special notes and suggestions

### 7.1.0

- HSM does not 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 are using the HSM certificate to avoid potential handshake failure.
- Keep the old SSL version predefined configuration to ensure a smooth upgrade.

### 7.0.2

- After upgrading to 7.0.2, 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®**



Copyright© 2023 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.