

# Release Notes

**FortiSandbox PaaS 5.2.0**



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



June 9, 2026

FortiSandbox PaaS 5.2.0 Release Notes

34-520-1293244-20260612

# TABLE OF CONTENTS

<b>Change Log</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Upgrade Information</b> .....	<b>6</b>
Before and after any firmware upgrade .....	6
Upgrade path .....	6
Upgrade procedure .....	7
Downgrading to previous firmware versions .....	8
<b>Product Integration and Support</b> .....	<b>9</b>
<b>Resolved Issues</b> .....	<b>10</b>
Common vulnerabilities and exposures .....	10

# Change Log

Date	Change Description
2026-06-09	Initial release.

# Introduction

This guide provides release information for FortiSandbox PaaS version 5.2.0 build 0290.

- [Upgrade Information on page 6](#)
- [Product Integration and Support](#)

For information on deploying and maintaining FortiSandbox PaaS, see the [FortiSandbox PaaS 5.2.0 Deployment Guide](#).

For details about FortiSandbox features, refer to the [FortiSandbox Release Notes](#) and [FortiSandbox Administration Guide](#).

# Upgrade Information

## Before and after any firmware upgrade

Before any firmware update, complete the following:

- Download the FortiSandbox firmware image and Release Notes document from the [Fortinet Customer Service & Support](#) portal. Review the Release Notes, including the special notices, upgrade information, product integration and support, and resolved and known issues.
- Backup your configuration file. It is highly recommended that you create a system backup file and save it to your management computer. You can also schedule to back up system configurations to a remote server.
- Plan a maintenance window to complete the firmware update. If possible, you may want to setup a test environment to ensure that the update does not negatively impact your network.
- Once the update is complete, test your FortiSandbox device to ensure that the update was successful.



### Firmware best practice:

Stay current on patch releases for your current major release. Only update to a new major release or version when you are looking for specific functionality in the new major release or version. For more information, see the FortiSandbox Release Notes or contact [Technical Support](#).

### To update the FortiSandbox firmware:

1. Go to *Dashboard > Insights > System Information* widget.
2. Click the widget and select *Update Firmware* from the options list.
3. Click the *View all firmware* link beside *Firmware Version*.
4. Click *Upload firmware* and then click *Upload File* to locate the firmware image on your management computer.
5. Click *Submit* to start the upgrade.



The image file name For FortiSandbox PaaS starts with FSA\_CLP.

## Upgrade path

FortiSandbox PaaS is maintained separately from the main GA release. Use the specific builds as listed in the upgrade information table below.

FortiSandbox PaaS 5.2.0 officially supports the following upgrade path.

From	To
5.0.6 build 8020	5.2.0 build 0290
5.0.2 build 8005, 5.0.4 build 134, 5.0.5 build 155	5.0.6 build 8020
24.1 build 4436	5.0.2 build 8005
23.4 Build 4374	24.1 build 4436
23.4 Build 4367	24.1 build 4436
23.4 Build 4350	23.4 Build 4374
23.3 Build 4329	23.4 Build 4374
23.2 Build 4260	23.3 Build 4374
23.1 Build 4245	23.3 Build 4374
22.2.1 Build 4151	23.1 Build 4374
22.2 Build 4134	23.1 Build 4260
22.1 Build 4113	22.2.1 Build 4134



To obtain these builds, please contact Fortinet Customer Support.

## Upgrade procedure

You can manually download then upgrade the FortiSandbox PaaS firmware or click the blinking link beside *Dashboard > System Information widget > Firmware Version* to be redirected to a page where you can download and install the available firmware automatically.

### To manually update the firmware:

1. Download the firmware image from the [Fortinet Customer Service & Support](#) portal.
2. Go to *System > Dashboard*. In the *System Information* widget, click the *View all firmware* icon next to *Firmware Version*. The *FortiSandbox Firmware Information* page opens.
3. Under *Upload Firmware*, click *Upload Firmware*.
4. Click *Upload File* and *browse* to the firmware image on your computer and click *Submit*.

## Downgrading to previous firmware versions

Downgrading to previous firmware versions is not supported.

# Product Integration and Support

The following table lists FortiSandbox PaaS version 5.2.0 product integration and support information.

<b>Web browsers</b>	<ul style="list-style-type: none"><li>• Google Chrome version 147</li><li>• Microsoft Edge version 147</li><li>• Mozilla Firefox version 147</li></ul> Other web browsers may function correctly but are not supported by Fortinet.
<b>FortiOS/FortiOS Carrier</b>	<ul style="list-style-type: none"><li>• 8.0.0</li><li>• 7.6.0 and later</li><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li></ul>
<b>FortiMail</b>	<ul style="list-style-type: none"><li>• 8.0.0</li><li>• 7.6.0 and later</li><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li></ul>
<b>FortiClientEMS/FortiClient</b>	<ul style="list-style-type: none"><li>• 7.4.0 and later</li><li>• 7.2.0 and later</li></ul>

# Resolved Issues

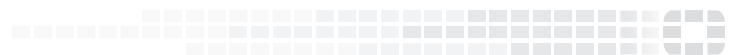
The following issues have been fixed in version 5.2.0. For inquiries about a particular bug, contact [Customer Service & Support](#).

## Common vulnerabilities and exposures

Bug ID	Description
1245752	FortiSandbox PaaS 5.2.0 is no longer vulnerable to the following CVE Reference: <ul style="list-style-type: none"><li>• CVE-2026-25089</li></ul>



**FORTINET®**



Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.