



Release Notes

FortiGuest 2.4.1



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

Oct 13, 2025

FortiGuest 2.4.1 Release Notes

70-1213274-241-20251013

TABLE OF CONTENTS

Change log	4
About this Release	5
Product Overview	6
Product Integration and Support	7
Common Vulnerabilities and Exposures	9
Resolved Issues	10

Change log

Date	Change description
2025-10-13	FortiGuest 2.4.1 release version.

About this Release

This release delivers key bug fixes. For more information, see [Resolved Issues](#).

Notes:

- Multi Pre Shared Key (MPSK): When an MPSK device is created, it gets its own Device Account Group (mapped under Guest Portal Access Plan). When the device actually connects, the authorization policy/profile decision is not based on the Device Account Group. Instead, it uses the User Account Group (to which the MPSK is mapped or bound).
- Change the interface IPs to static mode and configure static routes for interfaces before upgrading. This is because DHCP IP configuration is not supported in this release. To configure static IP addresses and routes, see the *FortiGuest Administration Guide*.
- CLI/GUI passwords:
 - After an upgrade, the CLI password remains the same until a user logs in using the GUI. Once the first successful GUI login occurs, the CLI password is automatically synchronized and set to match the GUI password.
 - On the first bootup of a new instance, a user must first log in using the CLI and change the default password. Once the CLI password is updated, it will also be used for logging into the GUI.
- Starting with FortiGuest version 1.3.0, support for time zones is limited to 132, down from 416 in previous releases. When upgrading from a version older than 1.3.0, any unsupported time zone setting will be automatically reset to UTC.
- Only one of the four port interfaces can support DHCP configuration at a time.

Product Overview

FortiGuest is a complete provisioning, management, and reporting system that provides network access for guests, visitors, contractors, consultants, or customers. FortiGuest works along side wireless controllers (FortiGate), LAN switches, NAC systems, firewalls, and other network enforcement devices that provide captive portal and enforcement point for user/remote user access. When user accounts are created, they are stored within the built-in database on the FortiGuest server. When using this database, external network access devices can authenticate users against FortiGuest using the RADIUS protocol. For more information, see the *FortiGuest User Guide* and the *New Features* document for this release.

Product Integration and Support

This section describes the following support information for FortiGuest.

- [FortiGuest GUI](#)
- [Captive Portal](#)
- [Virtual Appliance](#)

FortiGuest GUI

The following table lists the latest tested devices and web browsers for FortiGuest GUI.

Browser/Device	Version
Apple iOS	18.x and above
Apple iPad	18.x and above
Android	13 and above
Google Chrome	129.0.6668.110(64-Bit)
Mozilla Firefox	134.0
Safari	17.5
Windows	10 (1809 and above)

Captive Portal

The following table lists the latest tested devices and web browsers for captive portal.

Browser/Device	Version
Apple iOS	18.x and above
Apple iPad	18.x and above
Android	13 and above
Google Chrome	129.0.6668.110 (64-Bit)
Mozilla Firefox	134
Safari	17.5
Windows	10 (1809 and above)

Smart Connect

The following table lists the latest tested devices and web browsers for Smart Connect.

Browser/Device	Version
Windows	10 (1809 and above)
Linux-Ubuntu	20.04, 22.04, and 24.04
iOS	18.x
macOS	14.5
Chromebook	129.0.6668.110 (64-Bit)
Android	13, 14, 15

Note: Browser versions not listed in this section may work correctly but Fortinet does not support them.

Virtual Appliance

The following virtual appliance system requirements apply to this release of FortiGuest.

Platform	Version
VMware ESXi	7.0.3 and above
Microsoft Hyper-V	Windows 10 and above
Linux KVM	1.5.3 and above
Nutanix	20220304.342
Proxmox	9.0.3

Note: The supported CPUs include Intel Core i5 and higher.

The following minimum hardware specifications required for virtual appliances.

- 8 core CPUs
- 8 GB memory
- 500 GB disk space

Common Vulnerabilities and Exposures

Visit <https://www.fortiguard.com/psirt> for more information.

Resolved Issues

The following issues are resolved in this release of FortiGuest.

Issue ID	Description
1208368	If the Guest Portal default page is set to the self-service page while Remember Me is enabled, clients must manually navigate to the login page for the Remember Me feature to work.
1202917	The GUI incorrectly displays the error <code>Invalid OTP entered by user</code> , even when the correct OTP is provided. This issue is seen when there is a delay in the user entering the OTP.

www.fortinet.com



Copyright© 2025 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.