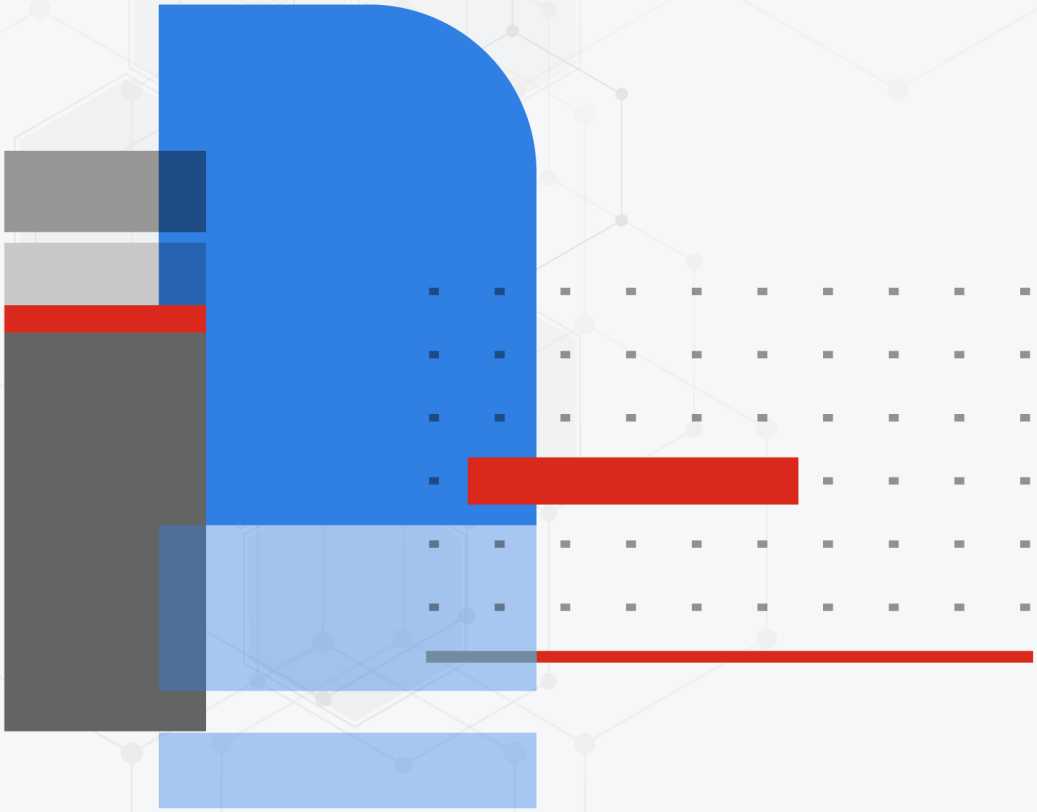
Release Notes

FortiGuest 1.2.2



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 26, 2024
FortiGuest 1.2.2 Release Notes
70-1005093-122-20240926

TABLE OF CONTENTS

Change log

Date	Change description
2024-08-29	FortiGuest 1.2.2 release version.
2024-09-05	Updated section About this Release.
2024-09-26	Updated section Known Issues.

About this Release

This release resolves some key vulnerabilities. For more information, see Common Vulnerabilities and Exposures.

Notes:

- The supported FortiOS versions are 7.4.4 and 7.6.0.
- Upgrade to current release of FortiGuest is supported only from version 1.2.0/1.2.1.
- [Smart Connect] For PEAP to work with Windows 10 devices, ensure that a FortiGuest certificate is included in the **Additional Certificates** of a Smart Connect profile.
- [Windows 11] Update the client's registry settings to ensure that TLS 1.2. is used for EAP authentication.
- Password complexity requirements are not enabled for the CLI.

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

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

Browser/Device	Version
Apple iOS	15.x
Apple iPAD	9.2.1 and 9.3.5
Android	12 and 13
Google Chrome	109.0.5414.120
Mozilla Firefox	109
Safari	12.1.2, 15.5, and 16.1.1
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	15.x
Apple iPAD	9.2.1 and 9.3.5
Android	12 and 13
Google Chrome	109.0.5414.120
Mozilla Firefox	109
Safari	12.1.2, 15.5, and 16.1.1
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 and 11-Pro
Linux-Ubuntu	20.04 and 22.04
iOS	15 and 16
macOS	12.04
Android	12 and 13

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

The following minimum hardware specifications required for virtual appliances.

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

Common Vulnerabilities and Exposures

This release of FortiGuest is no longer vulnerable to the following.

- CVE-2024-3596
- CVE-2024-39894
- CVE-2024-6387

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

Known Issues

These are the known issues in this release of FortiGuest.

Issue ID	Description
894407	TLS version 1.3 is not supported on FreeRADIUS.
913048	The CoA and logout functionalities are not working accurately for Meraki controllers (RADIUS clients).
966162	Setting the time zone through the graphical user interface (GUI) does not persist when checked using the command-line interface (CLI).
966166	Time based sorting fails in RADIUS authentication reports.
974257	[Hyper-V] All four network interfaces are selected as default when FortiGuest instance is brought up. You are required to manually un-select the irrelevant interfaces.
1080936	The user interface does not respond after restoring a backup file with multiple guest portal configurations.

www.fortinet.com