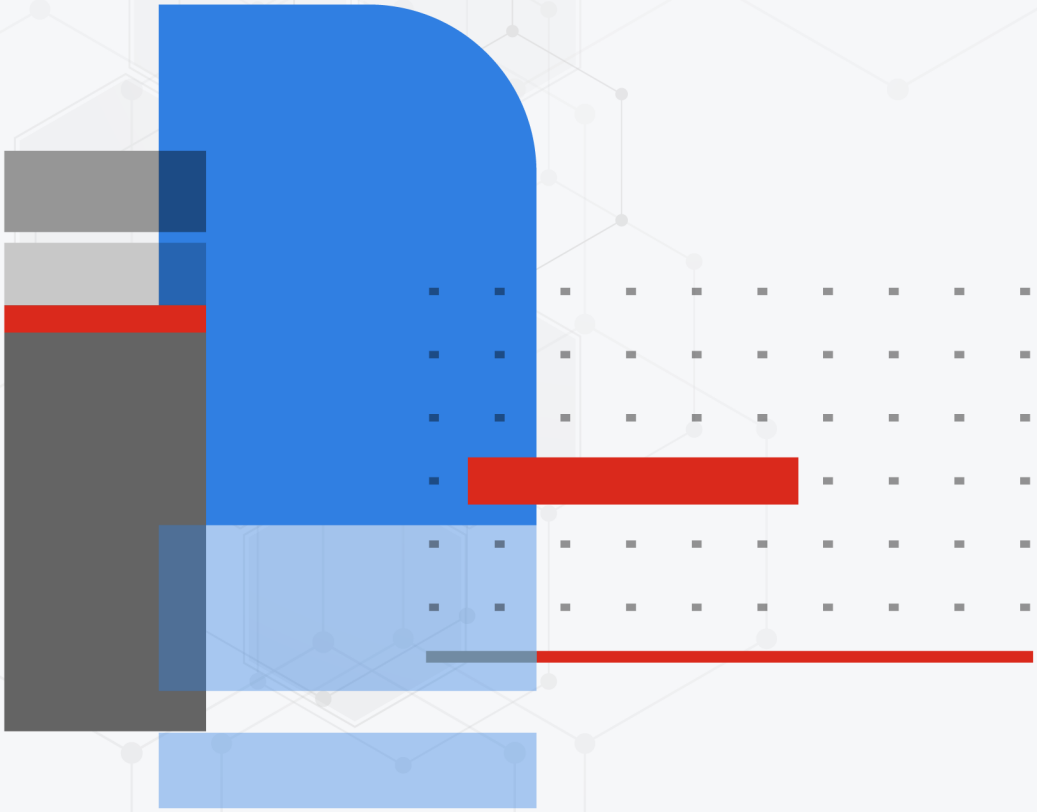
Release Notes

FortiGuest 2.4.3



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

April 17, 2026
FortiGuest 2.4.3 Release Notes
70-1280014-243-20260417

TABLE OF CONTENTS

Change log

Date	Change description
2026-04-17	FortiGuest 2.4.3 release version.

About this Release

This release delivers key new features and few bug fixes. For more information, see What's New and Resolved Issues sections.

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).
- 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.
- 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

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.

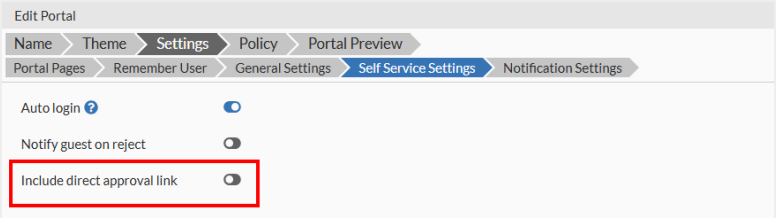
Platform	Version
VMware ESXi	7.0.3 and above
Microsoft Hyper-V	Windows 10 and above
Linux KVM	1.5.3 and above
Nutanix	20220304.342
Proxmox	9.0.3 **Note**: The supported CPUs include Intel Core i5 and higher.

The following minimum hardware specifications required for virtual appliances.

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

What's New

This section describes the key features of FortiGuest.

Feature	Description
Enhanced Sponsor Approval Workflow	This feature introduces a new configuration option, **Include direct approval link** under **Guest Portal** > **Settings** > **Self Service Settings**. This option enables you to customize the sponsor approval process.  When **Include direct approval link** is: • **Enabled**: Sponsors can approve or reject guest accounts directly from the email using embedded links. • **Disabled**: The email contains a link that directs the sponsor to the FortiGuest portal to log in and manage the approval.
SAML-only Admin Authentication	This feature introduces a SAML-only login option for the Admin Portal. When enabled, the portal displays a dedicated **Login with SAML** button and restricts authentication exclusively to SAML based identity providers, disabling local user account logins for enhanced security and centralized access management.

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
809753	The system experiences `too many clients` database error, with active connections exceeding the 100-connection limit, preventing the **Create Account** page from loading.
1192931	When FortiGuest logging is configured to `Errors Only` or `Admin Operations, General, and Security`, the log storage to reached 103 GB, rendering the system inaccessible.
1227159	When the **Content background color** is set to transparent, the button text becomes invisible.
1252478	Though the bandwidth limit is set to 3 GB, FortiGuest fails to send CoA disconnection requests to the Fortigate.

Known Issues

The following is the known issue in this release of FortiGuest.

Issue ID	Description
1150476	Captive Portal authentications may fail for new AD accounts if login occurs within a minute of creation during restricted usage periods, as RADIUS rejects access before profile restrictions apply.

www.fortinet.com