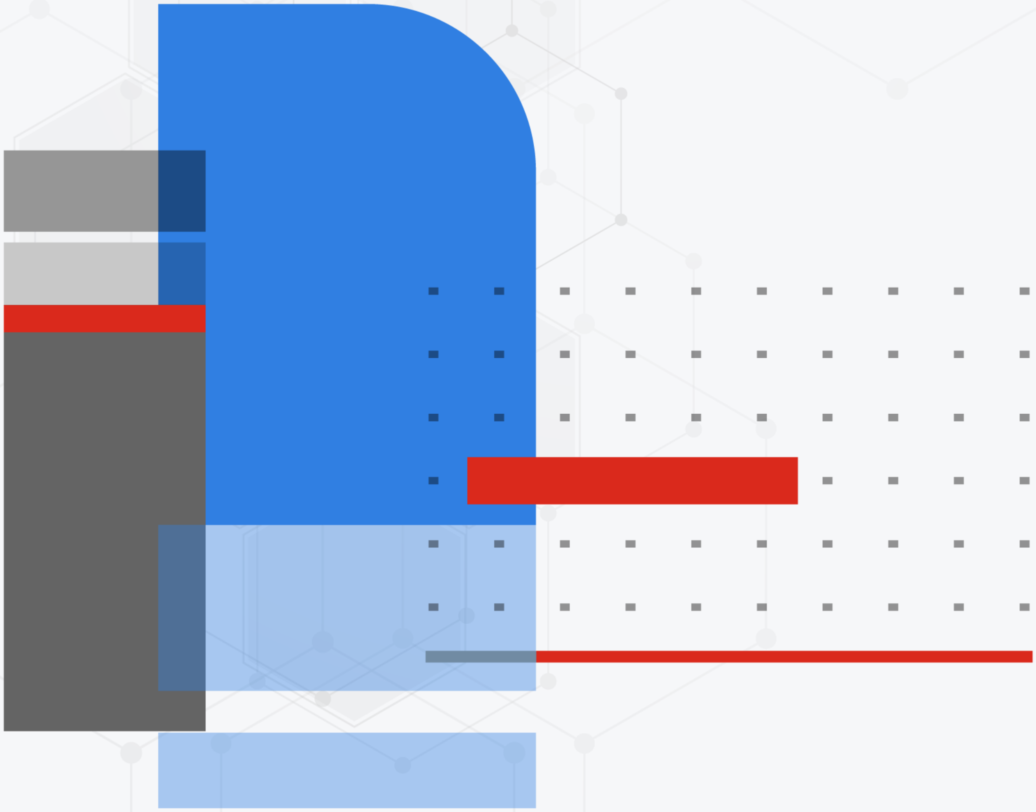
Release Notes

FortiGuest 2.2.0



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

May 23, 2025
FortiGuest 2.2.0 Release Notes
70-1150500-220-20250523

TABLE OF CONTENTS

Change log

Date	Change description
2025-05-08	FortiGuest 2.2.0 release version.
2025-05-23	Updated Known Issues section.
2025-06-05	Updated Product Integration and Support section.

About this Release

This release delivers key new features. For more information, see What's New.

Notes:

- For FortiEdgeCloud AP in standalone mode, you must configure the RADIUS type as FortiEdgecloud AP.
- Use the latest version of Smart Connect application with FortiGuest as it has important security enhancements. Older versions of Smart Connect app will no longer work with FortiGuest 1.3.1 onwards.
- Upgrade to current release of FortiGuest is supported only from version 1.2.0, 1.2.1, 1.2.2, 1.3.0, 1.3.1, and 2.0.0.
- Password complexity requirements are not enabled for the CLI.
- This release supports only 132 timezones in contrast to the 416 timezones supported in the previous releases. Hence, after upgrade to the current version, if your timezone is not supported, then FortiGuest sets it 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
Apple iPAD	18.x
Android	11, 12, 13, and 14
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
Apple iPAD	18.x
Android	11, 12, 13, and 14
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 and 11- Pro
Linux-Ubuntu	20.04, 22.04, and 24.04
iOS	18.1
macOS	14.5 (23F79-Sonoma)
Chromebook	129.0.6668.110 (64-Bit)
Android	11, 12, 13, and 14

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	6.5.2 LTS
Proxmox	8.4.1 **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
Support for OTP Authentication	FortiGuest now supports One-Time Password (OTP) authentication for accessing portals. This provides a more secure login process using time-sensitive, unique codes, while also improving ease of use.
Voucher Codes	This release introduces Voucher Codes. These new codes are generated and used in the same way as the existing event codes but offer the key advantage of having no time limitations. This provides increased flexibility for use cases such as extended promotions and ongoing access where time-sensitive codes are not ideal.
Improved Help Component	FortiGuest now features a significantly improved Help menu. This enhanced menu provides context-sensitive documentation for the current window, along with quick access to release notes and a range of support resources, including the Fortinet Community and Knowledge Base articles.
Simplified Captive Portal Access	Accessing the captive portal is now simplified. This release allows direct access to the Redirect URL from any internet source, eliminating the need to first authenticate to the Wi-Fi network (SSID) for a quicker, more convenient process.

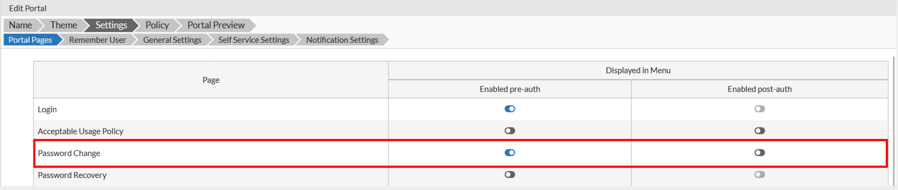
Resolved Issues

These issues are resolved in this release of FortiGuest.

Issue ID	Description
1125764	The FortiGuest Portal Rules interface displays a maximum of 40 entries, with the first rule disappearing when a 41st rule is added.
1130829	SAML authentication failures caused by attribute mismatches like Entity ID or SSO/Logout URLs in the backend are not logged accurately and reports a Redis unavailable session error.
1132626	Configuring an SFTP backup policy with a custom port results in backup failure.
1147538	Social media authentication fails with an `Oauth failed to get token (invalid client)Unauthorized` error.

Known Issues

These are the known issues in this release of FortiGuest.

Issue ID	Description
1104480	EAP-TLS authentication fails on Android devices when using WPA3 Enterprise 192-bit security.
1106355	In a scale setup, the initial MPSK client connection fails, but subsequent clients connect successfully.
1106848	Enhancement: WPA3 192 support for Elliptic Curve (EC) algorithm-based certificates.
1112645	Windows 10 devices are unable to add WPA3 Enterprise Only / Transition mode networks (Smart Connect also fails).
1155255	An account group can be created without specifying a name.
1150476	Captive Portal authentication failure occurs when users log in immediately on the same page after creating a self-service account.
1153935	Accounting Failure is observed on FortiGuest when Pseudo Username is provided during EAP-TLS authentication.
1154807	FortiGuest does not send COA-Disconnect packets to the FortiGate.
1155851	A system error occurs on the captive portal when users attempt to change their password post auth. **Workaround**: Select the portal and navigate to **Edit Portal** > **Settings** > **Portal Pages**. For Password Change, enable **Enabled pre-auth** and disable **Enabled post-auth**.  Edit Portal Name > Theme > Settings > Policy > Portal Preview Portal Pages > Remember User > General Settings > Self Service Settings > Notification Settings Page | Displayed in Menu: Enabled pre-auth | Enabled post-auth Login | ● | ○ Acceptable Usage Policy | ○ | ○ Password Change | ● | ○ Password Recovery | ○ | ○
1141818	On Hyper-V FortiGuest instance, the **Run Upgrade** button is not visible after a successful image upload when performing an upgrade from version 2.0.0 to 2.2.0. **Workaround**: Run the upgrade from the Command Line Interface (CLI). For information, see Upgrading Firmware.

www.fortinet.com