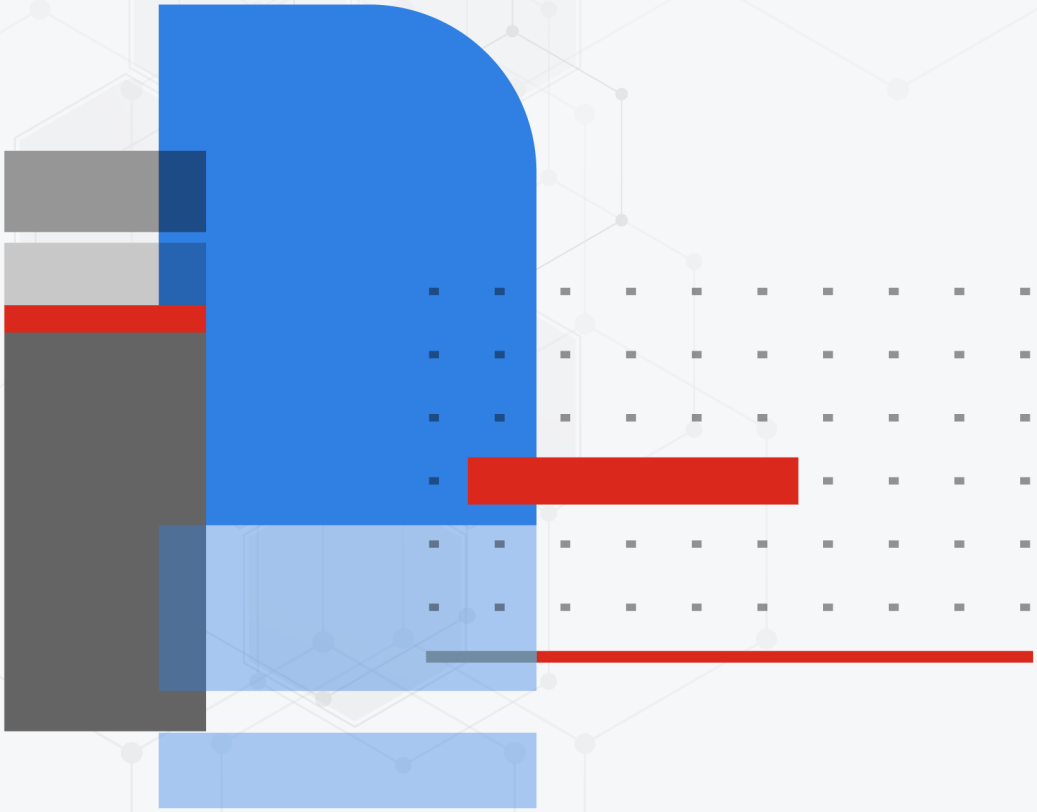
Release Notes

FortiGuest 2.4.0



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

Sep 22, 2025
FortiGuest 2.4.0 Release Notes
70-1201728-240-20250922

TABLE OF CONTENTS

Change log

Date	Change description
2025-09-22	FortiGuest 2.4.0 release version.

About this Release

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

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

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.

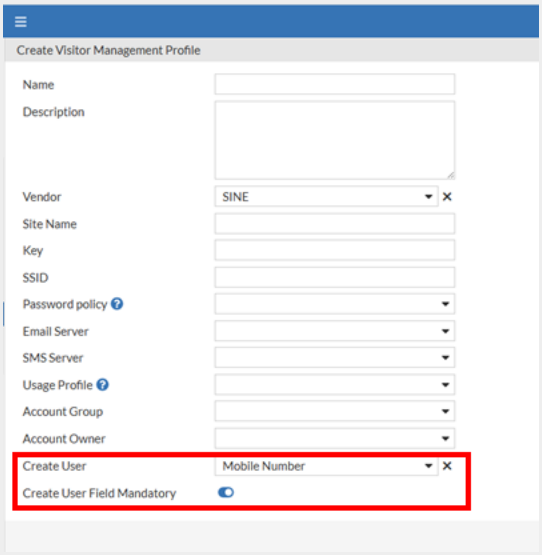
Platform	Version
VMware ESXi	7.0.3 and above
Microsoft Hyper-V	Windows 10 and above
Linux KVM	1.5.3 and above
Nutanix	20220304.342
Proxmox	9.0.3 **Note**: The supported CPUs include Intel Core i5 and higher.

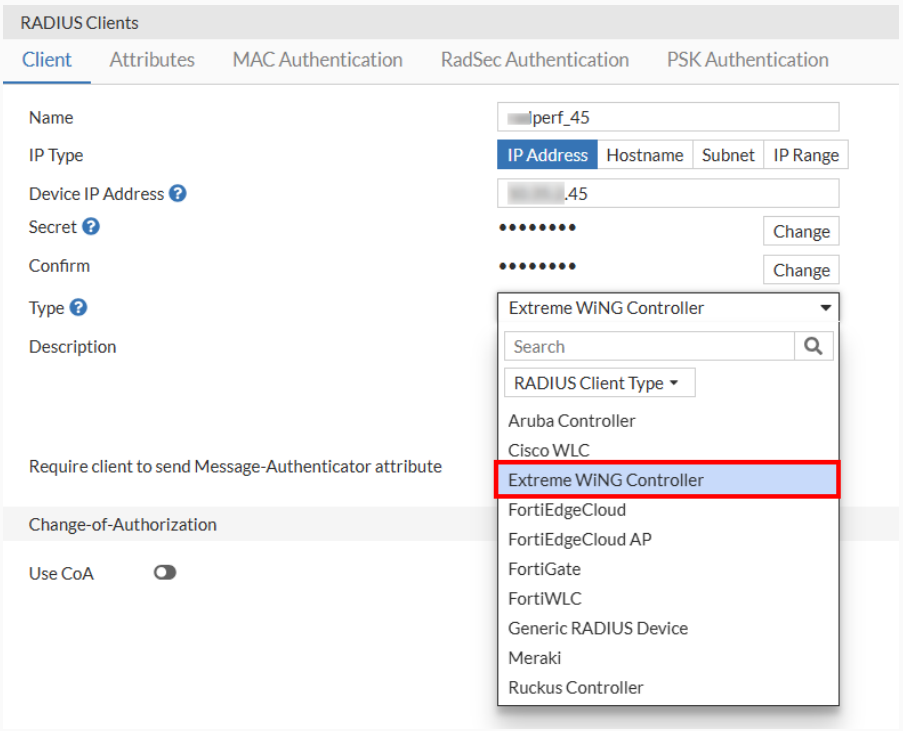
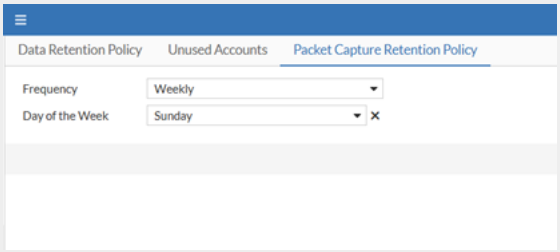
The following minimum hardware specifications required for virtual appliances.

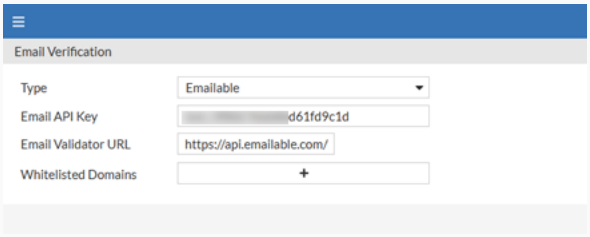
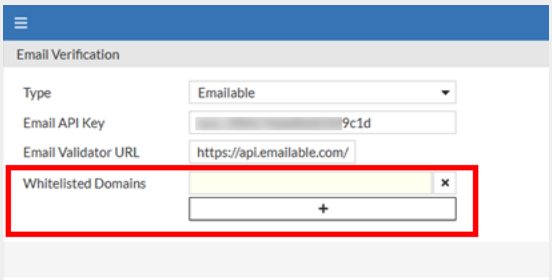
- 8 core CPUs
- 8 GB memory
- 500 GB disk space

What's New

This section describes the key features of FortiGuest.

Feature	Description
Visitor Management: Flexible User Creation	From this release, visitors can register using either a phone number or an email. By default, the system prioritizes the phone number as the username, but if it is not provided, the email address is used instead. On the Visitor Management window, administrators can now set a default preference for username (phone number or email) using the new **Create User** field. If a visitor provides both, the system uses the administrator's chosen default. If only one is provided, it is used as the username. Additionally, administrators can make their preferred contact information mandatory by enabling the **Create User Field Mandatory** option, which requires visitors to provide either a phone number or an email to create an account. 
RADIUS Support for Extreme Networks WiNG Controller	FortiGuest now supports Extreme Networks WiNG Controller, expanding its compatibility beyond the already supported vendors, which include Aruba Controller, Cisco WLC, FortiEdge Cloud, FortiEdge Cloud AP, FortiGate, FortiWLC, Generic RADIUS Device, Meraki, and Ruckus Controller. To select Extreme Networks WiNG Controller as vendor type, navigate to **Devices** > **RADIUS Clients**.

Feature	Description
	
Packet Capture Retention Policy	This release introduces a new feature that lets you set a data retention policy for packet captures on interfaces with RADIUS authentication enabled. This automatically deletes old, unnecessary data, which helps prevent the database from slowing down. To define this policy, navigate to **System** > **Data Retention Policy** > **Packet Capture Retention Policy**.  In the **Frequency** field, you can select how long you want to keep the data. The options available are: • **Daily**: Keeps packet data from the last 24 hours and deletes the rest. This is the default option. • **Weekly**: Retains the last one week data. You can choose which day of the week the retention period begins using the Day of the Week dropdown. • **Monthly**: Keeps the last one month data. You can select the day of the month for the retention period to begin using the Day of the Month dropdown.

Feature	Description
Email Verification for Guest Portals	A new option is now available for administrators to verify a visitor's email address. When the **Verify Email** option is enabled for a portal, FortiGuest sends the visitor's email to an external validation provider through an API. Based on the response (e.g., "valid," "invalid," or "disposable"), the visitor is either allowed to proceed or blocked. The following email validation providers are currently supported: • Neverbounce (https://api.neverbounce.com/v4/single/check) • Zerobounce (https://api.zerobounce.net/v2/validate) • Kickbox (https://api.zerobounce.net/v2/validate) • Emailable (https://api.emailable.com/v1/verify) • Hunter (https://api.hunter.io/v2/email-verifier) To enable email verification, navigate to **Portals** > **Settings** > **General Settings** and enable **Verify Email**. The email validation settings can be configured in the new **Email Verification** window. Navigate to **Guest Portal** > **Email Verification** and specify the following:  • **Type**: Select the type of validation from the drop down. • **Email API Key**: Enter the API key for the type of validation selected. • **Email Validator URL**: Enter the URL for the validation type selected.
Domain Whitelisting	You can now whitelist specific domains for guest portals. When a visitor enters an email address with a whitelisted domain, FortiGuest bypasses the email validation step, letting the user proceed immediately. To add whitelist domains, navigate to **Guest Portal** > **Email Verification**. In the **Whitelisted Domains** field, add the domains using **+**. 
Enable SAML-only Login for Guest Portals	FortiGuest now supports SAML-only login for guest portals. The portal can be configured to accept only visitors with SAML logins, and local user accounts will not be able to sign in.

Feature	Description
	To enable SAML-only login, after you have configured the SAML settings in the **Authentication Policy**, navigate to **Guest Portal** > **Portals** > **Policy** > **Realm Policy** tab. In the **Allowed Realms** field, select only the SAML realm.

MPSK Improvements	This release improves the RADIUS `Access-Accept` message, providing more detailed information for device management and reporting. The message now includes:
	• The preshared key name by default.
	• The username field for self-created MPSK.
	• Fortinet-Group-Name, based on the authorization profile mapping.
	Following is a sample RADIUS `Access-Accept` message:
	`Sent Access-Accept Id 96 from 10.32.4.53:1812 to 10.37.5.65:17291 length 180`
	`(113) Message-Authenticator = 0x`
	`(113) Fortinet-Webfilter-Category-Allow = 0x01067c214a388f7e0210b9256def34a532692177d650c6364fa9a da041067eda5ed8a6c3f2febba45335d5d144e506040000000`
	`(113) Fortinet-PreShared-Key-Name = "ADMIN1"`
	`(113) Session-Timeout = 3591`
	`(113) User-Name = "test1"`
	`(113) Fortinet-Group-Name = "Staff"`
	`(113) Acct-Interim-Interval = 60`
	Authorization Profile Mapping
	When an MPSK device connects, the authorization policy is evaluated based on the account group of the guest user the MPSK is mapped to, rather than the device's account group.
	Note: Other authorization policy settings do not apply to MPSK devices.

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
1192931	FortiGuest becomes inaccessible after log usage reaches 103 GB. A system reboot is required to reduce the log size to 60 GB.
1161248	Thought the Active Directory (AD) group contains several hundred users, only 100 users are visible on the FortiGuest GUI.
1146172	Unable to select multiple users in the **Manage Users** window as the **Select All** option is unavailable.
1161218	IDSNext sends a packet stream with FIAS commands encapsulated in `\x02` and `\x03` bytes and the IDS Connector in FortiGuest interprets these as `\xa0`.
1172600	Alphanumeric room numbers to be supported in Hotel Property Management System.
1172641	When submitting a billing plan in the Hotel Property Management System, the following error message is displayed: `It wasn't possible to process this transaction please try again, if the problem persists please contact reception.`
1178534	In Authorization Profile, if only **Email Notifications** are enabled (with **SMS Notifications** disabled), user authorization fails due to absence of phone number.

Known Issues

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

Issue ID	Description
1204682	A system error is displayed when trying to access SmartConnect after logging into captive portal. This error occurs when a non-default SmartConnect policy with a condition is used.
1202388	After bringing up a new FortiGuest instance, the Radread service fails to start due to DHCP IP assignment failure during the initial deployment. This issue prevents authentication reports from being generated, showing them as empty. While Radius authentications themselves are successful, there are no authentication logs in the `radread-port1.log` file. In rare cases, even if the service does start, reports may still be missing, and the log file remains empty. **Workaround:** Restart Radread services using the following command: `systemctl restart radread`

www.fortinet.com