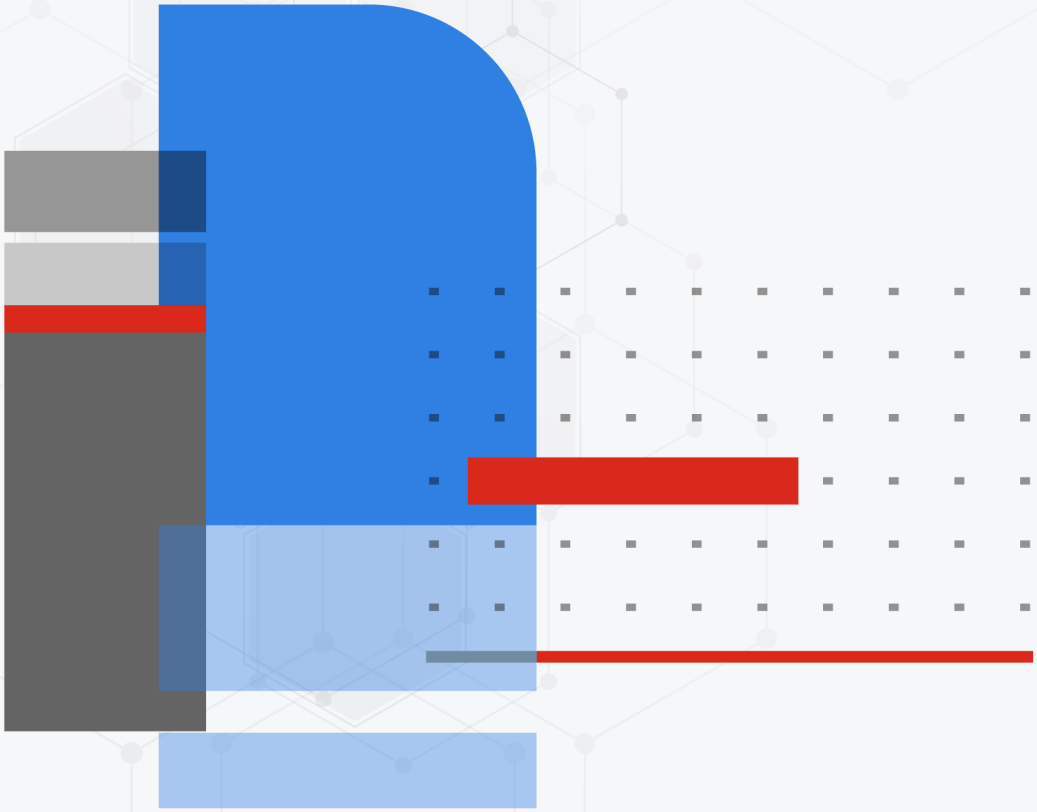
Release Notes

FortiGuest 2.0.0



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

Febuary 07, 2025
FortiGuest 2.0.0 Release Notes
70-1117196-200-20250207

TABLE OF CONTENTS

Change log

Date	Change description
2025-02-07	FortiGuest 2.0.0 release version.
2025-02-28	Updated Known Issues section.
2025-03-25	Updated Known Issues section and added Limitations section.

About this Release

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

Notes:

- New version of Smart Connect application is now available in the app stores (version 1.8.2 for Android and 2.0 for Windows). This new version of the app must be used with FortiGuest as it has an important security enhancement. 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, and 1.3.1.
- 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

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	20220304.342
Proxmox	8.3.3 **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
Event Codes	You can now configure unique event codes, which enable guest users to create their own accounts and access hot spots during specific events for specified time.
Smart Connect	Smart Connect profiles now support WPA3 Enterprise authentication for devices running the following operating systems. • Windows • Android • iOS • macOS • Linux • ChromeOS
Captive Portal	The following new features are added to Captive portal. • Captive portals can now be created in multiple languages. • Captive portals now supports a customizable secondary *Restriction Information* landing page with detailed information on access denial reasons, providing guest users with more context when they encounter usage limits or restrictions.
Multiple Pre-Shared Key (MPSK) Authentication	The following new features are added to MPSK. • Added MPSK accounting features, including support for all usage profiles and enhanced administrative control. • MPSK Authentication now supports devices using administrator created PSKs without prior MAC address registration or specific tagging.
Certificates	You can now, enter alternative names for the specified *Common Name* when generating Certificate Signing Request (CSR).
Upgrade	FortiGuest can now be upgraded from the GUI.
Others	• FreeRADIUS is upgraded to version 3.2.5, enabling native TLS 1.3.0 support. • DHCP can now be enabled for one of the four port interfaces at a time. • When using SCEP for certificate generation, FortiGuest now handles both revoked certificates with and without new replacements. • Enhanced password reset process with automatic password generation and user notification.

Common Vulnerabilities and Exposures

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

- CVE-2024-3596

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

Resolved Issues

These issues are resolved in this release of FortiGuest.

Issue ID	Description
1093510	Passwords are displayed in clear text in the *Password Change* and *Self Service* Portals.
1101432	Sponsor email verification fails if the email address contains uppercase letters.
1100927	Non-default authentication RADIUS port setting for external RADIUS server in Authentication policy are not applied.
1052626	Captive Portal authentication fails when using a SAML IdP realm.
1107289	Newly created account groups do not appear in the GUI when more than 100 account groups exist.
1113216	Sponsor names are not displayed in alphabetical order.

Known Issues

These are the known issues in this release of FortiGuest.

Issue ID	Description	Workaround
899774	Refreshing captive portal page creates a new self-service account.	
1104480	EAP-TLS fails to work with WPA3 Enterprise 192 bit security on Android devices.	
1112645	Unable to deploy WPA3 Enterprise profiles on Windows 10 devices.	
1121051	WPA3 Enterprise 192 bit security is not supported on Linux 20.04 devices due to operating system limitations.	
1106355	MPSK clients may fail to connect for the first time, but subsequent connections are not affected.	
1106848	SCEP server does not support certificates based on Elliptic Curve(EC) algorithm.	
1119653	Creating a new admin user can temporarily change the current admin user's language setting.	
1126946	MSCHAPv2 authentication fails with Microsoft Active Directory (AD).	
1136361	LDAP connection status displays `Strong(er) authentication required` error message.	On the LDAP server, make sure that Secure Connection is enabled and LDAPS is configured. On the domain controller, change the value of the parameter `ldapserverintegrity` on the LDAP server to 1: 1. Locate and then select the following registry subkey: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`. 2. Right-click the `LDAPServerIntegrity` registry entry, and then select **Modify**. 3. Change the value to 1 (default is 2). 4. Select **OK**.

Limitations

The following limitations apply to this release of FortiGuest.

- If RADIUS Authentication is by Access Point (AP), you must configure the RADIUS Type as FortiGate and not FortiLAN Cloud.

www.fortinet.com