



# Release Notes

FortiGuest 1.3.1



**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](mailto:techdoc@fortinet.com)

October 09, 2024

FortiGuest 1.3.1 Release Notes

70-1005093-131-20241009

# TABLE OF CONTENTS

<b>Change log</b>	<b>4</b>
<b>About this Release</b>	<b>5</b>
<b>Product Overview</b>	<b>6</b>
<b>Product Integration and Support</b>	<b>7</b>
<b>What's New</b>	<b>9</b>
<b>Common Vulnerabilities and Exposures</b>	<b>15</b>
<b>Known Issues</b>	<b>16</b>

## Change log

Date	Change description
2024-09-23	FortiGuest 1.3.1 release version.
2024-09-30	Content format changes in <a href="#">About this Release</a> .
2024-10-09	Updated <a href="#">Known Issues</a> .

## About this Release

This release delivers some enhancements and resolves system vulnerabilities. For more information, see [What's New](#) and [Common Vulnerabilities and Exposures](#).

**Notes:**

- New version of Smart Connect application is now available in the app stores (version 1.8.1 for Android and 1.4.2.0 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, and 1.3.0.
- 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*.
- 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.

## 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	15.x
Apple iPad	9.2.1 and 9.3.5
Android	12, 13, and 14
Google Chrome	125.0.6422.142
Mozilla Firefox	127.0.2
Safari	16.3
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, 13, and 14
Google Chrome	125.0.6422.142
Mozilla Firefox	127.0.2
Safari	16.3
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	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	8.1.4 <b>Note:</b> 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 release of FortiGuest delivers the following enhancements. For detailed configuration, see the *FortiGuest 1.3.1 User Guide*.

- [FQDN and IP Range Support for RADIUS Clients](#)
- [The Portal Redirection URL Supports RADIUS Client Type](#)
- [Managing message-authenticator in RADIUS](#)
- [NTP Settings from the User Interface](#)
- [License Status in the User Interface](#)
- [New Themes for Administrative Portal](#)

### FQDN and IP Range Support for RADIUS Clients

You can now configure the hostname/FQDN or the IP range when adding a RADIUS client in FortiGuest. Navigate to **Devices > RADIUS Clients**, additional options **Hostname** and **IP Range** are supported as the **IP Type**. The IP range can be specified with a hyphen, for example, *1.10.1.1 – 1.10.1.15*.

RADIUS Clients

Client

Attributes

MAC Authentication

RadSec Authentication

PSK Authentication

Name

RADIUS-FortiGuest

IP Type

IP Address

Hostname

Subnet

IP Range

Hostname ?

fortiguest.fortinet.com

## The Portal Redirection URL Supports RADIUS Client Type

You can now use the RADIUS client type to generate the redirection URL, this enables RADIUS clients of the same type to have a common redirection URL. Optionally, you can also include the RADIUS client group in the URL, this allows the admin to have a different URL within the same type of RADIUS clients. Navigate to **Devices > RADIUS Client Groups** and group some RADIUS clients of the same type. Select the **RADIUS Client Type** and add **RADIUS Clients** that belong to the selected type.

Create RADIUS Client Group

Name	<input type="text" value="Group1"/>
Description	<div></div>
RADIUS Client Type	FortiGate ▾
RADIUS Clients	<div>Fortigate-APIP ✕</div> <div>fgt-adminlogin ✕</div> <div>+</div>

When configuring the guest portal, in the **Portal Preview** tab, you can select the **RADIUS Client Type** and **RADIUS Client Group** (optional) to generate the Redirection URL. Click **Get Redirect URL** to generate the redirection URL. The following redirection URL formats are supported.

- `https://{Fortiguest}/cp/portal/v1/cp/portal/{Device_IP}`
- `https://{FortiGuest}/cp/portal/v1/cp/portal/{RADIUS_client_type}`
- `https://{FortiGuest}/cp/portal/v1/cp/portal/{RADIUS_client_type}/{RADIUS_client_group}`

Name > Theme > Settings > Policy > Portal Preview

Portal Setup Complete

The wizard has finished building your portal.

You can preview the portal at [https://\[redacted\]/portal/v1/cp/8](https://[redacted]/portal/v1/cp/8)

Please select RADIUS Client Type and RADIUS Client Group (optional) to generate the Redirection URL. You should configure your network devices to redirect to this URL.

Radius Client Type	FortiGate ▾
Radius Client Group	fortigate ▾ ✕
	<div>Get Redirect URL</div>
Redirect URL	<a href="https://[redacted]/portal/v1/cp/portal/fortigate/fortigate">https://[redacted]/portal/v1/cp/portal/fortigate/fortigate</a>

### Notes:

- The older redirection URL format using the device IP address is still supported.
- All access requests from the same RADIUS client type lead to the same portal, unless there are any other contrary conditions configured under the rules or have RADIUS client grouping.
- For a generic device, the redirection URL with the device IP address is only supported.

## Managing *message-authenticator* in RADIUS

You can now enable/disable sending the message authenticator attribute to the server when configuring the RADIUS client. Navigate to **Devices > RADIUS Clients** and set the **Require client to send Message-Authenticator attribute** option. This option is disabled by default.

Client	Attributes	MAC Authentication	RadSec Authentication	PSK Authentication
Name	RADIUS-FortiGuest			
IP Type	<div>IP Address</div> <div>Hostname</div> <div>Subnet</div> <div>IP Range</div>			
Device IP Address ?	10.1.1.1			
Secret ?	<div>.....</div> <div>.....</div>			
Confirm	<div>.....</div> <div>.....</div>			
Type ?	FortiGate			
Description				
<div>Require client to send Message-Authenticator attribute <input checked="" type="checkbox"/></div>				

The message-authenticator attribute can also be enabled in the authentication policies for RADIUS and RadSec server types.

### Notes:

- If this option is disabled, then FortiGuest processes RADIUS request packets with/without the message-authenticator attribute.
- If this option is enabled, then FortiGuest drops RADIUS request packets without the message-authenticator attribute in them.

Edit Authentication Policy	
Name	Settings
Support eduroam ?	<input type="checkbox"/>
Verify SSL Certificate CN	<input type="checkbox"/>
RadSec Type	TLS
Server [Hostname or IP Address]	
Authentication Port	2083
Secret	<div>.....</div> <div>Change</div>
Confirm	<div>.....</div> <div>Change</div>
<div>Require Message-Authenticator attribute in Response <input checked="" type="checkbox"/></div>	

## NTP Settings from the User Interface

You can now configure the synchronization interval with the configured NTP server. Navigate to **System > Date/Time Settings** and enable **Sync Interval**. The default is 60 seconds, and the allowed range is 1 – 1440 seconds.

NTP							
Use NTP	<input checked="" type="checkbox"/>						
Sync Interval	60						
NTP Servers	<table><tr><td>ntp1.fortiguard.com</td><td>×</td></tr><tr><td>ntp2.fortiguard.com</td><td>×</td></tr><tr><td colspan="2">+</td></tr></table>	ntp1.fortiguard.com	×	ntp2.fortiguard.com	×	+	
ntp1.fortiguard.com	×						
ntp2.fortiguard.com	×						
+							

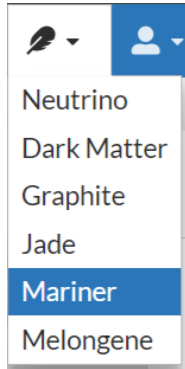
## License Status in the User Interface

You can now view the status of the FortiGuest license in the user interface. Navigate to **System > Licensing** and the **Status** is displayed as *Valid* or *Expired*.

Upload License	
System ID	15834d56-c566-2f92-b650-3e3cbf4f4b44
Serial Number	FSTVMSTM803041Local
License Summary	
Issue Date	2024-07-24
Begin Date	2024-07-24
End Date	2024-07-25
Allowed Connected Users	10000
Status	Expired
<div>Upload License File Update License</div>	

## New Themes for Administrative Portal

The FortiGuest administrative portal now supports multiple display themes for the user interface. The selected theme is saved in the browser per user, and the same theme is used on subsequent log-ins, unless it is changed. The default theme is *Mariner*.



## Common Vulnerabilities and Exposures

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

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

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


## Known Issues

These are the known issues in this release of FortiGuest.

Issue ID	Description
996795	MPSK supports unlimited usage profiles only.
1026948	Random time zone changes are observed when FortiGuest is upgraded from version 1.2.0.
1082365	The GUI is unresponsive after changing the HTTP mode in <b>System &gt; Interface Timeout</b> , followed by modifications to the network interface settings.



[www.fortinet.com](http://www.fortinet.com)



Copyright© 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.