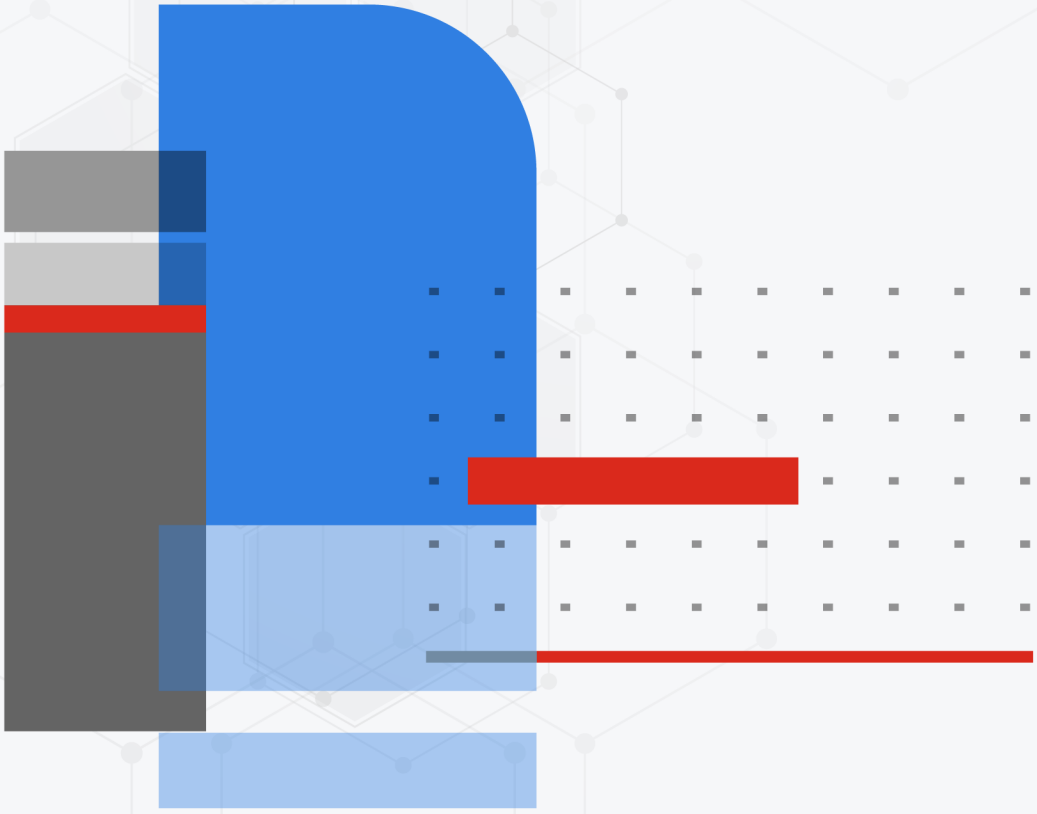
Release Notes

FortiGuest 1.2.0



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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

December 22, 2023
FortiGuest 1.2.0 Release Notes
70-867984-120-20231222

TABLE OF CONTENTS

Change log

Date	Change description
2023-12-22	FortiGuest 1.2.0 release version.
2024-01-25	Updated What's New topic.

About this Release

This release delivers a suite of new features for FortiGuest and resolves open issues. For more information, see What's New and Resolved Issues.

Notes:

- Upgrade to current release of FortiGuest is not supported, you are required to migrate data from FortiGuest 1.0.0 or 1.1.0 to 1.2.0. See Migrating to FortiGuest v1.2.0
- See the *FortiGuest 1.2.0 User Guide* for the detailed installation procedure.
- [Smart Connect] For PEAP to work with Windows 10 devices, ensure that a FortiGuest certificate is included in the **Additional Certificates** of a Smart Connect profile.

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.

What's New

This section describes the key features of FortiGuest.

Feature	Description
Listing sponsors in the guest portal	You can now list the sponsors on the guest portal that allows the user to select the sponsor instead of entering the sponsor email ID manually.
Secure Pay API	Secure Pay API is now supported as a payment provider.
Session Management	You can now view all active and connected sessions.
REST API rate limit	You can rate limit the REST API requests from a client per second, for the FortiGuest admin portal and captive portal.
Password change	You can now mandate the user to change the password after logging in into the guest portal.
Language template	FortiGuest now supports language templates in Spanish and Portuguese.
RADIUS client types	The FortiWLC, Aruba, and Meraki controllers are added as the supported vendors for RADIUS clients.
Sine Pro support	The Sine Pro visitor management platform is now integrated with FortiGuest.
SAML Support	You can configure an authentication server that supports the SAML protocol to access FortiGuest.
FortiGuard SMS support	You can now leverage existing FortiGuard SMS services within FortiGuest.

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	15.x
Apple iPAD	9.2.1 and 9.3.5
Android	12 and 13
Google Chrome	109.0.5414.120
Mozilla Firefox	109
Safari	12.1.2, 15.5, and 16.1.1
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 and 13
Google Chrome	109.0.5414.120
Mozilla Firefox	109
Safari	12.1.2, 15.5, and 16.1.1
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	12 and 13

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

The following minimum hardware specifications required for virtual appliances.

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

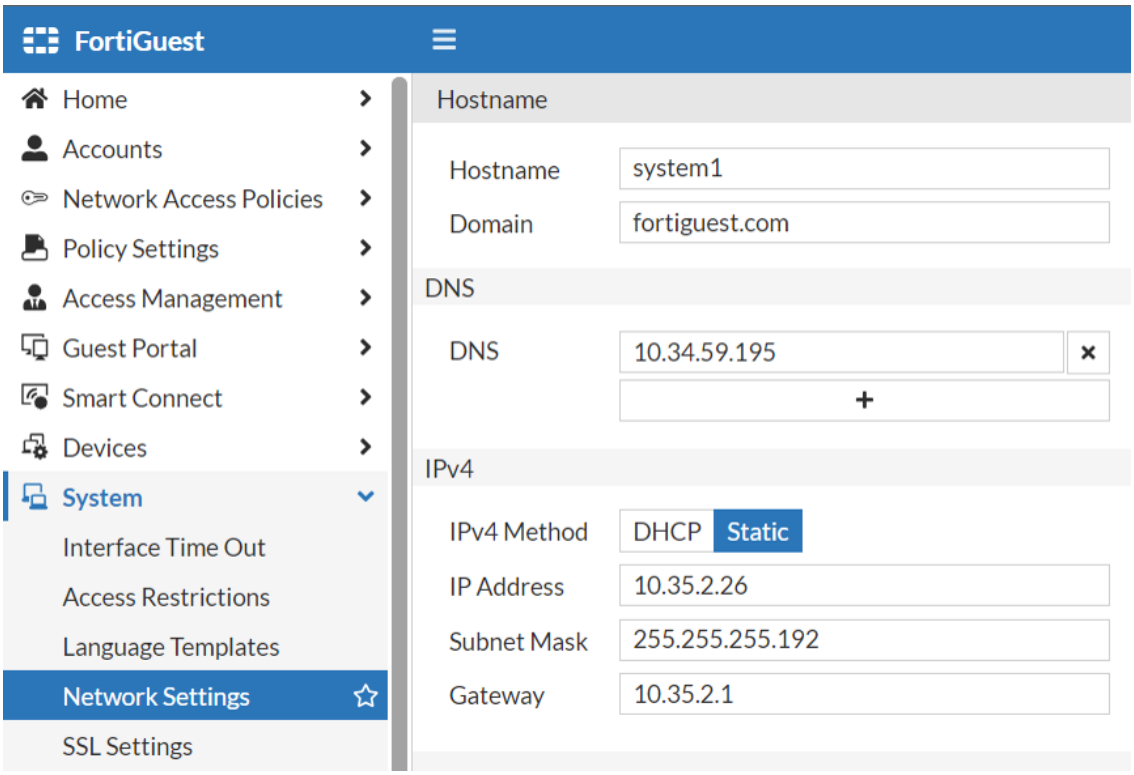
Migrating to FortiGuest v1.2.0

Follow this procedure to migrate the FortiGuest data from version 1.0.0 or 1.1.0 to 1.2.0.

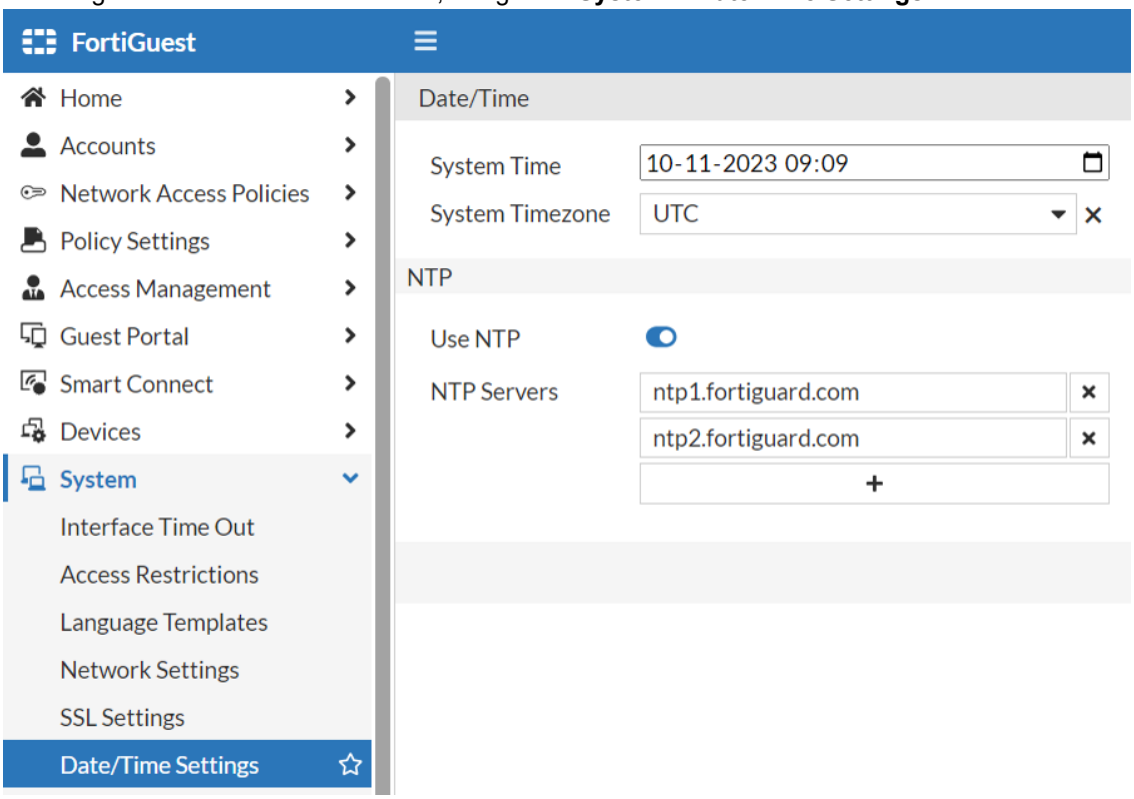
Notes:

- You are required to install a new license for FortiGuest 1.2.0.
- When a FortiGuest instance is configured, the default IP address is 192.168.1.99/24.

1. Navigate to **System > Backup Policy > Backup Settings** and take a backup of the data on the existing server (v1.0.0 or 1.1.0).
2. After the backup is successful, deploy FortiGuest 1.2.0 and configure the IP address and password, see Deploying FortiGuest.
3. Run the following commands to either assign a static IP address or DHCP.
   a. To assign a static IP address:
   ```
   fguest # config system interface
   fguest (interface) # edit port1
   fguest (port1) # set mode static
   fguest (port1) # set ip <IP/CIDR>
   fguest (port1) # end
   fguest # config router static
   fguest (static) # edit 1
   fguest (1) # set gateway <your_gateway>
   fguest (1) # set device port1 #Same as the port mentioned in interface.
   fguest (1) # end
   ```
   b. To assign DHCP:
   ```
   fguest # config system interface
   fguest (interface) # edit port1
   fguest (port1) # set mode DHCP
   fguest (port1) # end
   ```
   Note: To retain an existing IP address, power-off the existing VMs and deploy new VMs running FortiGuest 1.2.0 with the same IP addresses.
4. Access the FortiGuest GUI using the server IP address (*https://[server IP]/adminportal/auth/login*) and complete the configuration.
   a. To configure FQDN and assign IP address for the management interfaces, navigate to **System > Network Settings**.



b. To configure NTP server and time zone, navigate to **System > Date/Time Settings**.



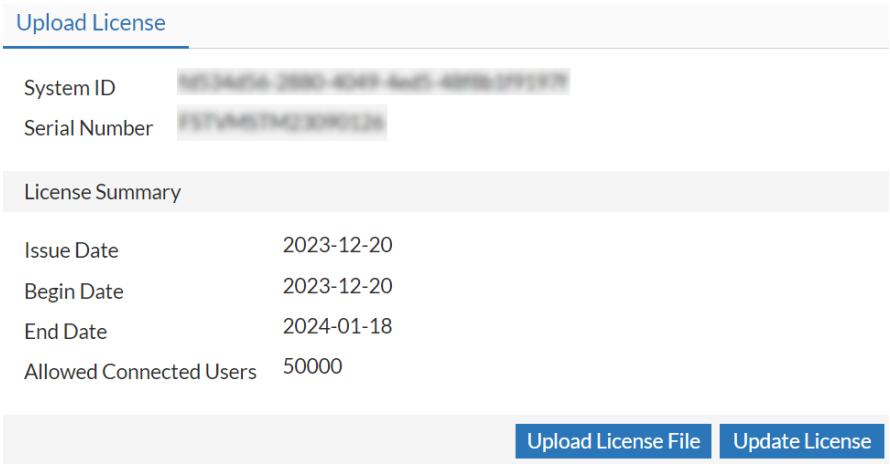
5. Navigate to **System > Backup Policy > Restore a Backup File**; select the backup file and restore the data on the new server.

If IP address restrictions are enabled, ensure that you attempt to log in to the instance from the same IP range after restoring the backup.

6. Installing the License

You can install a new license via the FortiGuest GUI.

a. Navigate to **System > Licensing**.
b. Click **Upload License File**.
c. In the Upload License File window, click **+ Browse**.
d. Browse and select the license file.
e. Click **OK**.



Note: Fortinet recommends that in order to restore the backup in the same network, ensure the current running VM is shut down after backup. This restores all network settings.

Resolved Issues

These issues are resolved in this release of FortiGuest.

Issue ID	Description
871983	Sometimes, FortiGuest was unable to send emails.
904330	Observed an internal error when the guest portal password recovery mode was set to *Email then if not successful via SMS* or vice versa.
908840	The license information was not displayed in the FortiGuest GUI after license update.
916508	In the **Policy Details** page, you have to scroll to the default country code, Norway (+47). This default value is not at the top of the list.
916509	The users are directed to the login page even if they deny the *Accept Usage Policy*.
916510	Some GUI pages did not launch sometimes; a reboot was required.
934086	FortiGuest allowed authorizing only 5 users (default) despite a license for 2000 users.
953652	Authentication failure with password containing Scandinavian characters.
955152	Smart Connect did not install the Smart Connect profile on Windows/Android devices.
965248	Sometimes, the *lang.error-keys.invalid_error.country_code* error was observed when trying to add a user to FortiGuest.

Known Issues

These are the known issues in this release of FortiGuest.

Issue ID	Description
894407	TLS version 1.3 is not supported on FreeRADIUS.
913048	The CoA and logout functionalities are not working accurately for Meraki controllers (RADIUS clients).
966162	Setting the time zone through the graphical user interface (GUI) does not persist when checked using the command-line interface (CLI).
966166	Time based sorting fails in RADIUS authentication reports.
966126	Password complexity requirements are not enabled for the CLI.
955957	[Windows 11] Update the client's registry settings to ensure that TLS 1.2. is used for EAP authentication.
974257	[Hyper-V] All four network interfaces are selected as default when FortiGuest instance is brought up. You are required to manually un-select the irrelevant interfaces.

www.fortinet.com