SonicWall SonicOS 6.5.4.13

Release Notes

October 2023

These release notes provide information about the SonicWall SonicOS 6.5.4.13 release.

Topics:

About SonicOS 6.5.4.13

SonicWall SonicOS 6.5.4.13 resolved key issues, which were found since the previous release. For more information, refer to the Resolved Issues section. This release supports all the features and contains all the resolved issues found in previous SonicOS 6.5 releases. The previous release notes are available on MySonicWall at: https://mysonicwall.com or on the Technical Documentation portal.

A significant enhancement has also been added in this release. It allows users to disable the Virtual Portal on the Wide Area Network (WAN) while keeping SSLVPN services unaffected. This feature offers greater control over network accessibility without disrupting secure remote connections. Key benefits include:

- **Enhanced Security**

  With the Virtual Portal disabled on the WAN, you can substantially reduce the attack surface for potential security breaches. External entities won't be able to access your Virtual Portals, enhancing overall network security.

- **Uninterrupted SSLVPN Services**

  By disabling the Virtual Portal on the WAN, SSLVPN services remain unaffected, ensuring that your users can continue to securely access your network resources.

The default behavior is that the virtual portal settings would be migrated from the previous SonicOS version.

To disable the virtual portal access on the WAN Zone:

1. Login to the firewall.
2. Go to **MANAGE > SSLVPN > Portal Settings**.

3 Select the option **Disable Virtual Office on Non-LAN Interfaces**.

Enabling the option disables the Virtual Portal access on the non-LAN zone.

Supported Platforms

SonicOS 6.5.4.13 is supported on the following SonicWall appliances:

- NS*a* 9650
- NS*a* 9450
- NS*a* 9250
- NS*a* 6650
- NS*a* 5650
- NS*a* 4650
- NS*a* 3650
- NS*a* 2650
- SuperMassive 9600
- SuperMassive 9400
- SuperMassive 9200
- NSA 6600
- NSA 5600
- NSA 4600
- NSA 3600
- NSA 2600
- TZ600 / TZ600P
- TZ500 / TZ500 Wireless
- TZ400 / TZ400 Wireless
- TZ350 / TZ350 Wireless
- TZ300 / TZ300P / TZ300 Wireless
- SOHO 250 / SOHO 250 Wireless
- SOHO Wireless

Resolved Issues

This section provides a list of resolved issues in this release.

Resolved Issue	Issue ID
Post-authentication, stack-based buffer overflow vulnerability in the SSL VPN's getPacketReplayData.json URL endpoint.	GEN6-4006
Post-authentication, stack-based buffer overflow vulnerability in the SSL VPN's sonicflow.csv, appflowsessions.csv endpoints.	GEN6-3988
Post-authentication, stack-based buffer overflow vulnerability in the SSL VPN's ssoStats-s.xml, ssoStats-s.wri endpoints.	GEN6-3987
Due to an issue with internal wireless driver, SOHOW, TZ 300W, TZ 400W, TZ 500W firewalls will not connect to a Wi-Fi access point with a hidden SSID.	GEN6-3932
When configuring a DDNS profile for changeip.com, the error **Network Error** is reported due to an API change by **ChangeIP**.	GEN6-3898
Configuring the Radius PIN on NetExtender may fail due to incorrect SonicOS handling of the **Radius State** field.	GEN6-3432

Known Issues

This section provides a list of known issues in this release.

Known Issue	Issue ID
VPN management access rule still exists when “Disable auto-added VPN management rules” is enabled.	GEN6-2567
The VLAN ID, when edited for a trunked port, reverts to the default setting after restarting the firewall or importing the settings.	GEN6-2557

Known Issue	Issue ID
Under certain conditions SSLVPN IP leases cannot be released and may result in the IP pool being exhausted. Logging out the users using the user status page will free up the IP addresses.	GEN6-2333
An established IPSEC VPN tunnel intermittently fails in a NAT environment.	GEN6-2296
10G interface goes down after configuring it as a dedicated uplink for a Sonicwall Switch due to negotiation issue. **Workaround**: Login to switch console and enable auto negotiation on the interface which went down.	GEN6-2265

Additional References

GEN6-3986, GEN6-3955, GEN7-3847, GEN6-2819, GEN6-2523

System Compatibility

This section provides additional information about hardware and software compatibility with this release.

Wireless 3G/4G Broadband Devices

SonicOS 6.5.4 provides support for a wide variety of PC cards, USB devices and wireless service providers. For the most recent list of supported devices, see:
https://www.sonicwall.com/support/knowledge-base/what-wireless-cards-and-broadband-devices-are-supported-on-sonicwall-firewalls-and-access-points/170505473051240/

GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.4 requires GMS 9.3.

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWall recommends using the latest Chrome, Firefox, Internet Explorer, Edge or Safari browsers for administration of SonicOS. This release supports the following web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- Edge 81.0 and higher
- IE 10.0 and higher
- Safari 10.0 and higher running on non-Windows machines

NOTE: On Windows machines, Safari is not supported for SonicOS management.

NOTE: Mobile device browsers are not recommended for SonicWall appliance system administration.

Product Licensing

SonicWall network security appliances must be registered on MySonicWall to enable full functionality and the benefits of SonicWall security services, firmware updates, and technical support. Log in or register for a MySonicWall account at https://mysonicwall.com.

Upgrading Information

For information about obtaining the latest firmware, upgrading the firmware image on your SonicWall appliance, and importing configuration settings from another appliance, see the *SonicOS 6.5 Upgrade Guide* available on the Support portal at https://www.sonicwall.com/support/technical-documentation.

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Last updated: 10/17/23

232-006079-00 Rev B