# SonicWall® SonicOS 6.5.4.5

## Release Notes

### November 2019

These release notes provide information about the SonicWall® SonicOS 6.5.4.5 release.

**Topics:**

- About SonicOS 6.5.4.5
- Supported Platforms
- New Features
- Resolved Issues
- Known Issues
- System Compatibility
- Product Licensing
- Upgrading Information
- SonicWall Support

# About SonicOS 6.5.4.5

SonicWall SonicOS 6.5.4.5 provides several new features and fixes a number of issues found in previous releases. For more information, see the New Features and Resolved Issues sections.

This release supports all the features and contains all the resolved issues found in previous SonicOS 6.5 releases. For more information, see the previous release notes, available on MySonicWall at: https://mysonicwall.com.

# Supported Platforms

SonicOS 6.5.4.5 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

# New Features

This section describes the new features in this release.

**Topics:**

- Configuration Auditing
- FQDN Support in Dynamic Objects
- Capture Client User SSO Integration
- Capture Client User Alerts
- SD-WAN Performance Class Object Flexibility

## Configuration Auditing

Configuration Auditing automatically records any configuration changes that an administrator attempts from one of the available user interfaces, web management (via HTTP and HTTPS), command line (via console or SSH), or SonicWall GMS. A configuration auditing records table in the **MANAGE | Log Settings > Auditing Records** page records all attempted configuration changes, both successful and failed. With configuration auditing, SonicOS archives the history of its configuration changes, so that the administrator or others can later revisit and analyze the records. This feature is enabled by default. Refer to the *SonicOS 6.5 Logs and Reporting* administration documentation for details about Configuration Auditing.

## FQDN Support in Dynamic Objects

SonicOS 6.5.4.5 extends the existing Dynamic External Objects feature to include Fully Qualified Domain Names (FQDNs) in the Dynamic External Address Group (DEAG) file. The DEAG file previously could only contain the IP addresses of the included DEAG members, and now can also contain FQDNs that define the group members.

Dynamic External Objects are configured on the **MANAGE | Policies | Objects > Dynamic External Objects** page. They are comprised of Dynamic External Address Groups (DEAG) and Dynamic External Address Objects (DEAO). A Dynamic External Address Group is an Address Group whose members are dynamic and are determined by the contents of the DEAG file. Dynamic External Address Objects are intermediate, internal objects that are dynamically created and placed under a Dynamic External Address Group when a DEAG file is downloaded.

The Dynamic External Objects feature eliminates the need for manually modifying an Address Group to add or remove members. You can simply edit the DEAG file to add or remove members, and let SonicOS automatically download the file and update the Dynamic External Object. Refer to the *SonicOS 6.5 Policies* administration documentation for details about configuring Dynamic External Objects.

## Capture Client User SSO Integration

A **Capture Client** screen with an **Enable SSO Capture Client** option is added to the **CONFIGURE SSO** window in SonicOS 6.5.4.5. This option enables user authentication via SonicWall Capture Client by client PCs configured in the Client AV Enforcement lists, with any zone. This allows the user to access the internet via their browser with no SSO agent involvement. This option is disabled by default, and it is not necessary to enable it if you just want to use Client AV Enforcement with Capture Client. Refer to the *SonicOS 6.5 System Setup* administration documentation for details about Single Sign-On configuration, including this Capture Client option.

In the **MANAGE | Security Configuration | Security Services > Client AV Enforcement** page, the new **Enable SSO Login via Capture Client Enforcement** option enables the periodic sharing of user login information (domain/user format) from Capture Client endpoints to SonicWall firewalls that enforce Capture Client, when there is proper connectivity between the Capture Client endpoints and the Client Management Console (CMC).

The firewalls are also notified if user information is changed or updated on the Capture Client endpoint IP address. Refer to the *SonicOS 6.5 Security Configuration* administration documentation for details about Client AV Enforcement configuration, including this option.

# Capture Client User Alerts

SonicOS 6.5.4.5 provides a new option to enable push notifications from the firewall to the Capture Client endpoint when a connection is blocked or traffic is dropped due to actions by other SonicWall security services. This is the **Enable Alert Message from Firewalls to Capture Client Endpoint Devices** option on the **MANAGE | Security Configuration | Security Services > Client AV Enforcement** page. Without this option, clients have little visibility into firewall actions taken on traffic other than HTTP/HTTPS. These alert notifications provide a summary of the event containing the following information:

- Timestamp
- Source IP/Port
- Destination IP/Port
- Category - The SonicWall security service that blocked traffic or dropped the connection:
    - App Control
    - Botnet
    - Geo-IP Filter
    - Content Filter Service
    - Gateway Anti-Virus
    - Anti-Spyware
    - Capture ATP
    - Message (if available)

Refer to the *SonicOS 6.5 Security Configuration* administration documentation for details about Client AV Enforcement configuration.

# SD-WAN Performance Class Object Flexibility

SD-WAN Performance Class Objects are used to configure the desired performance characteristics for the application/traffic categories. These objects are used in the Path Selection Profile to automate the selection of paths based on these metrics.

SonicOS 6.5.4.5 provides new options when configuring Performance Class Objects for use with SD-WAN:

- **Include Latency** – Select this option to include the performance class latency attribute for this object, or clear the checkbox to exclude the latency attribute.
- **Include Jitter** – Select this option to include the performance class jitter attribute for this object, or clear the checkbox to exclude the jitter attribute.
- **Include Packet Loss** – Select this option to include the performance class packet loss attribute for this object, or clear the checkbox to exclude the packet loss attribute.

Starting in SonicOS 6.5.4.5, you can include or exclude the Latency, Jitter, or Packet Loss attributes in your custom Performance Class Object, although you cannot exclude all three attributes in the same object. When excluded, the value of that attribute is not used as a criterion or threshold when determining whether a particular path is qualified or not. For example, if you want to evaluate a particular path only on the Latency attribute but you don’t care about the other attributes, you can include Latency and exclude Jitter and Packet Loss in your custom object.

These options appear in the **Add Performance Class Object** dialog when you click **Add** on the **MANAGE | System Setup | SD-WAN > Performance Class Objects** page. Refer to the *SonicOS 6.5 System Setup* administration documentation for details about configuring SD-WAN Performance Class Objects.

# Resolved Issues

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

### App Control

| Resolved issue | Issue ID |
|---|---|
| The existing signature in App Control does not block the Psiphon proxy access application. | 219479 |

### DPI-SSL

| Resolved issue | Issue ID |
|---|---|
| DPI-SSL certificate shows as not trusted on MacOS devices after Catalina update. MacOS Catalina is not working with the custom certificate or with the SonicWall DPI-SSL 2048 bits certificate. | 222349 |
| Removal of Go Daddy SHA1 root certificate causes the browser to warn incorrectly that certain websites are not secure.<br>Occurs when DPI-SSL is enabled and the SonicWall DPI certificate is imported into the client computer. | 221874 |
| DPI-SSL stops working and the CFS HTTPS Content Filtering option is not working. Users are able to access blocked web sites. | 221416 |
| Client DPI-SSL may stop operating correctly after a period of time due to an internal resource becoming depleted. | 221232 / 221196 |

### High Availability

| Resolved issue | Issue ID |
|---|---|
| When the active firewall in an Active/Standby HA pair is accessed from the virtual IP address and the FORCE ACTIVE/STANDBY FAILOVER button is clicked multiple times, the error message, “Error: Force Failover in progress” is displayed and failover is not triggered. | 215053 |

### Management Interface

| Resolved issue | Issue ID |
|---|---|
| The SonicOS web management interface does not render any Local User’s VPN access and Groups section properly on Chrome.<br>Occurs with Chromium v76 & v77 based web browsers. | 222183 |
| If the user’s password contains the British pound key ‘£’, web login fails with the error message, “This browser window does not appear to be the one used most recently to log in to the SonicWall from here.” | 218981 |

### Networking

| Resolved issue | Issue ID |
|---|---|
| SD-WAN routes are dimmed/disabled and take a long time to activate, although all the links show as qualified.<br>Occurs when the SD-WAN routes are modified. | 222185 |
| The **Enable IPv6** option might not work correctly when it is selected multiple times or when **ACCEPT** is clicked multiple times on the **System > Administration** page. | 219931 |

### System

| Resolved issue | Issue ID |
|---|---|
| Capture ATP may stop operating correctly after a period of time due to an internal resource becoming depleted. | 222433 / 221102 |
| SonicOS may fail to process certain types of traffic and restart. | 222064 |
| SonicOS may restart when enforcing login uniqueness under certain scenarios. | 221971 |
| The firewall deletes a WAN to WAN access rule created for management by GMS or CSC-MA.<br>Occurs when the FQDN name is used in the access rule, HTTPS management mode is enabled for GMS, and then the firewall is rebooted. | 221919 |
| DPI-SSL processing may trigger a SonicOS restart under certain scenarios. | 221858 |
| Unable to SSH into the firewall and the error “maximum number of ssh sessions are active, please try again later” is displayed.<br>Occurs after the firewall has been up for about one month. | 206881 |

### Users

| Resolved issue | Issue ID |
|---|---|
| Imported LDAP users are lost after the firewall restarts or fails over to the secondary unit in a High Availability deployment.<br>Occurs when the users are imported with a domain component. | 220825 |

### VPN

| Resolved issue | Issue ID |
|---|---|
| VPN policies are deleted when the Create Group VPN option is disabled on the WAN zone and the firewall is rebooted. | 222155 |
| “IKEv2 Out of memory” message may be triggered under certain incorrect IKE configurations. | 215736 |

### Wireless

| Resolved issue | Issue ID |
|---|---|
| L3 managed SonicPoint N2 and SonicPoint ACe become non-responsive after firmware upgrade. | 222154 |

# Known Issues

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

## DPI-SSL

| Known issue | Issue ID |
|---|---|
| In certain scenarios, downloading large files might not succeed when Server DPI-SSL is enabled. | 220430 |

## Log / Syslog

| Known issue | Issue ID |
|---|---|
| The **Log Settings > Auditing Records** page is not displayed due to a JavaScript error with IE 11. | 222235 |
| The DELETE ALL function might not work correctly when there is more than one page of servers listed in the **Syslog Servers** table on the **MANAGE \| Log Settings > SYSLOG** page, and the **DELETE ALL** button is clicked on a page other than the first page. | 220409 |
| In certain scenarios, syslog messages might not be sent to GMS over a site-to-site VPN tunnel. | 220405 |

## Networking

| Known issue | Issue ID |
|---|---|
| An SD-WAN route is not disabled or greyed out when all interfaces in the Path Selection Profile (PSP) have a status of Not Qualified. | 219900 |

## SSL VPN

| Known issue | Issue ID |
|---|---|
| The password must be entered twice when logging into an SSH bookmark with Firefox. | 222269 |

## Switch X-Series

| Known issue | Issue ID |
|---|---|
| On a High Availability pair with an X-Series switch connected and configured, traffic flow stops after link failover.<br>Occurs when a dedicated uplink with VLAN in HA is port shielded to a switch interface, and then the dedicated uplink is disconnected from the primary firewall while traffic is flowing. | 222138 |
| An interface that is configured as a dedicated uplink to an X-Switch cannot be reconfigured as a link aggregator. | 222123 |

## Users

| Known issue | Issue ID |
|---|---|
| Firewall user status in the session table is not updated after user sign-out.<br>Occurs when User SSO via Capture Client is enabled. | 222252 |
| The Simple usernames check box is missing under SSO configuration. | 222213 |
| The RADIUS Filter-ID attribute works only for PAP authentication, but is not working for CHAP, MSCAP and MSCHAPv2, preventing users from being authenticated. | 222196 |
| On a connect failure, LDAP does not retry with a different IP address when an LDAP server has more than one. | 220325 |
| A connectivity test of a RADIUS server failed after adding a LAN zone partition selection policy. | 219737 |

### VPN

| Known issue | Issue ID |
|---|---|
| Remote VPN networks might not be reachable in certain conditions after enabling and configuring GMS. | 220398 |
| A VPN compatibility issue with AWS prevents the firewall from having a successful negotiation with AWS VPN. | 222375 |

# 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/en-us/support/knowledge-base/170505473051240

## GMS Support

SonicWall Global Management System (GMS) management of SonicWall security appliances running SonicOS 6.5.4 requires GMS 8.7 SP1 for management of firewalls using the new features in SonicOS 6.5.4.

## WAN Acceleration / WXA Support

The SonicWall WXA series appliances (WXA 6000 Software, WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are supported for use with SonicWall security appliances running SonicOS 6.5.4. The recommended firmware version for the WXA series appliances is WXA 1.3.2.

## 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, or Safari browsers for administration of SonicOS. This release supports the following Web browsers:

- Chrome 45.0 and higher
- Firefox 25.0 and higher
- IE Edge or 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 and to customers who have trial versions.

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 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.

**Copyright © 2019 SonicWall Inc. All rights reserved.**

This product is protected by U.S. and international copyright and intellectual property laws. SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserve the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/eupa.

### 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: 11/6/19

232-005174-00 Rev A