

Analytics 2.5.6

Release Notes

April 2024

These release notes provide information about the SonicWall Analytics 2.5.6 release.

Topics:

- [About On-Premises Analytics](#)
- [System Requirements](#)
- [Upgrading to Analytics 2.5.6](#)
- [Resolved Issues](#)
- [Known Issues](#)
- [Additional References](#)
- [Licensing Model](#)
- [SonicWall Support](#)

About On-Premises Analytics

SonicWall On-Premises Analytics 2.5.6 is a maintenance release that provides a single new feature as well as fixes for known issues. Refer to [Resolved Issues](#) for more information.

Analytics extends security event analysis and reporting by providing real-time visualization, monitoring and alerts based on the correlated security data. You can perform flexible drill-down and gain insight into your network, user access, connectivity, application use, threat profiles and other firewall-related data. SonicWall On-Premises Analytics provides the following key features:

- Data collection that includes normalizing, correlating, and contextualizing the data to the environment
- Streaming analytics in real time
- Analytics including activity trends and connections across the entire network
- Real-time, dynamic visualization of the security data from a single point
- Real-time detection and remediation

SonicWall On-Premises Analytics is designed for customers requiring long term storage of firewall and supports designated SonicWall firewalls.

For firewalls not under management, you can do reporting and analysis using On-Premises Analytics. It can be deployed as a virtual machine using OVA on VMware ESXi, Microsoft Hyper-V, or Microsoft Azure. Refer to the On-Premises Analytics ESXi Deployment Guide, On-Premises Analytics Hyper-V Deployment Guide, and On-Premises Analytics Azure Deployment Guide which can be found at the [Technical Documentation portal](#) (select **Management and Analytics > Analytics**).

The IPFIX-based and Syslog-based Analytics can be used as a standalone on-premises solution for collecting and storing various kinds of data from firewalls and use for data analytics and reporting.

❗ | **NOTE:** In this kind of deployment, you do not have firewall management capabilities.

System Requirements

Analytics 2.5.6 requires these minimum system requirements.

- [Hardware Requirements](#)
- [Browser Levels](#)
- [MySonicWall Account](#)

Hardware Requirements

For details for a specific platform deployment refer:

- For HyperV - [Analytics Deployment Guide - HyperV](#)
- For ESXi - [Analytics Deployment Guide - ESXi](#)
- For Azure - [Analytics Deployment Guide - Azure](#)

Browser Levels

To access the On-Premises Analytics GUI, the following browser levels are supported:

Browser Supported	Notes
Google Chrome (version 73)	This is the preferred browser for the real-time graphics display on the Dashboard.
Apple Safari (version) 12	
Microsoft Edge (version 42)	
Mozilla Firefox (version 66.0.3)	

MySonicWall Account

Having a MySonicWall account for licensing and registration of any SonicWall products is required. If you do not have one, set one up.

To set up a MySonicWall account:

1. Navigate to <https://mysonicwall.com>.
2. Click **Sign Up**.
3. Provide the information requested by the **Sign Up** wizard, after which you can sign in and register products.

Upgrading to Analytics 2.5.6

Upgrading to Analytics 2.5.6 is supported only from 2.5.5 using SWI files. For details on how to upgrade to Analytics 2.5.5, refer to the **Upgrading On-Premises Analytics** section in the below deployment guides:

- For HyperV - [Analytics Deployment Guide - HyperV](#)
- For ESXi - [Analytics Deployment Guide - ESXi](#)
- For Azure - [Analytics Deployment Guide - Azure](#)

Resolved Issues

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

Resolved Issue	Issue ID
ANA-286	Intrusions/Details filter does not allow selecting Priority Threat Options of Low Medium High.
ANA-253	There is longer page load time while generating reports with filter criteria.
ANA-229	Log Analyzer export is only 100 rows, even though max export has been increased to 10000.
ANA-206	File Manager manual upload of syslog files is failing.
ANA-192	Customer is unable to login to On-Prem Analytics after entering MSW account credentials as he is getting error message "invalid contents found in request".
ANA-153	Flow DB size is shown differently on Flow Agent > Devices and Flow Agent > Usage page.

Known Issues

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

Known Issue	Issue ID
ANA-308	Hyper-V v10.0.17763.1 new analytics installation fails on initial setup using wizard.
ANA-204	Analytics needs an auto export tool for backup files larger than 2GB.
ANA-169	On-Prem Analytics 2.5.2 is unable to modify time zone.
ANA-127	Analytics flow based Search Filter should not be case-sensitive.

Additional References

ANA-105.

Licensing Model

The IPFIX-based Analytics and Syslog-based Analytics have different licensing models.

- [IPFIX-based Licensing](#)
- [Syslog-based Licensing](#)

IPFIX-based Licensing

① **NOTE:** Syslog-based Analytics storage limits are independent of license level and dependent on assigned resources.

On-Premises Analytics licensing levels are based on how much data from firewalls is logged. So, specific licenses support collection of firewall data in increments of 2, 5, 15, 30, and 100 GB per day. If an On-Premises Analytics instance exceeds its daily limit in a 24 hour period, the excessive logs are dropped and data is logged starting with the next day.

The following table summarizes currently available licensing levels.

Storage (based on licenses)	Flows per second or day	Storage Limit ¹
2 GB/day	2 GB/day — 300 flows/sec and 20 million flows/day	500 GB
5 GB/day	5 GB/day — 750 flows/sec and 50 million flows/day	1 TB
15 GB/day	15 GB/day — 2250 flows/sec and 150 million flows/day	5 TB

Storage (based on licenses)	Flows per second or day	Storage Limit ¹
30 GB/day	30 GB/day — 4500 flows/sec and 300 million flows/day	10 TB
100 GB/day	100 GB/day — 15000 flows/sec and 1 billion flows/day	Unlimited

¹This is the maximum amount of analyzed data that can be stored, not the maximum size of external storage that can be supported by the VM. Maximum size of external storage supported by the VM depends on Hypervisor on which Analytics is installed.

Syslog-based Licensing

When considering licensing for a Syslog-based solution, you will need to plan for the appropriate capacity for storing and retain reports.

Additionally, a new subscription is required for each firewall that you want reports from. The license is called SYSLOG Analytics and can be enabled through the MySonicWall portal, as described in the following section.

Activating Syslog Analytics

To activate Syslog Analytics:

1. Log in to <https://mysonicwall.com>.
2. Under **Product Management**, select **My Products**.
3. Click on the serial number of the firewall.
4. In the **LICENSES** page, click on the key icon.
5. Enter the activation key and click **Confirm**.
6. In the **ACTIVATE SERVICE** page, select the tenant, and then click **Activate**.
7. On-Premises Syslog Analytics serial is auto-generated.

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.

The [Support Portal](#) enables you to:

- View [Knowledge Base articles](#) and [Technical Documentation](#)
- View and participate in the [Community Forum](#) discussions
- View [Video Tutorials](#)
- Access [MySonicWall](#)
- Learn about [SonicWall Professional Services](#)
- Review [SonicWall Support services and warranty information](#)
- Register at [SonicWall University](#) for training and certification

About This Document

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

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

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

Analytics Release Notes

Updated - April 2024

Software Version - 2.5.6

232-006126-00 Rev A

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall 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 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 reserves the right to make changes to specifications and product descriptions at any time without notice. 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>.