View Page online: https://www.sonicwall.com/support/knowledge-base/sonicwall-analytics-faq/190425204812546/

SonicWall Analytics - FAQ

Description

What is SonicWall Analytics?

SonicWall Analytics is a new product from for IPFIX / Flow/ Syslog (Analytics 2.5 and above) based reporting for its firewalls.

Is SonicWall Analytics replacement for the current Analyzer?

SonicWall On-premise Analytics 2.5 is the replacement for Analyzer. However, as this is a separate product, we need to purchase a separate license for Analytics.

Will the current Analyzer meet end of life, if so when will that be?

þÿSonicWALL Analyzer 8.5 reached End of Support on the 24.April.2020. Pleas page: https://www.sonicwall.com/support/product-lifecycle-tables/sonicwall-analyzer/software/.

Is there a migration path from existing Analyzer to SonicWall Analytics?

No, there is no migration path from existing *Analyzer* to *SonicWall Analytics*þÿ as its a completely new produ there is no direct upgrade path from Analyzer to Analytics.

- ***Does SonicWall Analytics include syslog-based reporting?***

Yes, SonicWall On-premise Analytics 2.5 and above supports syslog-based reporting.

- ***How is SonicWall Analytics different from existing Analyzer?***

Please refer the below matrix to understand the key differences:

	SonicWall Analytics	**Analyzer**
Reporting	IPFIX/Syslog(Analytics 2.5 and above) based	Syslog-based
Licensing/Pricing	Usage-based	Unit-based
UI/UX	Same as CSC-Analytics	Old GMS UI/UX

How does the licensing and pricing for on-prem Analytics work?

SonicWall Analytics provides usage-based licensing/pricing. The licenses apply to a product group/tenant on MySonicWall. The licenses come with variants - 500GB, 1TB, 5TB, 10TB and Unlimited. For each of these licenses, there is a corresponding daily limit on the data analyzed, please refer below:

SKU	**Daily limit**

SKU	Daily limit
02-SSC-1503 SONICWALL ANALYTICS ON-PREM 500GB STORAGE LICENSE	2GB
02-SSC-1526 SONICWALL ANALYTICS ON-PREM 1TB STORAGE LICENSE	5GB
02-SSC-1530 SONICWALL ANALYTICS ON-PREM 5TB STORAGE LICENSE	15GB
02-SSC-1531 SONICWALL ANALYTICS ON-PREM 10TB STORAGE LICENSE	30GB
02-SSC-1532 SONICWALL ANALYTICS ON-PREM UNLIMITED STORAGE LICENSE	100GB

What dþÿ o e s Daily limitþÿ mean?

It define, how much data you can Analyze on system per day. *For ex:* On a 500GB license, the max daily limit is 2GB. Once daily limit quota is met, the SonicWall Analytics VM will STOP analyzing data for the day. It will continue next day with fresh limit i.e. 2 GB in this example.

Will it stop analyzing data when the Total quota limit (per License) has been met?

No, On-Prem *SonicWall Analytics* will keep analyzing the data, however it will keep only the latest Analytics data as per the quota & license and old data will be purged

*Can the SonicWall Analytics licenses be stacked?*1. *To increase the storage capacity?*

Stacking licenses in *SonicWall Analytics* is NOT SUPPORTED. For ex: If had a 500GB license and later want to expand it to 1.5 TB license, you CANNOT apply 1TB license on top of 500 GB.
Please refer the sizing guide (check question 9) to get the right sizing for your deployment.

Which products are supported on SonicWall Analytics for reporting?

Following firewalls are supported on *SonicWall Analytics*.

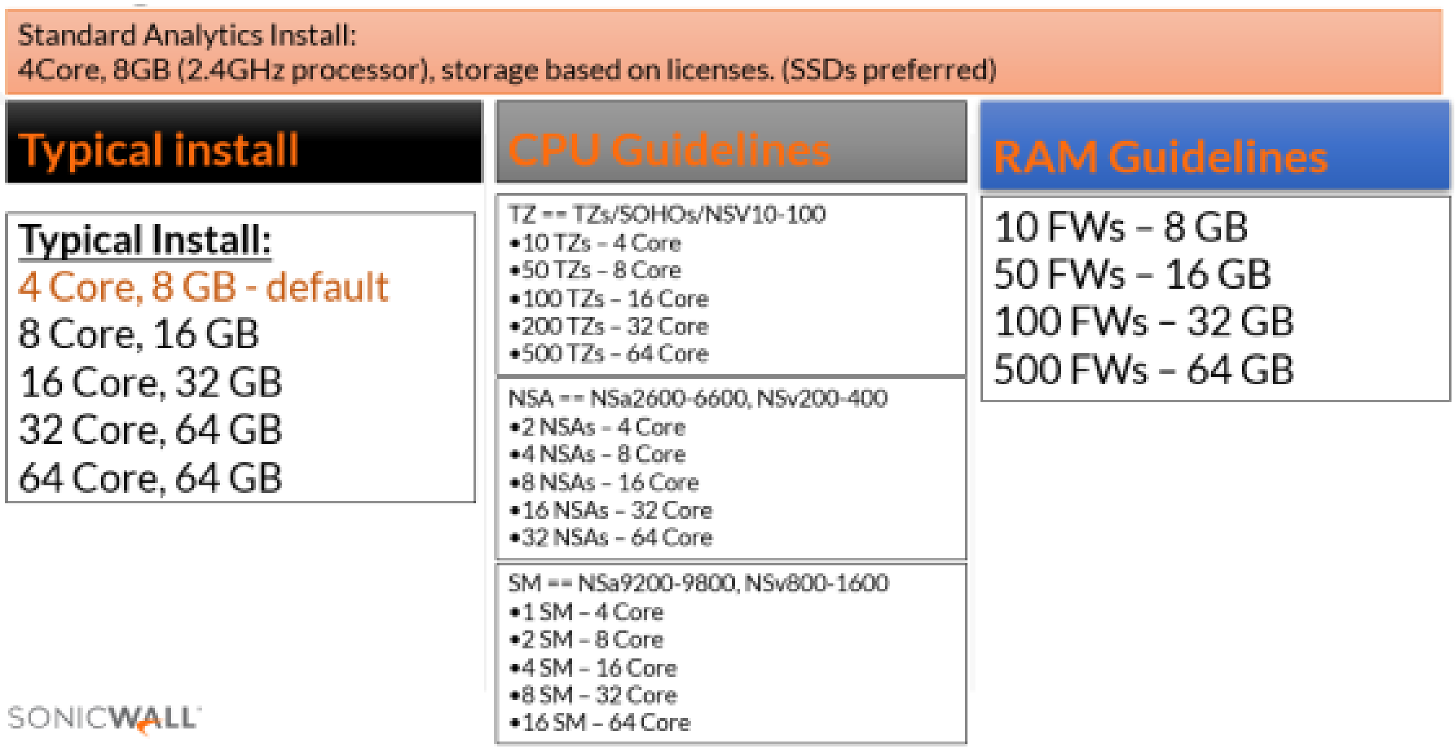
Entry Level Firewal	SOHO-W, TZ Series, NSv 10-100
Mid Range Firewalls	NSA 2500-6600, NSa 2650-6650, NSv 200-400
High-End Firewalls	SuperMassive 9000, 12K Series, NSa 9250-9650, NSv 800-1600

What are support platform for SonicWall Analytics?

SonicWall Analytics currently supported only on Vmware EXSi and Hyper-V.(Analytics version2.5.2518 and above).

How to size SonicWall Analytics?

Please refer below sizing guide.



Standard Analytics Install:
4Core, 8GB (2.4GHz processor), storage based on licenses. (SSDs preferred)

Typical install

Typical Install:
4 Core, 8 GB - default
8 Core, 16 GB
16 Core, 32 GB
32 Core, 64 GB
64 Core, 64 GB

CPU Guidelines

TZ == TZs/SOHOs/NSV10-100
- 10 TZs - 4 Core
- 50 TZs - 8 Core
- 100 TZs - 16 Core
- 200 TZs - 32 Core
- 500 TZs - 64 Core

NSA == NSa2600-6600, NSv200-400
- 2 NSAs - 4 Core
- 4 NSAs - 8 Core
- 8 NSAs - 16 Core
- 16 NSAs - 32 Core
- 32 NSAs - 64 Core

SM == NSa9200-9800, NSv800-1600
- 1 SM - 4 Core
- 2 SM - 8 Core
- 4 SM - 16 Core
- 8 SM - 32 Core
- 16 SM - 64 Core

RAM Guidelines

10 FWs - 8 GB
50 FWs - 16 GB
100 FWs - 32 GB
500 FWs - 64 GB

SONICWALL

- ***Does external hard disk mount supported for SonicWall Analytics VM?***

To utilize allocate storage as per license, use external hard disk (preferably SSDs) for Analytics deployment. Please refer the following KB for instructions to mount external storage.
https://www.sonicwall.com/support/knowledge-base/?sol_id=190425200209091

- ***How SonicWall Analytics integrate and work with CSC?***

SonicWall Analytics can be used in conjunction with CSC, which will help to manage firewall from CSC and generate reports from *SonicWall Analytics* while storing data locally.
Even though the data is stored/analyzed locally in SonicWall Analytics, user can view Reports or Analytics data in both CSC as well as On-prem SonicWall Analytics.
Note:

The integration DOES NOT allow to configure/view *Rules and Notifications* from *CSC-Analytics* and can only be done On-Prem1. *SonicWall Analytics* UI.

Zero Touch deployment is NOT supported in SonicWall Analytics hence2. **the unit/s need to be added manually on SonicWall Analytics**. Hence the firewall added to CSC using Zero Touch will not get added automatically to SonicWall Analytics and need to be added manually.

Note: Firewall added to CSC using Zero Touch will NOT get added to SonicWall Analytics system as the above þÿoptions won t show up. Hence need to be added manually. Please refere to kb
https://www.sonicwall.com/support/knowledge-base/?sol_id=190523123417256

Can the firewall with CSC Reporting & Analytics licenses be added to Analytics?

The firewall can be added to SonicWall Analytics but data will be stored locally. In such case firewall need to delete þÿfrom CSC and added to Analytics first and then again back on CSC with correc
details.

- ***How to use Full Management and Reporting & Analytics on CSC while using SonicWall Analytics.?***

This requires full management license for firewall and an On-Prem SonicWall Analytics license applied to same Product Group/Tenant under MySonicWall account.
þÿðØ First setup CSC / MSW account and register the firewall in a Product Group/Tenant

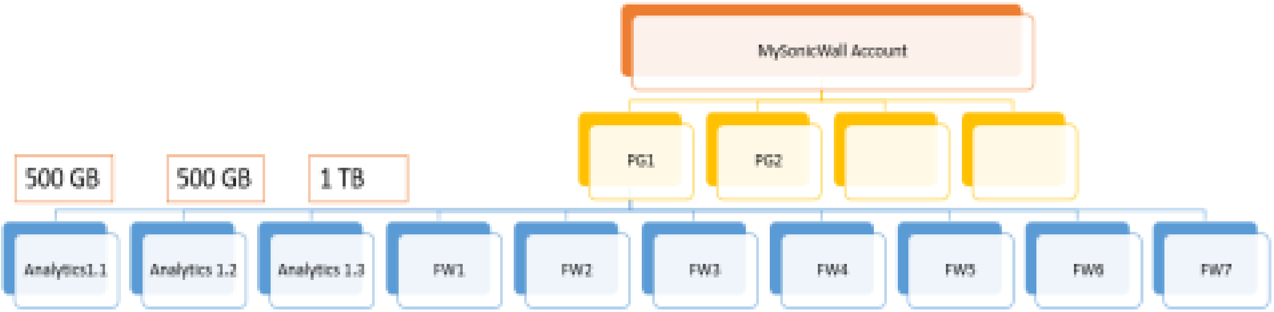
þÿðØ Now enable Analytics2.0 license on the same Product Group where firewall was registered
þÿðØ Setup and configure the SonicWall Analytics VM as per Startup guide and note down the IP
þÿðØ License firewall for CSC (Management) and add it to the CSC. Refer KB to add firewall

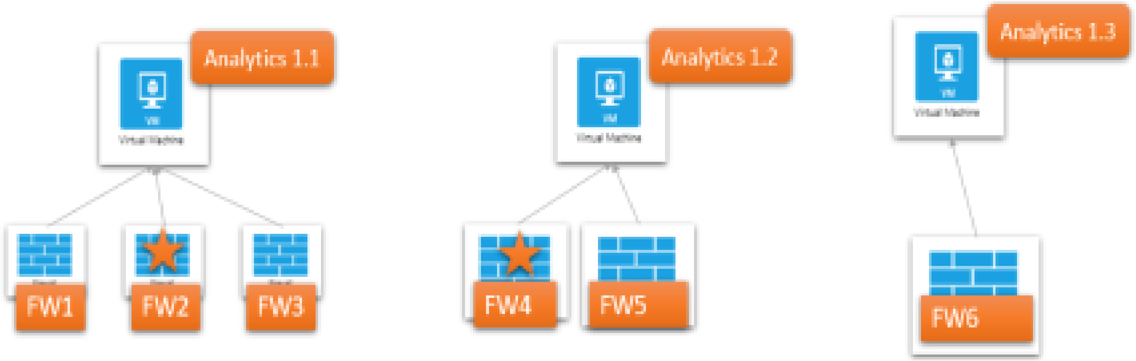
Where Reporting data is stored when integrated with CSC?

When firewall is added to CSC for Management and to On-Prem Analytics, the data will always be stored locally in On-Prem Analytics system.

Can we have more than one SonicWall Analytics system under same Tenant?

Yes, More than one SonicWall Analytics deployments are supported under same Tenant with separate license for each instance. See example below:
A MySonicWall account have two product groupsþÿ PG1 and PG2. In PG 1, there are 3 instances of SonicWall Analytics enabled with different licenses and has 7 firewalls associated.
Now firewalls FW1, FW2, FW3 are sending flow data to Analytics 1.1, FW4, FW5 sending flow data to Analytics 1.2 and FW 6 sending flow data to Analytics 1.3 respectively while FW7 is NOT sending flow data to any of On-prem SonicWall Analytics VMs. (below is a sample diagram)





Analytics 1.1 (and 1.2) have 500GB license which means the VMs will analyze a maximum of last 500GB flows data sent from the FWs and if the firewalls send more than 2 GB data for any given day, the SonicWall Analytics will NOT analyze data beyond 2GB (it will drop those flow-logs).
For analytics 1.1 VM, if the firewalls send a >= 2GB flow data for 250 days, the Analytics will continue to analyze the data until the usage limit (500GB) is hit, and then will only keep last 500GB of analyzed data.
The star marked firewalls - FW2 and FW4 þÿ have been added using CSC-Integration (Please refer question steps). It means for FW2 and FW3, the reporting/analytics data can be viewed on On-prem SonicWall Analytics as well on CSC-Analytics.

How does On-prem SonicWall Analytics gets information about Applications and Websites visited.

On-prem Analytics analyses flow dataþÿ sent by firewalls these logs contain key information Websites etc. The firewalls must be configured with appropriate settings for it to be able to send appropriate logs to

Analytics.
Please refer SonicWall Knowledge Base Articles to learn about enabling settings such as CFS, DPI-SSL etc.
https://www.sonicwall.com/support/knowledge-base/?sol_id=190205194634363
https://www.sonicwall.com/support/knowledge-base/?sol_id=181015225631727

How to backup IPFIX / Flow reporting data?

In SonicWall Analytics, you can backup Only System configuration but NOT the IPFIX data as that is stored on External Mount. In such case, please backup External Mount Drive outside Analytics system.