



Contents

About this Guide	. 4
Guide Conventions	. 5
System Requirements	6
Supported Firewalls	. 6
Additional Firewall Requirements	. 7
Supported Platforms	. 7
Hardware Compatibility	. 7
Minimum Requirements	8
IPFIX Based Licensing Model	. 8
IPFIX Based Capacity Planning	. 8
Backup and Recovery Information	10
Importing Firewall Configurations	.10
Creating a MySonicWall Account	11
Installing On-Premises Analytics on ESXi	13
Obtaining the Installation Image	.13
Installing On-Premises Analytics on ESXi	.14
Configuring On-Premises Analytics on ESXi	22
Adding Firewalls to On-Premises Analytics	34
Licensing and Registering Your On-Premises Analytics Instance	40
Registering the On-Premises Analytics Instance	.40
Activating Firewall Licensing for Syslog-Based On-Premises Analytics	44
Deregistering Your On-Premises Analytics Instance	.47
Upgrading On-Premises Analytics	.48
Upgrading Analytics 2.5.7	.48
Upgrading Analytics with data in external disk	.49
Upgrading Analytics with data in internal disk	49
Unmounting the Hard Disk from older Analytics Version	50
Mounting the Hard Disk on new Analytics Upgrading Analytics using SWI file	51
Migrating Data From Internal to External Diak	EC
Migrating Data From internal to External Disk	50
Preparing the Analytics to Add External Disk	00
	J/

Migrating the Data To External Disk
Using the Management Console
Connecting to the Console
Management Console Operations
System Info64
Storage
Network Interfaces
Diagnostics
NTP Server
Reboot Shutdown
About
Logs
Using SafeMode on the Management Console
Enabling SafeMode
Disabling SafeMode
Configuring the Network Interfaces in SafeMode71
Installing a Software Upgrade in SafeMode
Downloading Logs in SafeMode
SonicWall Support
About This Document

About this Guide

This SonicWall On-Premises Analytics Deployment Guide describes how to install and manage SonicWall Analytics package on ESXi.

On-Premises Analytics collects data from firewalls, analyze them, and present them as actionable intelligence. For an overview of product features, refer to the SonicWall On-Premises Analytics Getting Started Guide.

Chapter 3, Installing On-Premises Analytics on ESXi, details how to install on ESXi

Chapter 4, Licensing and Registering Your On-Premises Analytics Instance, tells how to access serial numbers and authorization codes and how to use them.

Chapter 5, Upgrading On-Premises Analytics, tells how to load a new revision or software patch of On-Premises Analytics on ESXi.

Chapter 6, Migrating Data From Internal to External Disk, describes the process to migrate Analytics data from internal disk to external disk.

Chapter 7, Using the Management Console goes over steps using the Management Console to configure the software and diagnose problems.

Guide Conventions

These text conventions are used in this guide:

- (i) **NOTE:** A NOTE icon indicates supporting information.
- (i) | IMPORTANT: An IMPORTANT icon indicates supporting information.
- () | **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.
- M WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<variable></variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber= < <i>your serial number</i> >, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

System Requirements

2

Before moving to installation or upgrade of Analytics, review the following requirements:

Topics:

- Supported Firewalls
- Additional Firewall Requirements
- Supported Platforms
- Hardware Compatibility
- Minimum Requirements
- IPFIX Based Licensing Model
- IPFIX Based Capacity Planning
- Backup and Recovery Information
- Importing Firewall Configurations
- Creating a MySonicWall Account

Supported Firewalls

On-Premises Analytics can collect data from the following firewalls:

Entry-Level Firewalls	SOHO W
	TZ Series
	NSv 10 -100
	NSv 270 - 870
Mid-Range Firewalls	NSA 2500 - 6600
	NSa 2650 - 6650
	NSv 200 - 400
	NSA 2700 - 6700

High-End Firewalls	SuperMassive 9000
0	Series 10K Series, 11K Series, 12K Series, 13K Series and 15K Series
	NSa 9250 - 9650
	NSv 800 - 1600

Additional Firewall Requirements

Additional requirements include the following:

- Each firewall must be licensed with the Comprehensive/Advanced Gateway Security Suite (CGSS/AGSS).
- Firewalls supported by an On-Premises Analytics instance must be in a single group or tenancy.
- Firewalls added to On-Premises Analytics should not have NSM Advanced licenses enabled in CSC.
- Firewalls with NSM Advanced licenses added to CSC using Zero Touch are not supported for On-Premises Analytics.
- Each firewall must have HTTPS management enabled.
- (i) **IMPORTANT:** If a firewall is behind a NAT device, then the HTTPS management port must be opened for the cloud services to communicate with the firewall.

Supported Platforms

Release Version	Supported ESXi Version
SonicWall_On-Prem_Analytics_2.5	ESXi 5.5 or higher

(i) NOTE: ESXi 5.5 or higher (except ESXi 7.0.3) is recommended for production environments. The ESXi vswitch configuration should have the MAC address changes option enabled.

- (i) | NOTE: The image files for installation are available on MySonicWall.
- (i) NOTE: Analytics does not support vSphere 8.

Hardware Compatibility

SonicWall On-Premises Analytics is supported on ESXi platforms running on relatively modern chip-sets, Intel Penryn and above (2008). If the chip-set is too old, the installation will halt with a message, "This system does not support SSE4_1". For more information, see KB Article.

Minimum Requirements

Standard minimal hardware settings for an On-Premises Analytics instance running on any platform include:

- 4 CPUs (2.4 GHz processor)
- 8 GB main memory for IPFIX reporting, 16 GB main memory for Syslog reporting
- 68.41 GB disk size (preferably SSDs)
- 1 virtual NICs (vSwitches)

At the lowest license level, an additional external mount of 500 GB of storage is required for logs storage.

IPFIX Based Licensing Model

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 will simply be dropped and data will again be logged starting with the next day.

(i) **IMPORTANT:** To choose when the day starts, regardless of the deployment location, refer to ESXi documentation. This requires advanced competence with ESXi.

Storage (based on licenses)	Flows per second or day	Storage Limit
2 GB/ day	300 flows/sec and 20 million flows/day	500 GB
5 GB/ day	750 flows/sec and 50 million flows/day	1 TB
15 GB/ day	2250 flows/sec and 150 million flows/day	5 TB
30 GB/ day	4500 flows/sec and 300 million flows/day	10 TB
100 GB/ day	15000 flows/sec and 1 billion flows/day	Unlimited

The following table summarizes currently available licensing levels.

IPFIX Based Capacity Planning

The following table links hardware requirements to license levels and flows/logs per second or per day.

Typical Installations	Storage(based on licenses)	Flows per second or day
4 Core, 8 GB -default	2 GB/ day	300 flows/sec and 20 million flows/day
8 Core, 16 GB	5 GB/ day	750 flows/sec and 20 million flows/day
16 Core, 32 GB	15 GB/ day	2250 flows/sec and 20 million flows/day
32 Core, 64 GB	30 GB/ day	4500 flows/sec and 20 million flows/day

64 Core, 64 GB	100 GB/ day	15000 flows/sec and 20 million flows/day
,		

In the following three tables, hardware requirements for specific license levels are linked to specific numbers of different models of firewalls.

4 Core, 8 GB - default 10 (Includes all TZ and SOHO models along with NSv models 10 to 100.) 8 Core, 16 GB 40 16 Core, 32 GB 80 32 Core, 64 GB 160 64 Core, 64 GB 350 VM Hardware Configuration VSa / NSv medium capacity (number of firewalls) 4 Core, 8 GB - default 1 (Includes NSa 2600-6600, NSv 200-400.) 8 Core, 16 GB 3 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration SM / NSa / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 4 Core, 3 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 1 16 Core, 32 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 3	VM Hardware Configuration	TZs / SOHOs / NSv low capacity (number of firewalls)
8 Core, 16 GB 40 16 Core, 32 GB 80 32 Core, 64 GB 160 64 Core, 64 GB 350 NSa / NSv medium capacity (number of firewalls) 4 Core, 8 GB - default 1 (Includes NSa 2600-6600, NSv 200-400.) 8 Core, 16 GB 3 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration M Sa / NSv high capacity (number of firewalls) 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration SM / NSa / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6	4 Core, 8 GB - default	10 (Includes all TZ and SOHO models along with NSv models 10 to 100.)
16 Core, 32 GB 80 32 Core, 64 GB 160 64 Core, 64 GB 350 NSa / NSv medium capacity (number of firewalls) 4 Core, 8 GB - default 1 (Includes NSa 2600-6600, NSv 200-400.) 8 Core, 16 GB 3 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration SM / NSv high capacity (number of firewalls) 4 Core, 64 GB 25 VM Hardware Configuration SM / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6 32 Core, 64 GB 1	8 Core, 16 GB	40
32 Core, 64 GB 160 64 Core, 64 GB 350 VM Hardware Configuration 4 Core, 8 GB - default 1 (Includes NSa 2600-6600, NSv 200-400.) 8 Core, 16 GB 3 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration SM / NSa / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 1	16 Core, 32 GB	80
64 Core, 64 GB350VM Hardware ConfigurationNSa / NSv medium capacity (number of firewalls)4 Core, 8 GB - default1 (Includes NSa 2600-6600, NSv 200-400.)8 Core, 16 GB316 Core, 32 GB632 Core, 64 GB1264 Core, 64 GB25VM Hardware ConfigurationSM / NSa / NSv high capacity (number of firewalls)4 Core, 8 GB - default0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800- 1600.)8 Core, 16 GB116 Core, 32 GB332 Core, 64 GB1	32 Core, 64 GB	160
VM Hardware ConfigurationNSa / NSv medium capacity (number of firewalls)4 Core, 8 GB - default1 (Includes NSa 2600-6600, NSv 200-400.)8 Core, 16 GB316 Core, 32 GB632 Core, 64 GB1264 Core, 64 GB25VM Hardware ConfigurationVM Hardware ConfigurationSM / NSa / NSv high capacity (number of firewalls)4 Core, 8 GB - default0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800- 1600.)8 Core, 16 GB116 Core, 32 GB332 Core, 64 GB6	64 Core, 64 GB	350
4 Core, 8 GB - default 1 (Includes NSa 2600-6600, NSv 200-400.) 8 Core, 16 GB 3 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration SM / NSa / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6	VM Hardware Configuration	NSa / NSv medium capacity (number of firewalls)
8 Core, 16 GB 3 16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration VM / NSa / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6	4 Core, 8 GB - default	1 (Includes NSa 2600-6600, NSv 200-400.)
16 Core, 32 GB 6 32 Core, 64 GB 12 64 Core, 64 GB 25 VM Hardware Configuration SM / NSv high capacity (number of firewalls) 4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6	8 Core, 16 GB	3
32 Core, 64 GB1264 Core, 64 GB25VM Hardware ConfigurationSM / NSa / NSv high capacity (number of firewalls)4 Core, 8 GB - default0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800- 1600.)8 Core, 16 GB116 Core, 32 GB332 Core, 64 GB6	16 Core, 32 GB	6
64 Core, 64 GB25VM Hardware ConfigurationSM / NSa / NSv high capacity (number of firewalls)4 Core, 8 GB - default0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800- 1600.)8 Core, 16 GB116 Core, 32 GB332 Core, 64 GB6	32 Core, 64 GB	12
VM Hardware ConfigurationSM / NSa / NSv high capacity (number of firewalls)4 Core, 8 GB - default0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800- 1600.)8 Core, 16 GB116 Core, 32 GB332 Core, 64 GB6	64 Core, 64 GB	25
4 Core, 8 GB - default 0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.) 8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6	VM Hardware Configuration	SM / NSa / NSv high capacity (number of firewalls)
8 Core, 16 GB 1 16 Core, 32 GB 3 32 Core, 64 GB 6	4 Core, 8 GB - default	0 (Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800- 1600.)
16 Core, 32 GB 3 32 Core, 64 GB 6	8 Core, 16 GB	1
32 Core, 64 GB 6	16 Core, 32 GB	3
	32 Core, 64 GB	6
64 Core, 64 GB 12	64 Core, 64 GB	12

The following table shows recommended guidelines for main memory to support different numbers of firewalls.

Number of Firewalls Recommende	ed Amount of Main Memory
10 8 GB	
40 16 GB	
80 32 GB	
350 64 GB	

Example:

This example considers license levels required to collect and analyze IPFIX data from five TZ series firewalls and one NSa 9450 firewall.

Looking at the table linking VM hardware configurations to entry-level firewall numbers, we see that a 4 CPU, 8 GB VM should handle up to ten of these TZ series firewalls.

VM Hardware Configuration	TZs / SOHOs / NSv low capacity (number of firewalls)
4 Core, 8 GB - default	10

Likewise, we see that a 8 core, 16 GB can handle IPFIX flows from a single high-capacity firewall such as the NSa 9450.

VM Hardware Configuration	SM / NSa / NSv high capacity (number of firewalls)
4 Core, 8 GB - default	1

So, it makes sense choose the license level associated with 12 cores 24 GB VM. This will support 50 million log entries per day and should cover these six firewalls. 10 cores may suffice, but 12 should provide head room.

Of course, this sort of heuristic approach has its limits. Whether the firewalls are running applications that throttle throughput (for example, Advanced Threat Prevention), or whether the firewalls are deployed on the perimeters of a single-site, enterprise network or, instead the NSa 9450 is on an intercontinental link within the enterprise network; these are all factors to consider.

(i) | NOTE: Contact you SonicWall sales representative for further guidance.

Backup and Recovery Information

In certain situations, it might be necessary to contact SonicWall Technical Support, use SafeMode, or deregister the On-Premises Analytics instance:

- If the splash screen visible through the platform console remains displayed, this can indicate that the disk is corrupted. Please contact SonicWallTechnical Support for assistance.
- If the disk is not recoverable, then the instance needs to be deregistered with MySonicWall. See Deregistering Your On-Premises Analytics Instance for information.
- If On-Premises Analytics fails to boot, it may still allow access to the Management Console through the
 platform remote console. Check the platform webpage to ensure that the minimum required memory is
 available. If it still cannot boot up, check the logs at the Management Console, send diagnostics reports to
 technical support (see Diagnostics), and contact SonicWall Technical Support for assistance. For details
 on using the Management Console, refer to Using the Management Console.

Importing Firewall Configurations

The import of configuration settings is not supported from SonicWall firewalls in an On-Premises Analytics. Export of configuration settings to support re-deployment of an instance is possible. Contact SonicWall Technical Support for details.

Creating a MySonicWall Account

A MySonicWall account is required to obtain the file for initial installation and for product registration to enable full functionality of the On-Premises Analytics instance.

(i) **NOTE:** MySonicWall registration information is not sold or shared with any other company.

To create a MySonicWall account:

- 1. In your web browser, navigate to https://www.mysonicwall.com.
- 2. In the login screen, click the Sign Up link.

Sonic wall	
MYSONICWALL	
Login with your MySonicWall account credentials	
Username or Email address	
Next	
Forgot username or email? Sign Up	

- 3. In the Account page, enter the Email, Domain UserName, Domain Password.
- 4. Enable two-factor authentication, if desired.
- 5. If you enabled two-factor authentication, select one of the following authentication methods:
 - Email (one-time passcode) where an email with a one-time passcode is sent each time you log into your MySonicWall account.
 - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code.
- 6. Click on **Continue** to navigate to the **COMPANY** page.
- 7. Complete the company information and click **Continue**.
- 8. In the **YOUR INFO** page, select whether you want to receive security renewal emails.

- 9. Identify whether you are interested in beta testing new products.
- 10. Click **Continue** to go to the **EXTRAS** page.
- 11. Select whether you want to add additional contacts to be notified for contract renewals.
- 12. If you opted for additional contacts, input the information and click Add Contact.
- 13. Click Finish.
- 14. Check your email for a verification code and enter it in the **Verification Code** field. If you did not receive a code, contact Customer Support by clicking on the link.
- 15. Click **Done**. You are returned to the login window so you can login into MySonicWall with your new account credentials.

Installing On-Premises Analytics on ESXi

Topics:

- Installing On-Premises Analytics on ESXi
- Configuring On-Premises Analytics on ESXi
- Adding Firewalls to On-Premises Analytics

Obtaining the Installation Image

When you purchase a SonicWall On-Premises Analytics instance from a distributor, you will receive a fulfillment email with your Activation Key code. You can enter this information in MySonicWall in an initial registration process to gain access to the image (vhd) file.

If you do not have a MySonicWall account, see Creating a MySonicWall Account.

To perform initial registration and obtain the image file for deployment:

- 1. In a browser, log into your MySonicWall account.
- 2. Navigate to Product Management > My Products.
- 3. Fill in the Activation Key.



3

- Click Confirm and navigate to Resources & Support > My Downloads. You are now given access to the .ova file for installation on ESXi.
- 5. Download the image file and save it to your local.
 - INOTE: For additional details on this process, refer to Registering the On-Premises Analytics Instance.

Installing On-Premises Analytics on ESXi

Install On-Premises Analytics by deploying an OVA file to your ESXi server. Each OVA file contains the software components needed. Deploy the OVA file by using the vSphere or vCenter client, which are available with ESXi.

- (i) **NOTE:** The elements of VMware must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.
- (i) NOTE: Step 7 has some important information about selecting your networks. Even if you do not need all these step-by-step instructions, be sure to follow the instructions in Step 7 to avoid connectivity issues after the deployment.

To perform a fresh install of On-Premises Analytics on ESXi:

- 1. Download the On-Premises Analytics OVA file from MySonicWall to a computer with vSphere / vCenter access.
- 2. Access vSphere and log on to your ESXi server.
- 3. Navigate to the location where you want to install the virtual machine, and select the folder.
- 4. Right-click on the target folder or select Actions and click Deploy OVF Template.



- 5. In the Select template screen,
 - Select Local file.
 - Click **Browse** and navigate to the On-Premises Analytics OVA file that you had downloaded.

1 Select template	Select template
2 Select name and location	Select an OVF template.
3 Selecta resource	Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer,
Review details	such as a local hard drive, a network share, or a CD/DVD drive.
Select storage	O URL
6 Ready to complete	
	Local file
	Browse 1 file(s) selected, click Next to validate

- 6. Click Next.
- 7. In the **Select name and location** screen, type a descriptive name for the On-Premises Analytics instance into the **Name** field, and then select the location for it from the ESXi folder structure.

Deploy OVF Template		9
 1 Select template 2 Select name and location 3 Select a resource 4 Review details 	Selectneme and location Enter a name for the OVF and select a deployment location. Name [SonicWall_Analytics_For_VMWare	
5 Select storage 6 Ready to complete	Selec a datacenter or folder. Venter6-pr.s.vus.sonicwall.com Venter6-pr.s.vus.sonicwall.com Venter6-pr.sevices Venter6-pr.	
	Beck	Next Finish Cancel

- 8. Click Next.
- 9. In the **Select a resource** screen, click **Next** to accept the default resource for the selected folder, or select a different resource and then click **Next**. Wait while the resource is validated. This is the resource pool where you want to deploy the template.

1 Select template 2 Select name and location	Select a resource Select where to run the deployed template.	
3 Selecta resource	Filter Browse	
5 Select storage 6 Ready to complete	Select a host or cluster or resource pool or vapp. ▶ ■ IMResources ▶ ■ Matis-sonicosv ▶ ● Massing Projects ▶ ● MSWD8 ▶ ● SALT ▶ ● SALS ● SonicOS ▶ ● SonicOS – Wit	•
	G SonicOSv-Akbal G TecPhote G Vish-sonicosv G Vish-sonicosv G WWW	-

10. In the Review details screen, verify the template details and then click Next.

Deploy OVF Template			() »
1 Select template 2 Select name and location	Review details Verify the template	details.	
3 Select a resource	Publisher	No certificate present	
4 Review details	Download size	1.9 GB	
5 Select storage	Size on disk	Unknown (thin provisioned) 68.4 GB (thick provisioned)	
7 Customize template			
8 Ready to complete			
		Back Next Finish	Cancel

- 11. In the Select storage screen,
 - Select a data store from the table. This is the location where you want to store the virtual machine files.
 - Select virtual disk format from the drop-down list. SonicWall recommends Thick Provision, but any selection will work.

 1 Select template 2 Select name and location 	Select storage Select location to store the	files for the deployed to	emplate.							
 ✓ 3 Select a resource ✓ 4 Review details 	Select virtual disk format Thick provision lazy zeroed									
5 Select storage	Filter									
5 Select networks 7 Customize template 8 Ready to complete	Datastores Datastore	Clusters		@ % 📑 Q	Filter -					
 Ready to complete 	Name	Status	VM storage	policy Capacity	File					
	 Competent-Sor 	icOS-01 O No	rmai -	5 TB	402.44 GB					
	e i				1 Objects 🔁 Copy +					

- 12. Click Next.
- 13. In the **Select networks** screen, network interfaces are provided in a VM by default **GMS_X0** and **GMS_X1**. This is the same naming convention as a SonicWall firelwall. GMS_X1 is considered a WAN interface so the Destination Network should be changed to an externally accessible subnet.

1 Select template	1 6 6 6	
2 Selectname and location	Select networks Select a destination network for each source	ce network.
3 Selecta resource	Source Network	Destination Network
4 Review details	GMS_X0	10.203.26 X
5 Select storage	GMS_X1	10.203.26.X *
6 Select networks	1	
7 Customize template		
8 Ready to complete		
	IP Allocation Settings	
	IP protocol: IPv4	IP allocation: Static - Manual 🔞

(i) **NOTE:** The ESXi vswitch configuration should have the option for **MAC address changes** enabled for the vswitch ports connected to the On-Premises Analytics instance.

For advanced configurations (DVS), consult the VMware documentation on vswitch configuration.

(i) **NOTE: GMS_X1** (the default WAN Interface) is set to **DHCP** by default, with **HTTPS management** enabled for the On-Premises Analytics instance, as this configuration eases deployments in virtual/cloud environments.

- 14. Click Next.
- 15. In the **Ready to complete** screen, review the settings and click **Finish** to create the NSv appliance. To change any setting, click **Back** to navigate back through the screens to make any change.
- 16. The name of the new On-Premises Analytics appears in the left pane of the vSphere window when complete. To start the configuration of external storage, right click on the VM listing and select **Edit Settings**.

Navigator	¥	🔂 soniccore_de	eveloper_vm	ware_ova	*	
4 Back		Getting Started	Summary	Monitor	Configu	ure F
Control of the second end	Actions - sor Power Guest OS Snapshots Open Cons Migrats Clone Template Fault Toler: VM Policie: Compatibili Export Syst Edit Resou	ance s ty tem Logs	1W316_CV4	sonicco Guest C Compati VMW an IP Addi Hodd:	xe_deve DS: ibility: e Tools: me: esses:	loper_v Other 3 ES30 5 Not nur More in localho
Recent Objects K Created Created Sonicrore, developer, vmware Truck Name	Keit Setting Move To Rename Fdit Notes	5				

17. Select New Hard Disk from the dropdown for New device and click Add.

Virtual Hardware VM C	Options	SDRS Rules	VA	pp Optio	ns		
CPU	2		-	0			
Memory	10240		•	MB	-		
Hard disk 1	68.414	0625	*	GB	+	1	
G SCSI controller 0	LSI Log	gic Parallel					
Retwork adapter 1	10.203	3.26.X (dvSwitch	0		-	Connect	
Network adapter 2	10.203	3.26.X (dvSwitch	0			Connect	
CD/DVD drive 1	Client	Device				Connect	
Floppy drive 1	Client	Device			-	Connect	
Video card	Specif	y custom setting	is .		-		
WMCI device							
Other Devices							
Upgrade	Sch	edule VM Comp	atibi	ity Upgra	de		
New device:		A New Han	d Die	sk		Add	

- 18. In this case, an additional 500 GB for log storage is defined.
 - (i) **NOTE:** Define additional storage in line with your license level. Refer to Licensing Model. Including additional storage space, at minimum 500 GB is recommended.

Virtual Hardware	VM Options	SDRS Rules	vApp O	ptions						
Sharing		No sharing								
Disk File		[Compellen soniccore_c ore_develop	I-SonicOS teveloper per_vmws	S-01] _vmw are_ov	are_ova/si /a.vmdk	onicc				
Shares		Normal		-	1,000					
Limit + IOPs		Unlimited								ł
Disk Mode		Dependen	t		0					1
Virtual Devic	e Node	SCSI contr	olier 0		SCSI(0	:0)		-		1
SCSI control	ler 0	LSI Logic P	arallel							1
Network ada	pter 1	10.203.26.X (dvSwitch)			-	Co	nnect		1	
Network ada	pter 2	10.203.26.	10.203.26.X (dvSwitch)			-	Co	nnect		1
CD/DVD driv	ve 1	Client Devi	ce	e 🛛 🗐 🗔 Connect				÷		
Floppy drive	1	Client Devi	Client Device			Co	nnect		1	
Video card		Specify custom settings							1	
VMCI device	í.									1
Other Devices										1
Upgrade		Schedule	e VM Con	npatib	iity Upgra	de				1
New Hard d	isk	500			GB				0	
New o	levice:	A New Har	d Disk			Add				

19. Bring up the On-Premises Analytics instance. The System Console will show a boot message. This initial boot-up may take 5 to 10 minutes.



Configuring On-Premises Analytics on ESXi

To configure On-Premises Analytics on ESXi:

- 1. Launch the Management Console.
- 2. Navigate to Storage.



3. Select Add Storage, select Yes and press enter to confirm.

-Menu	Storage	
Sustem Info	Additional storage status	Found and not encrumted
Storage	Additional storage action	Add storage
Netuonk Intenfaces	naareronar storage actron	i nuu storuge i
Disgreation		
NTD Services		
nir server		
Reboot I Shutdown		
About		
Logs		
	_Destroy Data	
	Encrypt entire disk? This will destru	by ALL data on the disk.
	Yes	
	No	
	Confirm (Enter)	Cancel (Esc)
		ounder (List)

4. Enter a key for the additional storage. The key is set when the Mount operation is performed for the first time on an additional storage disk. This key is required to re-mount the additional storage after upgrade or redeployment.

- (i) **IMPORTANT:** Be sure to securely store/note down your additional storage key. This key cannot be modified or reset once it has been set. Should the key be lost, misplaced or forgotten, it will be impossible to access or recover the data stored in the additional storage media.
- 5. Click enter to start disk encryption.

Menu System Info Storage Metwork Interfaces Diagnostics NTP Server Reboot I Shutdown About Logs	Storage Additional storage status Additional storage action	Found and not encrypted Add storage
-Adding stor Starting dis	age k encryption. Please wait. Scooll (Un Down Left Right)	Close (Ecc.)
	botorr top bown here nights	

6. Click enter to reboot. You will have to enter the encryption key.

Sureng Storage Network Interfaces Diagnostics NTP Server Locklown Mode Reboot i Sbotdown About Logs	Additional storage states Additional storage	Found and not mounted	
	- Pestroj Dela A rebot is required to complete the d Yes No		
Up > Down to amignet its TAB to move between vie Enter to actionswift ar	ens INC N item		

7. Navigate to the Network Interface setting, press Enter and select ens160. The system will use DHCP, if available, to assign an IP address.

Take note of the IP address. This will be the access point for the On-Premises Analytics instance.

(i) **NOTE:** Without DHCP, you will enter a static IP address along with associated Netmask, Mac address, Gateway entries.

	Network Interfaces		
ustem Info	Network Interface	ens160 1	
etwork Interfaces	DHCP	[Enabled]	
lagnostics	ll an e sea	10.000 01.010	
ITP Server	IPU4 Address	10.203.26.240	
leboot Shutdown	Mac address	00:50:56:9f:60:fb	
ibout	Gateway	10.203.26.1	
ogs			
	DNS 1	[173.249.212.25]	
	DHS 2	[8.8.4.4]	
Up / Down to select items			
TAB to move between views			
Enter to action/edit an item			

- 8. Set DNS for your network environment.
- 9. Enter the IPv4 address in a web browser. The login screen will appear.

SONIC WALL analytics			
Login with your credentials Username			
Next		0	What is SonicWall Analytics? SonicWall Reporting and Analytics Platform
	and a	0	SonicWall Analytics Live Demo Learn more about SonicWall Analytics by watching the live demo
		0	Empowered by Capture Security Center Reduce operating expenses while increasing service agility by partnering with SonicWall Analytics and Capture Cloud

- 10. For initial access, use admin and password.
- 11. The first time up, the instance presents an initialization wizard. Use the Serial Number and Authorization Code. For this information, refer to Registering the On-Premises Analytics Instance.
- 12. The initialization wizard will be displayed. Click Next.

Introduction Network Settings Time Settings Summary	Step 1. Introduction Welcome to the System Configuration wizard Configuring the system involves setting Host name, IP address, DNS, Time and other system specific parameters. This wizard will guide you through the process of configuring a host, step by step.
	1

13. In Network Settings screen, you may choose to change the settings. Then click Next.

SONICWALL SonicWall Analytics 2.5	-			
	SYSTEM CONFIGU Introduction Network Settings Time Settings Summary	RATION Select IP type: © DHCP + IPv4 Network Settin Name Domain Host IP address/ Subnet mask Default gateway	 Static gs analytics sonicwall.com 10.206.56.137 255.255.0 10.206.56.1 	eg:hostname eg:domain.com /
		DNS server 1 DNS server 2 + IPV6 Network Settin	10.50.129.148 10.50.129.149 gs Cancel	
				- SONICWALL

14. In Time Settings screen, make adjustments, if necessary, and click Next.

SYSTEM CONFIGN Introduction Network Settings Time Settings Summary	Step 3. Time Settings Time (Mrmmss) 20 • : 08 • : 24 • Date April • 22 • 2019 • TimeZone (UTC) Coordinated Universal Time • Set time automatically using NTP To continue, click Next.
	Back Next Cancel

15. In Summary screen, review the configurations. Click Back to adjust else click Apply.

SONICWALL' S	nicWall Analytics 2.5
	SYSTEM CONFIGURATION
	Introduction Step 4. Summary Network Settings Network Settings Network Settings Time Settings Network Settings Network Settings Domain sonicwall.com P address 10.206.56.137 Default gatewary 10.206.56.1 Summary DDS server 1 10.50.129.148 DNS server 2 10.50.129.149 Time Settings Click "Apply" and proceed to complete the setup process. NOTE This may take up to 5 minutes. Please don't close the browser window while system setup is running
	Back Apply Cancel SONICWALL

16. Click **OK**, when prompted to confirm.

SONICWALL	SonicWall Analytics 2.5		10.206.56.137 s Do you want to ap	ays pply the changes?
	SYSTEM	CONFIGURATION		OK Cancel
	Introductio Network 5 Time Setti Summary	n Step 4 lettings N ngs Ti Click NOTI while	Summary etwork Settings Hostname Domain III address Dataut gatewary Suboret mask DNS server 1 DNS server 2 me Settings Time TimeZone "Apply" and proceed t This may take up to 1 system setup is runni	analytics sonicivalizom 10.206.56.137 10.206.56.1 255.255.255.000 10.50.129.148 10.50.129.149 2019/04/22.20.08.24 (UTC) Coordinated Universal Time to complete the satup process. 5 minutes. Please don't close the browser window ng
		(Back Apph	Cancel SONICWALL

17. Success message will be displayed. Click **Finish**.

(i) **NOTE:** The On-Premises Analytics instance will restart on clicking Finish.

Sonic wall '	SonicWall Analyt	tics 2.5		
		SYSTEM CONFIGU Introduction Network Settings Time Settings Summary	Step 4. Summary Stylen Configuration applied successfully.	
		1	Finsh	SONICWALL

- 18. When the login screen reappears, enter admin in **Username**, click **Next** and enter password in **Password** to login.
- 19. When the installation wizard appears, click Next.
- 20. Choose Flow based or Syslog based to depending the use case for your deployment and click Next.

ntroduction	Step 2. Reporting type
Reporting type	Please select a report type that will be used in report generation for units added to the system.
Summary	Flow based
,	Reports are generated using IPFIX packets for units that have reporting licensed and enabled. The Analytics and Live Monitor feature will be available with this selection.
	\bigcirc Syslog based
	Reports are generated using Syslog packets for units that have reporting enabled.

21. The system will then ask for confirmation, click **Apply**.

SONICWALL AN	ALYTICS INSTALLATION
Introduction	Step 3. Summary
Reporting type	SonicWall Analytics will be configured for Flow based reporting and Analytics.
Summary	Click "Apply" and proceed to complete the setup process.
	NOTE This may take up to 5 minutes. Please don't close the browser window while system setup is running
	Back Apply Cancel
	SONICWALL'

22. When the system indicates that the configuration is complete, click **Finish**.

SONICWALL ANALY	TICS INSTALLATION
Introduction Reporting type Summary	Step 3. Summary Install mode and Role configuration settings have been applied successfully. Image: Please click Finish to perform a restart of the system for the changes to take effect.
	Finish

23. You will be prompted to link to your MySonicWall account.

	iceren Anaryces
Please register your Soni	cWall product
	Serial Number Not Registered
MySonic	Wall username/email
I	Password
	Login
Forgot your Username o	r Password?
Croate MySonicWall acc	ount 📀

- 24. To complete licensing for a Syslog-based Analytics instance, go to Activating Firewall Licensing for Syslog-Based On-Premises Analytics.
- 25. After linking to MySonicWall, you will provide the Serial Number and Authorization Code from Step 10. Use a Friendly Name to distinguish from other instances of On-Premises Analytics.

ONIC WALL SonicWall Analytics	
Serial Number	Not Registered
Authentication Code	
- What is this?	
Friendly Name	
ibmit	

26. Click Submit.

Serial Number	Not Registered
Serial Number	
004010363A89	
Authentication Code	
3CNK - EITLE What is this?	
Friendly Name	
Analytics 2.0 - Technical Publication	
Submit	

27. On completion of the registration process, click **Continue**.

SONICWALL	
SonicWall Analytics Serial Number 004010363A89	
Thank you for registering this product. Registration completed successfully.	
Continue	

28. Navigate to **System > Administration** and set new login credentials.

Analytics			
System	HOST SETTINGS		
- Status	Inactivity Timeout	10 minutes (-1 ~ never times out)	
- Licenses	ENHANCED SECURITY ACCESS (ESA)		
Time	1	Enforce Password Security	
- Administration	Number of failed login attempts before user can		
- Settings	be locked out		
 Diagnostics 	User lockout minutes		
- File Manager	Number of days to force password change		
- Backup/Restore	ADMINISTATOR PASSWORD		
- Shutdown	Administrator Name	admin	
1 1 1	Current Password		
Network	New Password		
	Confirm Password		
Deployment	Contract Parameter		
		C	Update Reset
ER Pow Agent			

Adding Firewalls to On-Premises Analytics

To add firewalls to On-premises Analytics:

1. Navigate to **HOME | Overview > Status** and click the Device Manager icon.



2. Click add icon +.

← → C ▲ Not secure	https://10.206.56.137/sgmi/auth				The second s
+ Q, C V DEVICE MANAGER 4	SONICWALL	SonicWall Analytics	HOME	REPORTS	ANADITICS
GobalVew (Locationwe)	Dverview	© / GlobalView			
	- Status - Devices - Dashboard	FIRMWARE DETAILS Number of Firewalls in the System FLOW DETAILS	0		
	Sumay 5	Flow Agent Firmware Version Data Stored for a Day Total Disk Size as per the License Available (Mounted) Disk Size ADDING AND DELETING FIREW.	2.2-1184412 0 tryte/2.68 500.68 40.68 ALLS		

3. Enter the Friendly Name, the Serial Number, and the Model of the firewall.

ADD FIREWALL	
Firewall Name	Ø
Serial Number	Ø
Model	▼ ①
CONFIGURATION 1. Login to the firewall and Co 2. And go to AppFlow -> GMS time.	ntigure "GMSFlow Settings" Flow server. Enable AppFlow

- 4. Click OK.
- 5. Navigate to a browser window and log into the firewall.

For IPFIX-based instances, follow steps 6 to 10 below.

For Syslog-based instances, go to Step 11.

- 6. Navigate to MANAGER | Appflow Settings > Flow Reporting | GMSFlow Server.
- 7. In the GMSFlow Server screen,
 - a. Enable Send AppFlow to SonicWall GMSFlow Server.
 - b. Enable Send Real-Time Data To SonicWall GMSFlow Server.



- 8. Navigate to Manage > AppFlow Settings | GMS Flow Servers.
- 9. In the GMS Flow Servers page,
 - a. Enter the IP address of the Analytics instance in the **GMS Flow Server Address** field (this is your Analytics deployment IP adress).
 - b. Click **Test Connectivity** to ensure the Analytics instance is accessible. The UP/REGISTERED message should appear.

If connectivity with the Analytics instance is a problem, go to MySonicWall and check that the firewall and Analytics instance are in the same Group or tenancy.

c. When configuration in this panel is complete, click **Accept** at the bottom of the page.


10. Repeat Step 2 to Step 9 for each firewall in the Group that you want to analyze IPFIX data from.

To configure firewalls to send syslogs to a Syslog-based Analytics instance:

- 11. Navigate to **MANAGE > Log Settings > SYSLOG**, click **Add**.
- 12. Enter the firewall details,
 - a. Select Name or IP address from the dropdown list.
 - b. Select Server Type as Syslog Server from the drowndown list.
 - c. Enter other parameters as required.

Sonic wall " M	letwork Security Appliance
Event Profile:	0
Name or IP Address:	syslog_deployment
Port:	514
Server Type:	Syslog Server ▼
Syslog Format:	Default
Syslog Facility:	Local Use 0
Syslog ID:	firewall
Enable Event Rate Limiting	
Maximum Events Per Second:	1000
Enable Data Rate Limiting	
Maximum Bytes Per Second:	1000000
Bind to VPN Tunnel and Create	Network Monitor Policy in NDPP Mode:
Local Interface:	Select an interface
Outbound Interface:	Select a tunnel interface ▼

13. Navigate to Log Settings > Base Setup and click Import Template.

SONIC WALL	Network Security Appliance MONITOR INVESTIGATE MANAGE QU	ICK CONFIGURATIO	N	_
Firewall Name: 2CB8ED233B5C • Objects	Filter View			_
System Setup Appliance Users	Logging Level Inform - Alert Level Alert - 🌣 🗙 📄 Save Template	↓ Import Templat	te View Logs	
Network	Category	Color ID	Priority 🝚	•
SD-WAN	▶ System		Mixed 🝚	
 High Availability 	▶ Log		Mixed 🝚	5
WAN Acceleration	Security Services		Mixed 🝚	5
VOIP	▶ Users		Mixed 🝚	5
Security Configuration	Firewall Settings		Mixed 🝚	5
Firewall Settings	Network		Mixed 🕥	ĩ
Security Services Decountion Services	VPN		Mixed	5
 Anti-spam 	High Availability	-	Mixed	1
	 3G/4G Modem and Module 		Mixed	
Logs & Reporting	• 30,40, Houen, and House	_	Mixed	1
Appflow Settings	 Firewall 		Mixed 🔵	1
Log Settings Base Setup	▶ Wireless		Mixed 🕥	P
SYSLOG	▶ VoIP		Mixed 🔵	Þ

14. Select Analyzer / Viewpoint / GMS as template and click Accept.

- 15. Repeat **Step 11** to **Step 14** for each firewall in the Group or tenancy you wish to receive Syslog data from.
- 16. To complete licensing for a Syslog-based Analytics instance, go to Activating Firewall Licensing for Syslog-Based On-Premises Analytics

Licensing and Registering Your On-Premises Analytics Instance

Topics:

- Registering the On-Premises Analytics Instance
- Activating Firewall Licensing for Syslog-Based On-Premises Analytics
- Deregistering Your On-Premises Analytics Instance

Registering the On-Premises Analytics Instance

Once you have purchased a license for a SonicWall On-Premises Analytics instance, you will receive an Activation Key code and a software image as a file. Use the file in the installation process described in . Use the Activation Key to register your product on MySonicWall. You will get the product serial number and authorization code from MySonicWall, these can be used to register the instance as you bring it up the first time.

To register your On-Premises Analytics appliance:

- Log into MySonicWall, navigate to Product Management > My Products and click on the add products icon at the upper right \$
- 2. Enter your activation key.



- 3. Select a product group into which you will deploy the instance.
 - a. Navigate to **My Groups**, either create a new group or tenancy.

	ATION		
My Group	S		
✿ / Resources & Suppo	rt		
4 Q	CREATE NEW TENANT	>	<
# TENANT NAME	Enter a group name to create new tenant	to share the products	I GROUP
1 Analytics-Beta	Tenant Name	Tenant Name	
2 Memory Products	UserGroup Name	Analytics	
		Cancel Confirm	

h	Or choose the group for	vour On-Promises An	alvtice instance and click	Register a new instance
υ.	Of choose the group for	your On-Fremises An	alylics instance and click	Register a new instance.

CHOOSE THE PRO	DUCT / GROUP FOR ACTIVAT	rion ×						
You have multiple products/Client Distribution Groups registered, please click on the appropriate product link to activate the service - SonicWall Analytics On-Prem								
NAME	SERIAL NUMBER	PRODUCT LINE						
analytics 2062	004010363A54	ON-PREM ANALYZER						
	Cancel	ister a new instance Activate						

4. Establish a Tenant Name and a Friendly name for the product.

REGISTER A PRODUCT	×						
Enter details below to complete registration of the following product:							
Serial number	004010230BF6						
Friendly name	Friendly name						
Authentication code	Authentication code						
Tenant Name	Michael Meredith Products						
	Cancel Register						

5. Select a Data Center Location.

Data Center Locat	on Select 👻
	North America
	Europe

6. Navigate to My Products and click on the information icon of your product.

← → C ▲ https://beta.myse	Job Search	n/muir/ui/pr Results 🗧 🥐	SonicWall Capture Se	 Engineering Hor 	ne – 🙀 Browse proj	ects - Sci 🙀 Tech Pi	ahs Board - Ac 🛛 🥐 S	ionicWall Analytics 🛛 🔤 A	nelytics on-prem b-			\$	0
SONICWALL'		MySonic	Wall SIMULATION							0	8 0	F	6
Overview	M ⊛/			S									
- Dashboard	\$	Q.									÷.	+ - 13	0
Product Management		STATUS	FRIENDLY NAME	SERIAL NUMBER	PRODUCT TYPE		TENANT NAME	FIRMWARE VERSION	SUPPORT	-			
- My Products 🔶	1	Offine	Mike"s analytics	CB0000006973	SonicWall CLIENT	Jan 31 2019	Memory Products						_
- My Orders		Citting	Exceletion	CHARGEDORE	Societabil (*) IENT	las 20 2018							
- My Quote		Gmale	senerytics	COOLOUGAN	Soucesal CDENT =	Man 90 2019							1
 Pree that software Catalon 	3	Offine	analytics	004010000002	On-Prem Analyzer	Jan 30 2019	Analytics-Beta	8.1			0	17	: W
- My Groupe	4	Offine	Capture Client Ten	CC0000191971	Capture Client Ten	Jan 30 2019	Analytics-Beta						
- My Promotions	5	Offline	Mike	CERCERCORDOCARDER	SonicWall CUENT	Jan 29 2019	Memory Products						-
Service Cotermination My Autoreneworks	6	Offline	Milez	CB0000006967	SonicWall CLIENT _	Jan 29 2019	Memory Products						1
	7	Offline	Capture Client Ten	CC0000191978	Capture Client Ten	Jan 29 2019	Memory Products						
Reports	в	Offline	189169066018	109164066016	SONICWALL TZ4_	Dec 18 2015	Analytics-Beta	6.2.6.0	Dec 18 2016	0			
UTILITIES													
🔎 Tooki	Sho	wing 8 of 8 ite	ma										
SonicWall version 13.26.72											TO	5 Privac	Fined

7. Note down the Authorization Code and Serial Number.

PRODUCT DETAILS				×
A Offline , Not Licensed				ē
O This is a secondary device associated with t	the primary senalnumber : 0040102930C9 as ON-PREM ANAL	YZER		
Serial Number	004010363489	Friendly name	TechPubs Analytics 2.0	
Registered On	22 Apr 2019	Release Status	Active ()	
Node Support	Unimited	Support Expiration	NEA	
Description	On-Prem Analyzer	Registration Code	GDTXYRMM	
Authentication Code	3CNK-DFLX	Fernivare Version	8.1	
Trusted	YES			
70.00114				

(i) **NOTE:** The Serial Number and Authorization Code is needed when you bring up the On-Premises Analytics instance for the first time.

Activating Firewall Licensing for Syslog-Based On-Premises Analytics

When firewalls reporting to the On-Premises Analytics package are added to new or existing tenants, licensing must be activated.

To activate license for a firewall added to a new Syslog Analytics tenant:

- 1. Navigate to Product Management > My Products page.
- 2. Select the firewall and click on the Licenses icon.

Sonic wall '	∙≡ №	/lySonicWal	I								8	õ
My Workspace ^{BETA}	Му	Prod	ducts									
 My Workspace 	軬 / Pr	oduct Manag	ement									
 Tenant Products 					QUICK REGISTER	Enter serial numb	per or activation key or	assign tok	ISTER Registe	ing multiple	Product	ts? or
 Register Products 	(A) (2									*	
- User Groups	¥ 1	~									-0-	F .
.	#	RELEASE ST	FRIENDLY NAME	SERIAL NUMBER	PRODUCT TYPE	REGISTERED ON 🕹	TENANT NAME	FIRMWARE VERSI	SUPPORT			
Overview	1	ENABLED	25-RTQA	004010351F3B	SONICWALL NSV	Mar 25 2020	Michael Meredith P	7.0.0.0	Mar 25 2021			
Product Management	2*	ENABLED	TZ570-158	2CB8ED694664	SONICWALL TZ 5	Feb 08 2020	Tech Pubs-TechPu	7.0.0.0	Feb 08 2022			
	3*	ENABLED	TZ570-159	2CB8ED6942A4	SONICWALL TZ 5	Feb 03 2020	Tech Pubs-TechPu	7.0.0.0	Feb 03 2022	1	\$ I	×
My Products My Promotions	4*	ENABLED	TZ570-157	2CB8ED69468C	SONICWALL TZ 5	Jan 28 2020	Tech Pubs-TechPu	7.0.0.0	Jan 28 2021		Licenses	
 Free Trial Software 	5*	ENABLED	M8200	004010288529	SonicWall Aventail	Oct 16 2019	Tech Pubs-TechPu	11.4.0	Nov 15 2019 !			
 Product Claims My Groups 	6*	ENABLED	Mike's8200	004010288528	SonicWall Aventail	Oct 16 2019	SonicWal_Group	11.4.0	Nov 15 2019			
– Catalog	7	ENABLED	TP-8200v	004010288527	SonicWall Aventail	Oct 16 2019	SonicWal_Group	11.4.0	Nov 15 2019 \rm			
 MSSP Monthly 	8*	ENABLED	Capture Client Ten	CC00000157CC	Capture Client Ten	Oct 16 2019	Tech Pubs-Private					

3. When the licensing list appears, identify the **Syslog Analytics** row and click on the key icon.

	DESKTOP & SERVER SOFTWARE					
	Global VPN Client	Licensed , Max count- 12	2	×	Try	0-7
	Global VPN Client Enterprise	Not Licensed		a.	Try	0-7
	VPN Policy Upgrade	Licensed	10	Ξ	Try	0-7
	WAN Acceleration Software	Not Licensed		T	Try	07
	Content Filtering Client	Not Licensed		×	Try	97
	Note: When used with Sonic/Wall firewalls, it's supported in firmware versions 5.90.4, 6.1.1.6, 6.1.2.1 and 6.2.7.7 or higher.					
	WAN Acceleration Client	Licensed	1	Ē	Try	0-7
	Please note: This service is available and can be used only with firmware version 5.9 and above.					
	Virtual Assist	Not Licensed		Ξ.	Try	07
	Analyzer	Not Licensed		Ξ	Try	0-v
L	SSL VPN	Licensed , Max count- 51	1) E		07
	Syslog Analytics	Not Licensed		Ĭ	Try	0- 7
Ľ	Capture Client	Not Licensed		Ъ.	Try	0-7
	DPI-SSL Enforcement	Not Licensed		Ξ		0.7
	Capture Client Advanced Threat Protection	Not Licensed		Ξ.	Try	07
	▼ SUPPORT SERVICES					
	Standard Support	Not Licensed		×.	Try	0-7
	24x7 Support	Not Licensed		Ē	Try	0-7
	Software and Firmware Updates	Expired	Nov 27 2019	Ξ	Try	07
L	Hardware Warranty	Licensed	Aug 29 2020	X	Try	0.7

4. Enter the Activation Key provided in Registering the On-Premises Analytics Instance.

PLEASE ENTER ACTIVATION KEY		×
Enter the activation key for the Serialnumber	on the service Syslog Analytics	
Please enter Activation key		
Registering multiple keys? click here for Multiservice acti	vation.	
	Cancel Confirm	

5. The system will now ask if the firewall will be licensed to serve a new or existing tenant.

ACTIVATE SERVICE	×
New Analytics Tenant O Existin	ng Analytics Tenant
	Cancel Activate

6. Return to the licensing list page and check that licensing is complete.

WAN Acceleration Client	Licensed	1	Έ	Try	07
Please note: This service is available and can be used only with firmware version 5.9 and above.					
Virtual Assist	Not Licensed		Ξ	Trγ	0+
Analyzer	Not Licensed		Π	Τrγ	0+
SSL VPN	Licensed , Max count- 51	1	Ξ	Try	07
Suslog Analytics	Licensed	Apr 5 2022	5	Iry	
Capture Client	Not Licensed		Ξ	Trγ	0+
DPI-SSL Enforcement	Not Licensed		π		0.4
Capture Client Advanced Threat Protection	Not Licensed		Π	Try	0-1

7. Navigate back to the **My Products** page and click on the Product Details icon.

Vy Products / Product Management OUCK REGISTER Enter serial number or activation key or assign tok REGISTER Registering multiple Products? or Keye?										
	2			QUICK REGISTE	R Enter serial numb	er or activation key or	assign tok	ISTER Reg	alstering multiple <u>Products</u> ? or <u>Keys</u> ?	
¥ 1	~								-0 T · L v	
,	RELEASE ST	FRIENDLY NAME	SERIAL NUMBER	PRODUCT TYPE	REGISTERED ON +	TENANT NAME	FIRMWARE VERSE	SUPPORT		
1	ENABLED	25-RTQA	004010351F3B	$SONICWALLNS_{V^{**}}$	Mar 25 2020	Michael Meredith P	7.0.0.0	Mar 25 2021		
2*	ENABLED	TZ570-158	208860694664	SONECWALL TZ 5	Feb 08 2020	Tech Pube-TechPu	7.0.0.0	Feb 08 2022		
3*	ENABLED	TZ570-159	2CB8E06942A4	SONICWALL TZ 5	Feb 03 2020	Tech Pubs-TechPu	7.0.0.0	Feb 03 2022		
4*	ENABLED	T2570-157	2CB8ED69469C	SONECWALL TZ 5	Jan 28 2020	Tech Pube-TechPu	7.0.0.0	Jan 28 2021		
5*	ENABLED	M8200	004010288529	SonicWall AventaiL.	Oct 16 2019	Tech Pubs-TechPu	11.4.0	Nov 15 2019	000=/×6	
6*	ENABLED	Milor/s8200	004010288528	SonicWall Aventail.	Oct 16 2019	SonicWall_Group	11.4.0	Nov 15 2019	Product Details	

8. Verify that the serial number for On-Premises Analytics is generated.

PRODUCT DETAILS								
A Offline , Not Licensed	Cottine , Not Licensed							
This is a secondary device associated v	with the primary serialnumber : 00401024F085 as Syslog Analy	tics						
Serial Number	1881696F136C	Friendly name	Nachiket TZ300					
Tenant Name	Hello_Syslog 🖋	Registered On	29 Aug 2019					
Node Support	Unlimited	Enable Zero Touch						
Support Expiration	NGA	Description	SONICWALL T2300					
Registration Code	KX4ESP6T	Authentication Code	XM84-UIRD					
Firmware Version	6.5.1.3-12n	Trusted	YES					
Applicable on Firewalls running Sonic	OS 6.5.1 and above.							
TO-DO List		Associated Products						
You have no pending tasks		HA Secondary (0)						
		SonicPoint (0)						
		WAN Acceleration (0)						
		SonicWave (0)						
		StorageModule (0)						
Parent Products								

Deregistering Your On-Premises Analytics Instance

You can de-register your On-Premises Analytics instance directly from the management interface. Deregistration puts the instance into the unregistered state and deletes the binding between it and its serial number in MySonicWall. Then you can use the serial number to register the same or another instance. Only one On-Premises Analytics instance is allowed per serial number. Be sure to delete the old, now unused VM.

(i) | **IMPORTANT:** Contact SonicWall Technical Support for assistance in this operation.

Upgrading On-Premises Analytics

This chapter explains how to load a new revision or software patch of On-Premises Analytics ESXi.

- (i) **NOTE:** SWI upgrade to Analytics 2.5.7 is not supported.
- Inote: In the event the Analytic GUI is unavailable, upgrades and hotfixes may be applied through the remote web interface in ESXi. This allows access to the Analytics Management Console. See Installing a Software Upgrade in SafeMode. In the event this step is necessary, please contact SonicWall Technical Support for assistance.

Topics:

- Upgrading Analytics 2.5.7
- Upgrading Analytics using SWI file

Upgrading Analytics 2.5.7

Users can upgrade to Analytics 2.5.7 from 2.5.6, 2.5.5 or 2.5.4.

() NOTE: It is recommended to take a backup of the external disk before proceeding to any upgrade process.

(i) **NOTE:** For customers on any Analytics version older than Analytics 2.5.4, please contact support for upgrade. To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

The following table summarizes the various ways to upgrade to Analytics 2.5.7:

Current Analytics Version	Upgrade Procedure
Analytics 2.5.6, 2.5.5, 2.5.4 with data in external disk.	Follow the steps under Upgrading Analytics with data in external disk
Analytics 2.5.6, 2.5.5, 2.5.4 with data in internal disk.	Follow the steps under Upgrading Analytics with data in internal disk

To verify the data is present on the internal disk follow the below steps:

- 1. Launch the Management Console of Analytics.
- 2. Navigate to **Storage**. No additional storage text under **Additional storage status** confirms that no external disk is present.

-Menu	Storage	
System Info	Additional storage status	No additional storage
Storage	Additional storage action	[Add storage]
Network Interfaces		
Diagnostics		
NTP Server		
Reboot Shutdown		
About		
Logs		

Topics:

- Upgrading Analytics with data in external disk
- Upgrading Analytics with data in internal disk

Upgrading Analytics with data in external disk

To upgrade to Analytics 2.5.7, for customers with systems configured with the Analytics 2.5.6, or 2.5.5, or 2.5.4 and data present in external disk, the below steps summarizes the upgrade process:

- Unmount the hard disk from Analytics 2.5.6, or 2.5.5, or 2.5.4, refer Unmounting the Hard Disk from older Analytics Version.
- Mount it on Analytics 2.5.7, refer Mounting the Hard Disk on new Analytics.
- (i) **IMPORTANT:** When you mount a hard disk in Analytics you need to enter a Secret Key, which will be same as used in the previous version of Analytics and should be remembered before starting the upgrade procedure.

Upgrading Analytics with data in internal disk

To upgrade Analytics 2.5.6, or 2.5.5, or 2.5.4 with data present in internal disk to Analytics 2.5.7:

- 1. Prepare the Analytics to add external disk. Refer Preparing the Analytics to Add External Disk.
- 2. Add external disk. Refer Adding External Disk.
- 3. Migrate the data from internal to external disk. Refer Migrating the Data To External Disk.
- 4. Unmount the hard disk from older Analytics. Refer Unmounting the Hard Disk from older Analytics Version.
- 5. Mount it on the Analytics 2.5.7. Refer Mounting the Hard Disk on new Analytics.

Unmounting the Hard Disk from older Analytics Version

To unmount the hard disk from old Analytics version:

- 1. Login to the Analytics UI using the IPV4 address, username and password.
- 2. Navigate to System > Shutdown. Click Shutdown. On prompting for confirmation, click OK.



3. Once it is successfully powered off, select the Analytics instance, right-click and click Settings.

vm	vSphere Clien			10.194.56.132						
۵	0 9	Q		Actions - Ashish_flow_Analytics_2.5-65610.194.56.132 Power	, ytics_	_2.5-65610.194.56.132 🕨 🖷 😻 🧔	6	ACTIONS ~		
	Ashish2_Nsv2	200_10.194.56.69 low10_10.194.56.194		Guest OS	▶ jure	Permissions Datastores Networks				
	Ashish2_wind	low10_10.194.56.44		Snapshots	t OS: patibility:	Other 3.x Linux (64-bit) ESXI 5.0 and later (VM version 8)				
	ASHISH_53-10	0.194.53.14		Solution President Console	are Tools	Running, version:10282 (Guest Managed)				
	ashish_Cento	s710_10.194.56.106 base Analytics 2.5-36	5010.19	😤 Migrate	Name:	More info localhost				
	Ashish_flow_	Analytics_2.5-3320-10	.194.56.2	Clone	• dresses:	10.194.56.132				
	Ashish_flow_	Analytics_2.5-3320.10	.194.56.1	Fault Tolerance	•	View all 3 IP addresses 10.194.54.15				
	Ashish_flow_	Analytics_2.5-3563-10 Analytics_2.5-3709.10	.194.55.8 .194.55.x	VM Policies	•					
	Ashish_flow_	Analytics_2.5-65610	.194.56.13	Template	•					
	Ashish_FLOW	/_Analytics_c_2.5-727 /_GMS_9.3.9320.1289	.10.194.5 .10.194.5(Compatibility	•	^	1	Notes		
	Ashish_GMS_	9.3.9317.1273.		Export System Logs		4 CPU(s)		SonicWALL_Analytics_R656		
	Ashish_GMS_	9.3.9320.1296.250GB	10.194.5	😵 Edit Settings		8 GB, 4.72 GB memory active				
	Ashish GMS	FLOW_9.3.9320.1287	10.194.55	Move to folder	-	66.45.GB		Custom Attributes		
	Ashish_GMS_	syslog_9.3.9320.1287	.10.194.50	Pename				Attribute		Malue
	🗄 AShish_GMS_	TEST1_9.3.9320.1296	250GB.1	internet in the second s				201000		Toroe
	-		-	Edit Notes						
Recent	Tasks Alarm	1		Tags & Custom Attributes	•					
Task Nam	10 ×	Target			-	 Details 	~	Initiator v Queued For	Start T	me 4

4. Unmount the Hard disk 2 by clicking **X** button on right corner of **Hard disk 2** in ESXi interface.

(i) **NOTE:** Do not select the **Delete files from datastore** option as it will delete all the data on the disk.

vm vSphere Client Menu V Q 10.194.56.132			C @ v dmarlgowda@oxus.sonicwal.com v C
Image: Control (Control (Contro) (Control (Control (Contro) (Control (Control (Control (Contro) (Edit Settings Annue_two Vitual Hardware VM Options	ANYICIL 2-5456-10.194.56.12 Converting and	COULSARE 0 H2 0 H2 0 B 0 H2 0 H2 0 H2 0 H2 0 H2 0 H2 0 H2 0 H2
	Shares	Normal V 1000	Volue
Recent Tasks Alarms	Limit - IOPs	Unimited V	
Task Name v Target Intran guest OS B Annia, Sow, Analysis, 25.665–10194.56.92 Intelligent		CANCEL	V Sam Time J V Comparison Time V Same 10/11/2022,416:31 10/11/2022,416:31 10/11/2022,416:31 vetbr/67/avoid sontice. PM PM PM Vetbr/67/avoid sontice.

5. Click **OK** to complete the unmounting procedure.

Mounting the Hard Disk on new Analytics

To mount the hard disk on new Analytics version:

- 1. Install a fresh Analytics 2.5.7 VM using latest 2.5.7 VHD file and steps from Installing On-Premises Analytics on ESXi and configure the VM with same IPV4 address as the older Analytics version setup following the steps under Configuring On-Premises Analytics on ESXi.
 - (i) **NOTE:** There will be a downtime while unmounting older version Analytics and mounting new version Analytics.

Pienu Fletuork interfaces Storage Network interface [ens160] Network interfaces Diagnostics NTF Server Fletuork interfaces [10.194.56.195] Reboot I Shutdown Networks [255.255.0] About Network anderess 00:0e:29:9b:07:94 Logs Global DNS naneservers DNS 1 DNS 2 [10.194.31.51] DNS 2 [8.8.8.8]					
System Info Network Interface I ensite J Network Interfaces DHCP I Disabled J Diagnostics IP04 Address [10.194.56.195 J Netmask I 225.255.25.0 J About Nac address 00:00:23:50:07:94 Logs Gateway I 10.194.56.1 Bisginstructure J Sitter address 00:00:23:50:07:94 Jogs Gateway I 10.194.56.1 J Bisginstructure J I 10.194.31.51 J DNS 2 I 8.8.8.8 J	Plenu Tree	Network Interfaces			
Netuork Interfaces DHCP [bisabled] Plagnostics IPv4 Address [10.194.56.195] Network I Shutdown Netmask [255.255.255.0] About Nac address 00:0c:23:5b:07:94 Logs Gateway [10.194.56.1] BK 1 [10.194.31.51] DNS 2 [8.8.8.8]	System Info	Metwork Interface		ens160	
Network Intervaces Ditc I Disablea J Diagnostics IP04 Address [10.194.56.195] Reboot I Shutdown Nethaak [255.255.0] About Mac address 00:0c:29:9b:07:94 Logs Global DNS naneservers 00:0c:29:9b:07:94 Biognostics [10.194.56.1] Biognostics 00:0c:29:9b:07:94 Bott [10.194.56.1] Biognostics [10.194.31.51] DNS 2 [8.8.8.8]	Storage	DUCD		D411-4	
Inightsettes IPv4 Address [10.194.56.195] Reboot I Shutdown Netmask [255.255.255.0] About Hac address 60:0c:29:9b:07:94 Logs [10.194.56.1] Global DNS nameservers [10.194.31.51] DNS 2 [8.8.8.8]	network Interfaces	DHCL		Disablea	
Nil Server From Horses 1 10.191.36.135 J Reboot Station Netaask 255.255.0 J About Nac address 00.0c:23:5b:07:94 Logs Gateway [10.194.36.1] Bit S [10.194.31.51] DNS 1 [10.194.31.51] DNS 2 [8.8.8.8]	Diagnostics	TRud Allows		40 404 57 405	
netboot 1 subset 1 cost cost cost cost cost cost cost cost	nir Server	Iru4 Haaress		10.194.50.195	
Hourt Index address 00.00-02-23-30-07-34 Logs Gateway [10.194.36.1] Global DNS nameservers DNS 1 [10.194.31.51] DNS 2 [8.8.8.8]	Reboot I Shutdown	Manadanan	. Ч.	255.255.255.0	1. Contraction (1997)
Logs Gatebay 1 10.194.36.1 J Global DNS naneservers DNS 2 I 0.194.31.51 J DNS 2 I 0.88.8 J	HDOUT	nac address		00:0C:29:95:07:94	•
Global DNS nameservers DNS 1 [10.194.31.51] DNS 2 [8.8.8.8]	rogs	Gateway		10.194.56.1	
Global DNS haneservers DNS 1 [10.194.31.51] DNS 2 [8.8.8.8]					
DHS 2 E 8.8.8 J		GIODAI DAS nameservers		40 404 24 54	
				10.194.31.51	
		JHS Z		8.8.8.8	

- 2. Login to the Analytics UI using the IPV4 address, username and password.
- 3. Navigate to System > Shutdown. Click Shutdown. On prompting for confirmation, click OK.

SONICWALL'	SonicWall Analytics 2.5 Shutdown ₽ / Appliance	10.5.43.28 says Are you sure you wait to perform a Shuddown action on Bis applance?	※ Q 법					
System	SHUTDOWN							
— Status	Warning! This action will disconnect all users.							
 Licenses Time 	This action takes about 3 minutes. Remember that if you made any changes to the settings, you'll need to apply t	This action takes about 3 minutes. Remember that if you made any changes to the settings, you'll need to apply them before you restart or shutdown.						
- Administration			Restart					
- Settings								
- File Manager								
- Backup/Restore - Shutdown								

4. Right click on Analytics 2.5.7 instance and click Edit Settings.

vm	vSphere Client Menu V	0_10.194.56.132		
Ø	G 9 9	Actions - Ashish_flow_Analytics_2.5-65610.194.54 Power	^{6.132} , ytics_2.5-65610.194.56.132 ↓ • • • • •	
	Ashish2_Nsv200_10.194.56.69 Ashish2_windowiD_10.194.55.194 Ashish2_windowiD_10.194.56.194 Ashish2_windowiD_10.194.56.44 Ashish2_montorial Ashish2_montorial Ashish2_montorial Ashish2_montorial Ashish2_contorial Basish2_contorial Ashish2_montorial Basish2_contorial Ashish2_contorial Ashish3_contorial Ashish3_contorial <td>Guest OS Snapshots Topen Remote Console Gission Sector Console Gission Console</td> <td>Purre Permissions Datastores Networks Os: Other 3.x Linux (64-bit) abibility: ESXI 5.0 and later (VM version 8) are Tools: Running, version:10282 (Guest Managed) More info Name: locahost dresses: 01945.6.132</td> <td></td>	Guest OS Snapshots Topen Remote Console Gission Sector Console Gission Console	Purre Permissions Datastores Networks Os: Other 3.x Linux (64-bit) abibility: ESXI 5.0 and later (VM version 8) are Tools: Running, version:10282 (Guest Managed) More info Name: locahost dresses: 01945.6.132	
	Ashish_flow_Analytics_2.5-3320.10.194. Ashish_flow_Analytics_2.5-3563-10.194. Ashish_flow_Analytics_2.5-3709.10.194. Ashish_flow_Analytics_2.5-656-10.194.	56.17 Fault Tolerance 55.8 55.8 55.8 VM Policies 56.12 Template	View al 3 P addresses 10.194.54.15	
	 Ashish_FLOW_Analytics_c_2.5-727.10.1 Ashish_FLOW_GMS_9.3.9320.1289.10.19 Ashish_GMS_9.3.9317.1273. 	94.5 Kase Compatibility Export System Logs	• 4 CPU(s)	Notes SonicWALL_Ana
	Ashish_GMS_9.3.9320.1296.250GB.10.19	4.5 4.5 Difference Edit Settings	8 GB, 4.72 GB memory active	Edit Notes
	Ashish_GMS_FLOW_9.3.9320.1293.10.19 Ashish_GMS_syslog_9.3.9320.1287.10.19 Ashish_GMS_trest1_9.3.9320.1286.250	14.55 Move to folder 14.51 Rename 38.11 Edit Notor	66.45 GB	Custom Attribut
Recent	Tasks Alarms	Tags & Custom Attributes	•	

5. Click ADD NEW DEVICE button on the right corner and select Existing Hard Disk.

I ⊈ 6	b Edit Settings Ashish_fic	ow_Analytics_2.5-3709.10.194.55.xx	×	
vindow10_10.194.56.44 SL	Virtual Hardware VM Options			
3-10.194.53.14				
ntos710_10.194.56.106			ADD NEW DEVICE	
w-base_Analytics_2.5-365010.194.56.216_te w_Analytics_2.5-3320-10.194.56.236	> CPU	4 ~	CD/DVD Drive Host USB Device	
w_Analytics_2.5-3320.10.194.56.171	> Memory	8 GB	Hard Disk	
w_Analytics_2.5-3709.10.194.55.xx	> Hard disk 1	68.4140625 GB $^{\vee}$	Existing Hard Disk	
w_Analytics_2.5-65610.194.56.132 La .OW_Analytics_c_2.5-727.10.194.56.95	> SCSI controller 0	LSI Logic Parallel	SCSI Controller	
OW_GMS_9.3.9320.1289.10.194.56.249	> Network adapter 1	VLAN256 \vee	USB Controller SATA Controller	
MS_9.3.9320.1296.250GB.10.194.55.231	> Network adapter 2	VLAN256 V	NVMe Controller Shared PCI Device	R/soniccore/a
MS_FLOW_9.3.9320.1287.101.94.55.247 MS_FLOW_9.3.9320.1293.10.194.55.251	> CD/DVD drive 1	Client Device ~	PCI Device Serial Port	
MS_syslog_9.3.9320.1287.10.194.56.246 MS_TEST1_9.3.9320.1296.250GB.10.194.55.232	> Video card	Specify custom settings \vee		
MS_TEST3_9.3.9320.1296.40GB.10.194.55.234 MS_TEST4_9.3.9320.1296.40GB.10.194.55.235	VMCI device	Device on the virtual machine PCI bus virtual machine communication interfa	that provides support for the	

- 6. Navigate to the older Analytics VM in the Datastores section. Click OK.
 - (i) **NOTE:** VMDK files will be named based on the VM name and hard disk with reporting data will be usually named with extension _1.vmdk.

tual Hardware VM Options		
elect File		ADD NEW DEVICE
Datastores	Contents	Information
 Ashish_sysiog_Analytics_2.5.0.4_C Ashish_test2_Analytics_2.5.0.4_C Ashish_test2_Analytics_2.5.0.465 Ashish_test_Analytics_2.5.0.4374 Deepak-flow-Analytics_2.5.0.3-3320.1 Deepak-flow-test-Analytics_2.5-374 Deepak-flow-test-Analytics_2.5-37 Deepak-flow-test-Analytics_2.5-37 Deepak-syslog-test-Analytics_2.5-3320 Deepak-syslog-test-Analytics_2.5-3320 Deepak-syslog-test-Analytics_2.5-3320 Deepak-syslog-test-Analytics_2.5-3320 Deepak-syslog-test-Analytics_2.5-3320 Gepak-syslog-Analytics_2.5-3320 GMS8.7-10.194.xx.xx GMS8.7-10.194.53.(2-machine) GMS_Server_10.194.53.48 	 ▲ Deepak-flow-testAnalytics2.5- 3320.10.194.56.xxx.vmdk ▲ Deepak-flow-testAnalytics2.5- 3320.10.194.56.xxx_1.vmdk 	Name: Deepak-flow-test Analytics2.5- 3320.10.194.56.xxx_1.vmdk Size:110 GB Modified:10/28/2022, 6:37:29 PM Encrypted: No

- 7. Power on the Analytics 2.5.7 and mount the storage.
 - () **NOTE:** When you mount a new hard disk in Analytics you need to enter a secret key, which will be same as used in the previous version of Analytics and should be remembered before starting the upgrade procedure.

Menu- System Info Storage Network Interfaces Diagnostics NTP Server Reboot I Shutdown About Logs	-Storage Additional storage status Additional storage action	Found and not nounted Mount storage	
-Destro A reboo Ves No			

- 8. Login to the Analytics UI using the IPV4 address, username and password.
- 9. Navigate to **System > Status**. The page displays the details of the installed Analytics.

← → C ▲ Not secure	https://10.194.56.195/appliance/applianceMainPage	
SONIC	SonicWall Analytics 2.5 2 / Appliance GENERAL	
System	Name Serial Number	SonicWall Analytics 004010320AB2
— Status — Licenses	Version	2.5 (Wednesday October 26, 2022 01:32:26 PM PDT)
	Flow Agent Firmware Version	2.2-1252617
	License	Licensed for SonicWall Analytics
 — Settings — Diagnostics 	Role	SonicWall Analytics
	SYSTEM	
	l Host Name	analytics.sonicwall.com
	IPv4 Address	10.194.56.195
	Current Time	Oct 29, 2022 06:23:39 AM GMT
	Up Time	3 min
	Operating System	Linux (amd64-4.14.127-soniccore)
	CPU	Intel Xeon (2.10 GHz)
		4 Cores Cache: 22528 (4 Logical CPUs)
IPM	RAM	7984 MB
	Available Disk Space on Install Partition	45.00 GB (of Total 61.90 GB)
	Available Disk Space on Data Partition	105 GB

Upgrading Analytics using SWI file

To upgrade On-Premises Analytics using SWI file:

- 1. Login to the Analytics UI using the IPV4 address, username and password.
- 2. Navigate to the **System > Settings**.
- 3. Click Choose File and select the Analytics swi file.



4. Click Apply.

(i) NOTE: This process uploads and validates the SWI file and system reboots after that.

Migrating Data From Internal to External Disk

In absence of a secondary disk, Analytics data is stored in the primary hard disk which is inbuilt in the Analytics server. Data migration is required when Analytics server is configured without a secondary hard disk. This chapter describes how to migrate Analytics data from internal disk to external disk.

(i) **NOTE:** On successful migration of data from internal to external disk, the existing data in the internal disk will not get deleted but new data will get stored only in the external disk.

To transfer data from internal disk to external disk:

- 1. Preparing the Analytics to Add External Disk
- 2. Adding External Disk
- 3. Migrating the Data To External Disk

Preparing the Analytics to Add External Disk

To prepare the Analytics to add external data:

- 1. Navigate to the **System > Settings**.
 - NOTE: For migration preparation process, the Settings page will display a DATA MIGRATION section. If the DATA MIGRATION section displays an error that the DATA MIGRATION IS DISABLED, then expand the existing hard disk size to 2x times the current hard disk size available. Refer Expanding Existing Disk.
- 2. Click **Prepare** to start the process to allow the existing Analytics to support external disk addition. On prompting for confirmation click **OK**.

Migrating Data From Internal to External Disk

6

SONIC WALL '	SonicWall Analytics 2.5 Settings	10.5-43.28 says Migration preparation process will move all the existing data internally to apport addition of excondary hard dat. Please DD NOT REDOT or SHUTDION the analytic MM while mixed one evantation process. In enorges.	≫ 9 œ
5ystem	Support License for Upgrades is valid	Cancel	
— Status	FIRMWARE UPGRADE/SERVICE PACK/HOTFIX		
 Licenses T=- 	Upload the Firmware Upgrade/Service Pack/Hotfix file in order to update	the system.	
 Administration 	Current Version 2.5 () (Click here for history)	
- Settings	Uplead file Choose File		
 Diagnostics 			Apply
— File Manager			
 Backup/Restore 	DATA MIGRATION		
- Shutdown	Data migration is required when analytics server is configured without second	dary hard disk for storing analytics data. Please follow the instructions to move the data from primary disk to secondary disk	
🙏 Network	Prepare the system for migration by clicking Prepare button. This process will	organize the existing analytics data to support external disk addition.	Prepare

() **NOTE:** This process will take some time to complete. Refresh the page at regular intervals.

Adding External Disk

To add external disk:

1. Navigate to **System > Settings**. On successfully preparing the system to support external disk, the Settings page will display a message to add external disk.

SONICWALL	SonicWall Analytics 2.5	2 Q 🖻
K Analytics	Settings	
	🙅 / Appliance	
System	O Support License for Upgrades is valid	
- Status		
- Licenses	FIRMWARE OPGRADE/SERVICE PACKHOTHX	
- Time	Upload the Firmware Upgrade/Service Pack/Hotfix file in order to update the system.	
 Administration 	Current Version 2.5 (Click here for history)	
- Settings	Upland file Choose File	
 Diagnostics 		(Arrely
- File Manager		
- Backup/Restore	DATA MIGRATION	
- Shutdown	Data misration is remarked when analytics senar is configured without secondary hard fick for dovina analytics data. Please follow the instructions to move the data from originary disk to acrondary disk	
	And an external disk of size greater than 142.96 for tauth the migration process.	
👗 Network		
	Mon Jul 03 19:20:02 IST 2023 : Preparation process completed successfully.	
6 Device ment	Non Jul 03 19:20:02 IST 2023 : appLianceConf backup complete. Non Jul 03 19:20:13 T2023 : Starting service - mysold - true	
Cehrolyment	Non Jul 03 19:21:25 IST 2023 : Starting service vyscheduler - true Non Jul 03 19:22:27 IST 2023 : Starting service vyscheduler - true	
	Non Jul 03 19:22:49 IST 2023 : Starting service reported - true Non Jul 03 19:22:49 IST 2023 : Starting service sylon - true	
и рм	Please refresh the page once services are restarted.	

2. Navigate to System > Shutdown. Click Shutdown. On prompting for confirmation, click OK.



3. Bring up the vSphere Client, select the Analytics instance, right-click and click Edit Settings.

=	vSphere Client Q	Power Guest OS	>		@~
(])	Ø E Ø	Snapshots	>	-syslog1_Analytics_2.5-3320-10.194.55.185 D C C @ @ (8) ; Actions Monitor Configure Permissions Datastores Networks Snapshots	
	Gouri_Nsv870 Harsh-flow_Analytics_2	ଗୁୁ Migrate Clone	>	Guest OS: Other 3 x Linux (64-bit)	•
	Harsh-flow_Analytics_2 Harsh-GMS_8.7.8723.12	Fault Tolerance	>	Compatibility: ESXI 5.0 and later (VM version 8) O Hz	
	Harsh-syslog1_Analytics Harsh-syslog_Analytics	VM Policies	>	DNS Name: localhost OB	AGE
	Harsh-test-syslog_Analytics	Template Compatibility	>	CONSOLE HOSE: 10.194.54.27	SAGE GB
	 HArsh_Window-machin HarshArya 10.194.55.40 	Export System Logs			
~	Recent Tasks Alarms	@ Edit Settings		ne Notes	^
Task M	iame T Target	Move to folder Rename		s T Initiator T Queued T Start Time 4 T Completion Ti	ime
Powe	r Off virtual machine 🛛 🔀 Harsh-	Edit Notes		SV\dmarigowda 6 ms 07/07/2023.3.56.08 07/07/2023), 3.56:12

4. Click ADD NEW DEVICE and select Hard Disk.

		ADD NEW DEVICE
> CPU	4 ~	Disks. Drives and Storag
> Memory	8 🗸 GB 🗸	Hard Disk
> Hard disk 1	1.5 TB ~	Existing Mard Disk
> SCSI controller 0	LSI Logic Parallel	Host USB Device
> Network adapter 1	VLAN255 ~	CD/DVD Drive
> Network adapter 2	VLAN255 V	NVMe Controller
> CD/DVD drive 1	Client Device ~	SATA Controller
> Video card	Specify custom settings ~	USB Controller
VMCI device		Other Devices
> Other	Additional Hardware	PCI Device Serial Port
		Network

5. Enter the size of the New Hard disk, refer to IPFIX Based Licensing Model on recommendations in size and click **OK**.

					ADD NEW DEVIC
CPU	4 ~				C
Memory	8		~	GB v	
Hard disk 1	1.5	тв	~		
New Hard disk *	16	GB	~		
SCSI controller 0	LSI Logic Parallel				
Network adapter 1	VLAN255 ~				Connect
Network adapter 2	VLAN255 ~				Connect
CD/DVD drive 1	Client Device				
Video card	Specify custom s	ettings ~	·		
VMCI device					
Other	Additional Hardwa	ire			

- 6. Add and mount the storage. Follow **steps 1 to 6** under Configuring On-Premises Analytics on ESXi.
- 7. Login to the Analytics UI using the IPV4 address, username and password.
- 8. Navigate to **System > Status**. Verify that the added storage is displayed in **Available Disk Space on Data Partition**.

SONIC WALL	SonicWall Analytics 2.5	
🍓 Analytics	Status	
System		
— Status 🔶	Name	SonicWall Analytics
— Licenses	Serial Number	
 Time Administration 	Version	2.5
— Settings	Flow Agent Firmware Version	2.2-1252617
 Diagnostics 	Lisansa	Licensed for ConicMall Applicies
 File Manager 	License	Licensed for Sofictival Analytics
Backup/Restore Shutdown	Role	SonicWall Analytics
	SYSTEM	
📩 Network	Host Name	analytics.sonicwall.com
	IPv4 Address	_
Deployment	Current Time	Jul 04, 2023 04:23:49 PM GMT
*	Operating System	Linux (amd64-4.14.127-soniccore)
Flow Agent	CPU	Intel Xeon (2.10 GHz)
ирм		4 Cores Cache: 33792 (4 Logical CPUs)
	RAM	7984 MB
	Available Disk Space on Install Partition	44.20 GB (of Total 62.00 GB)
	Available Disk Space on Data Partition	492 GB
	GETTING STARTED	

Migrating the Data To External Disk

To migrate the data:

1. Navigate to the **System > Settings**. Verify a message is displayed indicating the system is ready for data migrate.

SONIC WALL	SonicWall Analytics 2.5	» 9 d
槸 Analytics	Settings	
5ystem	Support License for Upgrades is valid	
— Status	FIRMWARE UPGRADE/SERVICE PACK/HOTFIX	
- Licenses - Time	Upload the Firmware Upgrade/Service Pack/Hotfix file in order to update the system.	
- Administration	Current Version 2.5 (Click here for history)	
- Settings	Upload file Choose File	
- File Manager		(Apply)
- Backup/Restore	DATA MIGRATION	
- Shutdown	Data migration is required when analytics server is configured without secondary hard disk for storing analytics data. Please follow the instructions to move the data from primary disk to secondary disk	
A Network	System to ready for starting data migration momprimary data to secondary data.	Migrate
🥮 Deployment	Mp 20 (0) 1372-092 137 2023 : Preparation process completed successfully. Mp 20 (0) 1252-023 : TPU20 : application process completed successfully. Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 (0) 1252-023 : Distribution perfective - myraid - terr Mp 20 : Distribution perfective - myraid - terr Mp 20 : Distribution perfective - myraid - terr Mp 20 : Distribution perfective - myraid - terr Mp 20 : Distribution - terr Mp 20 : Distribution - terr	
В ; ри	Non Jul 83 19-22-44 IST 2023 : Starling service - report® - True Mon Jul 83 19-22-44 IST 2023 : Starling service - report® - True Please refresh the page once services are restarted.	

2. Click Migrate.

SONIC WALL	SonicWall Analytics 2.5	2 Q 🖻
🍬 Analytics	Settings	
5ystem	Support License for Upgrades is valid	
— Status — Licenses	RRMWARE UPGRADE/RERVICE PACKHOTFIX	
Time Administration	opendu err i mer kogi ander som som konstruktivnen er som en andere err system. Carrent Version 25 (Citck have for history)	
Secongs Diagnostics File Manager		Apply
 Backup/Restore Shutdown 	DATA MIGRATION Data migration is required when analytics server is configured without secondary hard disk for storing analytics data. Please follow the instructions to move the data from primary disk to secondary disk	
	System is ready for starting data migration from primary disk to secondary disk.	Migrate
	Fins Jul 03 19:2042 15T 2021 : Proparation process completed successfully. Fins Jul 03 19:2042 15T 2021 : splitschoff bekkyn complete. Fins Jul 03 19:2041 15T 2021 : Starting write: - myside true Fins Jul 03 19:2042 15T 2021 : splitschoff bekkyn complete. Fins Jul 03 19:2042 15T 2021 : splitschoff bekkyn complete. Fins Jul 03 19:2042 15T 2021 : Starting write: - myside true Fins Jul 03 19:2042 15T 2021 : Starting write: - myside true Fins Jul 03 19:2042 15T 2021 : Starting write: - myside true Fins Jul 03 19:2042 15T 2021 : Starting write: - myside true Fins Jul 03 19:2042 15T 2021 : Starting write: - myside true	
	No Julo 319:22:49 IST 2021 I Starting arrier. reporte - true Mo Julo 319:31:41 I ST 2021 I Starting service - replace true Please refresh the page once services are restarted.	

(i) **NOTE:** This process will take some time to complete.

3. On successful completion of the data migration, a message indicating data migration is successful will be displayed.

SONIC WALL	SonicWall Analytics 2.5	2 Q 🖻
🍕 Analytics	Settings	
	O Support License for Upgrades is wild	
Status Ucenses Time Administration	FIRMWARE UPGRADE/SERVICE PACK/HOTFIX Updad the Firmeare Upgrade/Service Pack/Hotfis file in order to update the system. Commer Version 2.5 [Clock terms for Pack/Hotfis] [Clock terms for Pack/Hotfis]	
Settings Diagnostics File Manager Backup/Restore		(Apply)
- Shutdown	Date improvements in required when unalytics same is configured without association, build dials for atoring unalytics data. Please follow the instructions to more the data from primary diak to associately diak. Data migration is successful. Please unmount the diak and mount it on measure and analytics. Regiment of the second s	
	No. 3.0 197 33:30 157 32:00 154 32:00 No. 3.0 197 33:00 197 32:00 154 400 No. 3.0 197 33:00 197 32:00 197 32:00 No. 3.0 197 33:00 197 32:00 197 32:00 No. 3.0 197 34:00 154 400 197 400 No. 3.0 197 34:07 157 32:00 154 410 No. 3.0 197 34:07 157 32:07 154 410 No. 3.0 197 34:07 157 32:07 154 410 No. 3.0 197 34:07 157 32:07 154 400 No. 3.0 197 34:07 154 400 154 400 No. 3.0 197 35:17 32:17 154 400 154 400 No. 3.0 197 35:17 154 400 154 400 No. 3.0 197 35:17 154 400 154 400	
	nom Jul ub 1913/100 151 2023 i Startung service - Systog - tive Plesse refresh the page once services are restarted.	

Using the Management Console

Z

Topics:

- Connecting to the Console
- Management Console Operations
- Using SafeMode on the Management Console

Connecting to the Console

To connect to the Management Console through ESXi virtual machine:

1. Navigate to the ESXi virtual machine monitor and choose Launch Web Console or Launch Remote Console.



2. The Management Console will appear.



Management Console Operations

The Management Console provides options for viewing and changing system and network settings, running diagnostics, rebooting the system, and other functions.

To access and navigate through the Management Console:

- 1. Bring up the Management Console. Refer to Connecting to the Console.
- 2. The main menu is displayed in the left side panel. Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.

System Info	GUID	CONTRACTOR AND A CONTRACTOR AND A CONTRACTOR
Storage		
Network Interfaces	System Time	: Thu 2019-02-21 23:20:48 UTC
Diagnostics	Up Time	: 0 seconds
NTP Server	Load Average	: 0.0 1min 0.0 5min 0.0 10min
Lockdown Mode		
Reboot Shutdown		
About		
Logs		
In / Down to select items		
TAR to move between views		
Futen to action adit an item		
Enter to action/cuit an item		

- 3. Press the Tab key to move the focus from left side menu to the main view (right pane), or vice versa.
- 4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.

-Test Ping	Management	Network-	E	Ping	1	

5. To select an option for editing or to choose the associated action, use the up/down arrow keys to move the focus to the editable/actionable items and press the Enter key.

An edit/selection dialog is displayed in the middle of the main view below the option list. Some dialogs have selectable actions and some are only for information.



Some dialogs are for input.



 Use the arrow keys as needed to move between selections in the dialog. To change a value, press Backspace to erase each character, then type in the new value. When ready, press Enter to commit the change or perform the selected action. You can dismiss the dialog by pressing Esc.

The On-Premises Analytics management menu choices are described in the following sections:

- System Info
- Storage
- Network Interfaces
- Diagnostics
- NTP Server
- Reboot | Shutdown
- About
- Logs

System Info



Some of the information in the System Info screen is dynamic. The following information is displayed:

- GUID Every On-Premises Analytics instance has a GUID which is displayed here.
- System Time This is the current system time on the On-Premises Analytics instance.
- Up Time This is the total time that the On-Premises Analytics instance has been running.
- Load Average This shows the average CPU load for the last 1 minute, 5 minutes, and 10 minutes. You can change the Average load time durations to view the CPU load over longer or shorter time periods.

Storage

rficm Susten Info Sitorayo Metwork Interfaces Diagwostics NTT Server Lockdown Mode Reboot I Skutdown About Logs	-Storage Additional storage Additional storage	Found and not encrypted Add storage	
Up / Down to select items TAB to more between views Enter to sction/edit on item			

The **Storage** screen enables configuration and encryption of secondary storage. For an example, see the first four steps in Configuring On-Premises Analytics on ESXi

Network Interfaces

Network Interfaces			
Network interface		ens160	
DHCP		Enabled	
IPu4 Address	10	.203.26.243	
Netmask	25	5.255.255.0	
Mac address	00:5	0:56:9f:8b:a	b
Gateway	1	0.203.26.1	
Global DNS nameservers			
DNS 1	I 173	.240.212.25	
DNS 2		8.8.4.4	
	Network Interfaces DHCP IPv4 Address Netnask Nac address Gateway Global DNS naneservers DNS 1 DNS 2	Network Interface [DHCP [IPv4 Address 10 Netnask 25 Hac address 60:5 Gateway 1 Global DNS naneservers 173 DNS 1 [173 173	Network Interface [ens160 DHCP [Enabled IPv4 Address 19,203,25,243 Netnask 255,255,255,0 Hac address 00:50:56:191:80:a0 Global DNS nameservers DNS 1 DNS 2 [8,8,4,4

In the **Network Interface** screen, you can configure these settings.

- Network Interface This is the current interface serving as the management interface.
- IPv4 Address This is the IPv4 address currently assigned to the management interface.
- Netmask This is the netmask currently assigned to the management interface.
- Mac Address This is the MAC address of the management interface.

- IPv6 address This is the IPv6 address currently assigned to the management interface.
- Gateway This is the default gateway currently in use by the On-Premises Analytics instance.
- **DNS** This is a list of the DNS servers currently being used by the On-Premises Analytics instance.

Diagnostics

Menu System Info Stanson	-Diagnostics- Ping No lookup	I.	Ping	1
Network Interfaces Diagnostics NTP Server Lockdown Mode Reboot Shutdown About	Send diagnostics to SonicWall support		Send	
Logs				
Up / Down to select items TAB to move between views Enter to action/edit an item				

The **Diagnostics** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the On-Premises Analytics instance. Another option is to **Send diagnostics to SonicWall support**.

To use Ping:

- 1. Select **Diagnostics** in the Menu and press Tab to move the focus into the Diagnostics screen.
- 2. Select Ping to highlight it and then press Enter to display the Enter IP address dialog.
- 3. Navigate into the dialog, press **Backspace** to clear the current value, and then type in the IP address that you want to ping.
- 4. Press Enter.

The ping output is displayed in the **Ping host** dialog.



5. Press the **Esc** key to close the dialog.

To use Nslookup:

- 1. Select **Diagnostics** in the Menu and press Tab to move the focus into the Diagnostics screen.
- 2. Select Nslookup to highlight it and press Enter to display the Enter hostname dialog.

- 3. Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.
- 4. Press Enter.

The Nslookup query results are displayed in an information dialog. You can scroll up and down within the dialog by using the up/down arrow keys.



5. Press the **Esc** key to close the dialog.

To send Diagnostic Report:

- 1. Select **Diagnostics** in the Menu and press Tab to move the focus into the Diagnostics screen.
- 2. Navigate to Send diagnostics to SonicWall support.
- 3. Select **Send** in the main view to highlight it, then press **Enter**. A dialog box showing the diagnostics send output is displayed. The last message indicates success or failure.

Henn Systen Info Storage Metwork Interfaces Diagnostics NTP Server Lockdown Mode Reboot I Shutdown About Logs	Diagnostics t Ping 1 Ping t Ping 1 Mslookup J Send diagnostics to SonicWall support (<u>Send</u>)	
	Send diagnostics Sending diagnostics to SonicWall support, please wait Contacting SonicWall support Sending information to SonicWall support Successfully sent information to SonicWall support	

4. Press the **Esc** key to close the dialog.

Any errors during the Send process are displayed in the Send diagnostics dialog box. Common reasons for the report failing to send include:

- Misconfigured/missing default gateway
- Misconfigured/missing DNS servers
- Inline proxy

() | NOTE: The Send Diagnostics tool does not currently work through HTTP proxies.

NTP Server

- Menu	NTP Server	
System Info	Sync with NTP server	[Perform sync]
Storage	Current time	Thu 2019-02-21 23:27:39 UTC
Network Interfaces	Network time enabled	No
Diagnostics	NTP sunchronized	Yes
NTP Server		
Lockdown Mode		
Reboot Shutdown		
About		
Logs		
Up / Down to select items		
TAB to move between views		
Enter to action/edit an item		

In the **NTP Server** screen, you can synchronize with an NTP server. For complete NTP Server configuration options, log into the SonicOS management interface and navigate to the **MANAGE | Appliance > System Time** page.

The NTP Server screen displays the following information:

- Sync with NTP server This button forces the On-Premises Analytics instance's NTP client to perform a sync with the configured NTP server(s).
- Current time The current time on the On-Premises Analytics instance.
- **Network time enabled** A Yes/No value determining whether the NTP client is currently configured to keep in sync with an NTP server.
- **NTP synchronized** A Yes/No value determining if the On-Premisese Analytics instance is currently synchronized with the configured NTP server(s).

Reboot | Shutdown



The **Reboot | Shutdown** screen provides functions for rebooting the instance, returning to factory defaults, and enabling SafeMode. To perform an action, position the focus on that menu and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

The actions available on the Reboot | Shutdown screen are:

- Reboot Analytics Restarts the instance with current configuration settings.
- Shutdown Analytics- Powers off the instance.
- **Boot Analytics into safemode** Puts the On-Premises Analytics instance into SafeMode. In this product, SafeMode does not offer additional functionality.

About

		4.5.4
System Info	Version	
Storage	Build name	6.5.0-286+Son1cCore-S665-S665-1.0.0-Da11y
Network Interfaces		
Diagnostics		
NTP Server		
Lockdown Mode		
Reboot Shutdown		
About		
Logs		
9-		

The About screen provides information about the software version and build.

Logs

r Menu	Feb 21 23:13:30 On-Prem_Analytics_623 MgmtCnsle: SVCGF: Interface successfully reloaded.
System Info	Feb 21 23:12:31 On-Prem Analytics_623 MgmtCnsle: ERROR: invalid CIDR address: 127.0.0.1/64
Storage	Feb 21 23:12:31 On-Prem Analytics 623 MgmtCnsle: ERROR: invalid CIDR address: 127.0.0.1/64
Network Interfaces	Feb 21 23:06:23 On-Prem_Analytics_623 Automatic secure crash analysis reporting is enabled
Diagnostics	Feb 21 23:06:23 On-Prem_Analytics_623 Automatic secure crash analysis reporting is enabled
NTP Server	Feb 21 23:06:23 On-Prem_Analytics_623 Periodic secure diagnostic reporting for support purpose
Lockdown Mode	Feb 21 23:06:23 On-Prem_Analytics_623 Initializing SonicWall support services
Reboot Shutdown	Feb 21 23:06:21 On-Prem_Analytics_623 MgmtCnsle: Management console has started
About	Reboot
Logs	Feb 21 23:02:56 On-Prem_Analytics_623 Automatic secure crash analysis reporting is enabled
	Feb 21 23:02:56 On-Pren_Analytics_623 Periodic secure diagnostic reporting for support purpose
	Feb 21 23:02:56 On-Prem_Analytics_623 Initializing SonicWall support services
	Feb 21 23:02:54 localhost MgmtCnsle: Management console has started

The Logs screen displays log events for the instance.

Using SafeMode on the Management Console

(i) | IMPORTANT: Please contact SonicWall Technical Support for assistance in the following operations.

The On-Premises Analytics instance can be configured to boot into SafeMode by using the Reboot | Shutdown screen in the management console.

In SafeMode, some of the features the management console provides are different in the following ways:

- Configurable interfaces
- Configurable default gateway

- Configurable DNS servers
- Download system logs
- Apply re-upgrade or hotfix

(i) | NOTE: Changes made to interfaces in SafeMode are not persistent between reboots.

The SafeMode Management Console always starts with the System Info screen.

-Safenode neuu- Systen Info Storage Hetwork Interfaces Diagnostics NTP Server Reboot Shutdown About Logs	System Info GUID System Time Up Time Load Average	: Thu 2019-03-21 17:55:07 UTC : 0 seconds : 0.0 1min 0.0 5min 0.0 10min
Up / Down to select items IAB to nove between views Enter to action/edit an item		

(i) | NOTE: To exit SafeMode, disable it on the Reboot | Shutdown screen. See for more information.

Topics:

- Enabling SafeMode
- Disabling SafeMode
- Configuring the Network Interfaces in SafeMode
- Installing a Software Upgrade in SafeMode
- Downloading Logs in SafeMode

Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

- 1. Access the On-Premises Analytics Management Console. Refer to Connecting to the Console.
- 2. In the console, select the **Reboot | Shutdown** option and then press Enter.
- 3. Navigate down to the Boot Analytics into safemode option to highlight Enable, and then press Enter.

Henu- Systen Info Storage Network Interfaces Diagnostics NTP Server Lockdown Mode Reboot I Shutdown About Logs	Reboot i Shutdoum Reboot Analytics I Reboot J Shutdoum Boot Analytics into safemode Example Boot Analytics into safe mode Resonant Shutdour No Confirm (Enter) Cancel (Esc)
Up / Down to select items TAB to nove between views Enter to action/edit an item	

- 4. Select Yes in the confirmation dialog.
- 5. Press Enter.

The On-Premises Analytics instance immediately reboots and comes back up in SafeMode.

(i) **NOTE:** In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

Disabling SafeMode

To disable SafeMode:

- 1. In the **SafeMode** menu in the Management Console, select the **Reboot | Shutdown** option and press **Enter**.
- 2. In the **Reboot | Shutdown** screen, navigate down to the **Boot Analytics into safemode** option to highlight Disable, and then press **Enter**.

	-Reboot Shutdown			
System Info	Reboot GMS into safemode	E Be	eboot	1
Storage	Shutdown GMS	L Sh	utdown	1
Network Interfaces	Boot GMS into safemode	[Dis	sable	1
Diagnostics				
NTP Server				
Reboot Shutdown				
About				
Logs				

- 3. Select **Yes** in the confirmation dialog.
- 4. Press **Enter**. The On-Premises Analytics instance immediately reboots and boots up in normal mode.

Configuring the Network Interfaces in SafeMode

When the Management Console is in SafeMode, the Network Interfaces screen in the On-Premises Analytics Management Console provides features to configure the On_Premises Analytics interfaces:

- **Network Interface** This is the currently selected interface. Use this to select any of the On-Premises Analytics interfaces.
- **DHCP** Determines whether addressing is static or handled automatically and dynamically by a DHCP server.
- IPv4 Address The current IPv4 address currently assigned to the Management Interface.
- Netmask The current Netmask assigned to the Management Interface.
- Mac Address The MAC address of the Management Interface.
- IPv6 Address The currently assigned IPv6 address of the Management Interface.
- Gateway The current Default Gateway currently in use by the On-Premises Analytics instance.
- DNS A list of the current DNS servers currently being used by the On-Premises Analytics instance.

(i) | NOTE: Changes made to interfaces in SafeMode are not persistent between reboots.

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

In SafeMode, the Network Interfaces screen includes editable and actionable items which are read-only when the management console is in normal mode.

- Menu	-Network Interfaces			
System Info	Network interface	eth0		
Storage				
Network Interfaces	DHCP	Disabled		
Diagnostics				
NTP Server	IPu4 Address	10.5.40.22		
Reboot Shutdown	Netmask	255.255.240.0		
About	Mac address	00:15:5d:20:08:23		
Logs	Gateway	10.5.32.1		
	Global DNS nameservers			
	DNS 1	8.8.8.8		
	DNS 2	8.8.4.4		

To edit an interface:

- In the SafeMode Network Interfaces screen, select the Network interface option and then press Enter. The Select Interface list appears, displaying all of the interfaces available on the On-Premises Analytics instance.
- Select the interface you wish to edit and press Enter.
 The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.
- To edit the IPv4 address, select IPv4 Address on the screen and press Enter. The on-screen dialog displays the current IP address.
- 4. Navigate into the dialog and make the desired changes, then press **Enter** to close the dialog or press **Esc** to cancel and close the dialog.
- 5. Two new buttons appear on the screen after you make changes to an interface setting: **Save changes** and **Cancel**. You can use the **Tab** key to navigate to these buttons.

Menu	-Network Interfaces-		
Sustem Info	Network interface	eth0 1	
Storage			
Network Interfaces	DHCP	Disabled 1	
Diagnostics			
NTP Server	IPu4 Address	0000 1	
Reboot Shutdown	Netmask	255 255 240 0 1	
About	Nac addwees	00:15:54:20:08:26	
Lorro	Category	10 5 27 1	
rogs	dateway	10.3.32.1	
	Clubel DNO encourses		
	GIODAI DHƏ HAMESCRUCTS		
	DIG 1	0.0.0	
	UNS Z	8.8.4.4	
	Save changes		Cancel
	and the second		and the second
In / Down to select items			
TAR to move between views			
Pater to action edit an item			
Lineer to action curt an rich			

() **NOTE:** You cannot navigate to the left navigation pane until you either save changes or cancel using these buttons. Changes made to interfaces in SafeMode are **not** persistent between reboots.

Do one of the following:

- To make changes to other settings for this interface, navigate to the desired setting, press **Enter**, make the changes in the dialog, then press **Enter** to close the dialog for that setting. Repeat for other settings, as needed.
- If finished making changes to the settings for this interface, press **Tab** to navigate to the **Save** changes button and then press **Enter** to save your changes.
- Press **Tab** to navigate to the **Cancel** button and then press **Enter** to cancel all changes to the settings for this interface.

Disabling an Interface

You can disable an interface while in SafeMode.

To disable an interface:

- 1. In the SafeMode Network Interfaces screen, select the Network interface option.
- 2. Select the interface you wish to edit and press Enter.

The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

For example, select **IPv4 Address** and press **Enter**.

The on-screen dialog displays the current IP address.

3. Navigate into the dialog and change the IP address to **0.0.0.0**, then press **Enter**.

r Menu	-Network Interfaces		
System Info	Network interface	eth0	
Storage Network Interfaces Diagnostics	DHCP	Disabled	
NTP Server	IPu4 Address	10.5.43.28	
Reboot Shutdown	Netmask	255.255.240.0	
About	Mac address	00:15:5d:20:08:2	26
Logs	Gateway	10.5.32.1	
	Global DNS nameservers		
	DNS 1	8.8.8.8	
	DNS 2	8.8.4.4	
	-Enter IP address-		
	0.0.0.0		
	Confirm <enter></enter>		
	L		
Up / Down to select items			
TAB to move between views			
Enter to action/edit an item			

4. Press **Tab** to navigate to the **Save changes** button and then press **Enter**.

Memu	-Network Intenfaces		
Sucton Info	Network intenface	f oth0 1	
Stevere	HE COULD THE CELEGE	L CON	
Network Interferen	DUCD	f Dischlad 1	
network Interfaces	DRGP	I DISADICA I	
Diagnostics	and the second	and the second	
MTP Server	IP04 Address	1 0.0.0.0 1	
Reboot Shutdown	Netmask	[255.255.240.0]	
About	Mac address	00:15:5d:20:08:26	
Logs	Gateway	1 10.5.32.1 1	
	Global DNS nameservers		
	DNS 1	T 8888 1	
	DNC 2	1 9944 1	
	DIN Z		
			and the second se
	Saue changes		Cancel
	oave changes		Gancer
Up / Down to select items			
TAB to move between views			
Enter to action/edit an item			

(i) **NOTE:** Disabling DHCP may be sufficient to disable the interface.

-Menu-	Network Interfaces			
System Info	Network interface		eth0	
Storage				
Network Interfaces	DHCP		Disabled	
Diagnostics				
NTP Server	IPo4 Address		10.0.0.1	
Reboot Shutdown	Netnask		255.255.240.0	
About	Mac address	1	00:15:5d:20:08:2	26
Logs	Gateway			
	Global DNS nameservers			
	DNS 1		8.8.8.8	
	DNS 2		8.8.4.4	

Installing a Software Upgrade in SafeMode

SWI files are used to upgrade On-Premises Analytics. You can download the latest SWI image file from MySonicWall.

In SafeMode, you can upload a new SWI image and apply it to the On-Premises Analytics instance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the Management Console. When viewing the Management Console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

(i) NOTE: In SafeMode, the web management interface is only available via http (not https).

To install a new system image from SafeMode:

1. With the On-Premises Analytics instance in SafeMode, view the management console. At the bottom of the screen, the URL for the SafeMode web management interface is displayed.

2. In a browser, navigate to the URL provided at the bottom of the Management Console screen. The SafeMode web management interface displays.

Appliance is running in Safe Mode	10				
Sate Mode will allow you to do any of th	e following				
Download the Safe Mode Logs for	ar troubleshooting by the SonicWall Suppor	Team			
> Upload new application images					
> Boot your choice of application in	nage				
Restore the settings to their factory defa	sult values				
Restore the settings to their factory defa	uut values				
Download Safe Mode Logs mage Management estart @ Refresh Upload	I mage	Last Marin Pala	Datus	Best	Tanan keline

- 3. Click the **Upload Image** button to select an SWI file and then click **Upload** to upload the image to the appliance. A progress bar provides feedback on the file upload progress. Once the upload completes, the image is available in the **Image Management** list in the SafeMode web interface.
- 4. In the row with the uploaded image file, click the **Boot** button and select one of the following:
 - Boot Uploaded Image with Current Configuration
 - Boot Uploaded Image with Factory Default Configuration

nage Management					
Kerresh 🐨 Upload I	mage				
Current Image Version 6.5.0.2-8v-sonicosv-37–f207f34d	Import Date 4/12/2018, 4:28:26 PM	Last Used Date 4/12/2018, 4:28:45 PM	Status Not Running: Safe Mode	Boot	Image Actions
Uploaded Image Version 6.5.0.2-8v-sonicosv-37-f207f34d	Load Date 4/12/2018, 4:49:31 PM	Build Date 4/12/2018, 3:39:33 AM		Boot () v	Image Actions
			Boot Uploaded Image (6.5.0.2-8v-s with Current Configuration Boot Uploaded Image (6.5.0.2-8v-s with Factory Default Configuration	onicosv-37f207f34d) onicosv-37f207f34d)	

The On-Premises Analytics Instance reboots with the new image.

Downloading Logs in SafeMode

When the On-Premises Analytics instance is in SafeMode, extra logging information is kept that can be downloaded. The logs are available from the SafeMode web management interface, which can be accessed via the URL provided at the bottom of the Management Console screen.

(i) | NOTE: In SafeMode, the web management interface is only available via http (not https).

To download logs from SafeMode:

1. With the On-Premises Analytics instance in SafeMode, view the On-Premises Analytics management console. At the bottom of the screen, the URL for the SafeMode page in the web UI is displayed.

2. In a browser, navigate to the URL provided at the bottom of the Management Console screen. The SafeMode web management interface displays.

Appliance is running in Safe Mode					
Safe Mode will allow you to do any of the	e following:				
> Download the Safe Mode Logs for	r troubleshooting by the SonicWall Suppor	t Team			
> Upload new application images					
> Boot your choice of application im	lage				
Restore the settings to their factory defa	ult values				
Restore the settings to their factory defa Download Safe Mode Logs Image Management	ult values				
Restore the settings to their factory defa Download Safe Mode Logs Image Management Restart Restart Upload	Image				
Restore the settings to their factory defa Download Safe Mode Logs Image Management Restart @ Refresh ① Upload Current Image Version ✓	Image Import Date	Last Used Date	Status	Boot	Image Actions

3. Click the **Download Safe Mode Logs** button. A compressed file is downloaded which contains a number of files, including a **console_logs** file that contains detailed logging information.

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

On-Premises Analytics for ESXi Updated - August 2024 232-005167-00 Rev H

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.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request Attn: Jennifer Anderson 1033 McCarthy Blvd Milpitas, CA 95035