On-Premises Analytics Deployment Guide

for Azure

SONICWALL®

Contents

About this Guide **4**
Guide Conventions 5

System Requirements **6**
Supported Firewalls 6
Additional Firewall Requirements 7
Supported Platforms 7
Minimum Requirements 7
IPFIX Based Licensing Model 8
IPFIX Based Capacity Planning 8
IPFIX-based VM Sizing 10
Syslog-based VM Sizing 10
Backup and Recovery Information 10
Importing Firewall Configurations 11
Creating a MySonicWall Account 11

Installing On-Premises Analytics on Azure **13**
Installing On-Premises Analytics on Azure 13
Configuring On-Premises Analytics on Azure 18
Adding Firewalls to On-Premises Analytics 30

Licensing and Registering Your On-Premises Analytics Instance **36**
Registering the On-Premises Analytics Instance 36
Activating Firewall Licensing for Syslog-Based On-Premises Analytics 40
Deregistering Your On-Premises Analytics Instance 43

Upgrading On-Premises Analytics **44**
Upgrading Analytics 2.5.5 44
- Upgrading Analytics with data in external disk 45
- Upgrading Analytics with data in internal disk 45
- Unmounting the Hard Disk from older Analytics Version 46
- Mounting the Hard Disk on new Analytics 47

Upgrading Analytics using SWI file 50

Migrating Data From Internal to External Disk **52**
Preparing the Analytics to Add External Disk 52
Adding External Disk 53

Migrating the Data To External Disk 55

Using the Management Console **57**
Connecting to the Console 57
Management Console Operations 59
- System Info 60
- Storage 61
- Network Interfaces 61
- Diagnostics 62
- NTP Server 64
- Reboot | Shutdown 64
- About 65
- Logs 65

Using SafeMode on the Management Console 65
- Enabling SafeMode 66
- Disabling SafeMode 67
- Configuring the Network Interfaces in SafeMode 67
- Installing a Software Upgrade in SafeMode 71
- Downloading Logs in SafeMode 72

SonicWall Support **74**
About This Document 75

1

About this Guide

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

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 Azure, details how to install on Azure

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 Azure.

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:

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

ⓘ | **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.**

⚠ | **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>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=***<your serial number>*, 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.

2

System Requirements

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

Topics:

- Supported Firewalls
- Additional Firewall Requirements
- Supported Platforms
- 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 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.

ⓘ **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 Azure Versions
SonicWall_On-Prem_Analytics_2.5	Azure Standard_D2_v2 or higher

ⓘ **NOTE:** The image files for installation are available on MySonicWall.

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.

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

The following table summarizes currently available licensing levels.

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

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.

VM Hardware Configuration	TZs / SOHOs / NSv low capacity (number 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	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 / 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
64 Core, 64 GB	12

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

Number of Firewalls	Recommended 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.

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

IPFIX-based VM Sizing

The following table describes the size of the VM based on the license levels:

VM Size in Azure	License Level
Standard_D2_v2	5 GB/day
Standard_D3_v2	15 GB/day
Standard_D4_v2	30 GB/day
Standard_D5_v2	100 GB/day

Syslog-based VM Sizing

The following table describes the size of the VM based on the syslog volume:

VM Size in Azure	Syslog Volume
Standard_D2_v2	100 million log entries/day
Standard_D3_v2	225 million log entries/day
Standard_D4_v2	360 million log entries/day
Standard_D5_v2	500 million log entries/day

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.

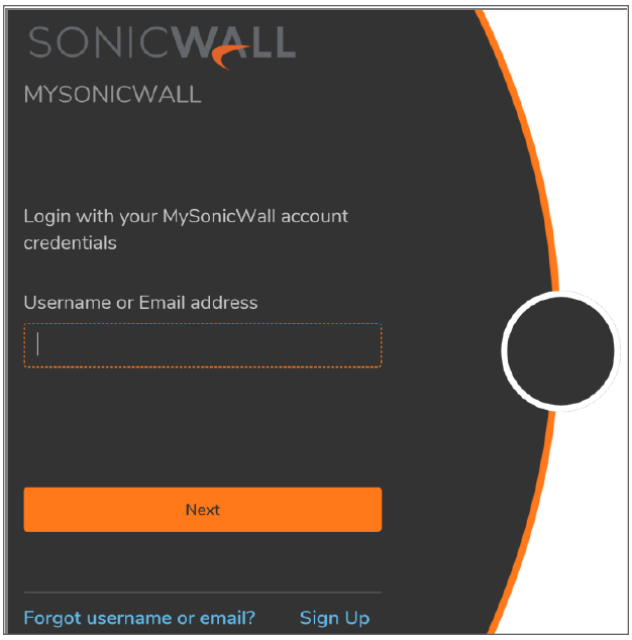
Creating a MySonicWall Account

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.

ⓘ | **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.



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.

3

Installing On-Premises Analytics on Azure

Topics:

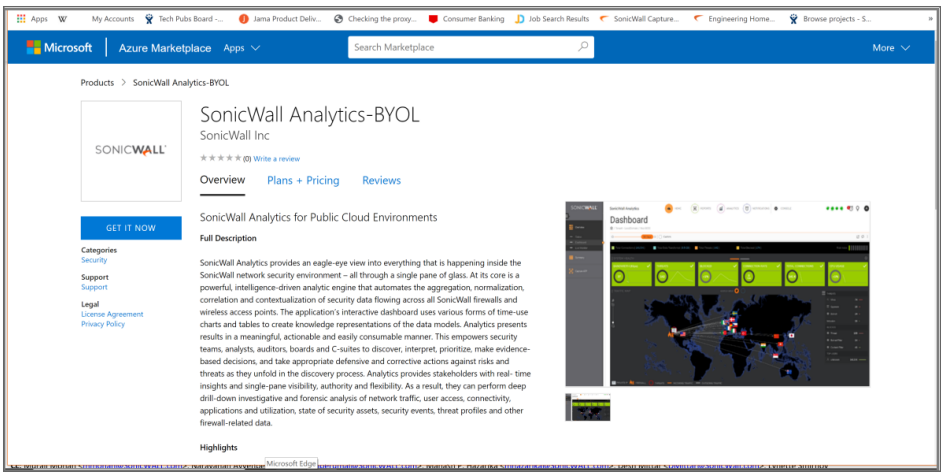
- Installing On-Premises Analytics on Azure
- Configuring On-Premises Analytics on Azure
- Adding Firewalls to On-Premises Analytics

Installing On-Premises Analytics on Azure

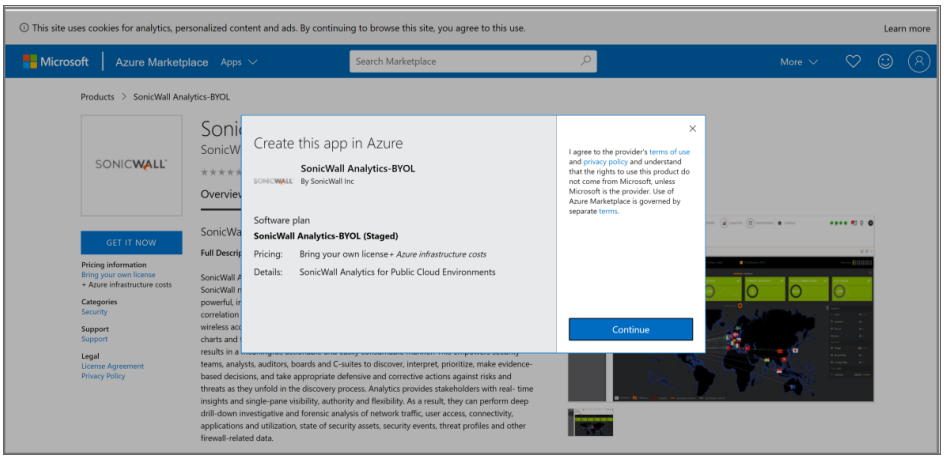
NOTE: The installation procedure provided here leaves Azure VM settings in default positions as much as possible while ensuring the Analytics VM will work. Depending on your use pattern for Azure, you may choose to change these settings during this installation process or later.

To install On-Premises Analytics on Azure:

1. Login into Azure Marketplace. Navigate to **Products > SonicWall Analytics**.

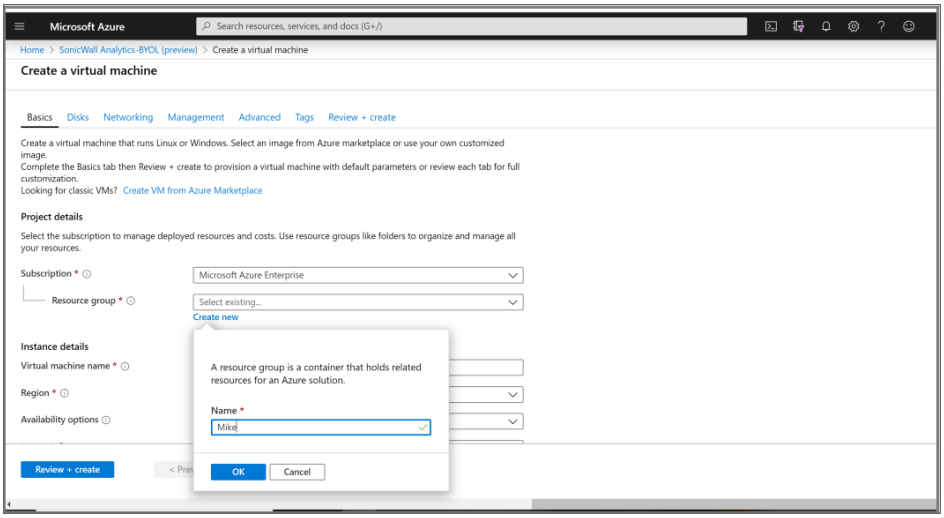


2. Choose to create this application in Azure and agree with the End User license agreement.



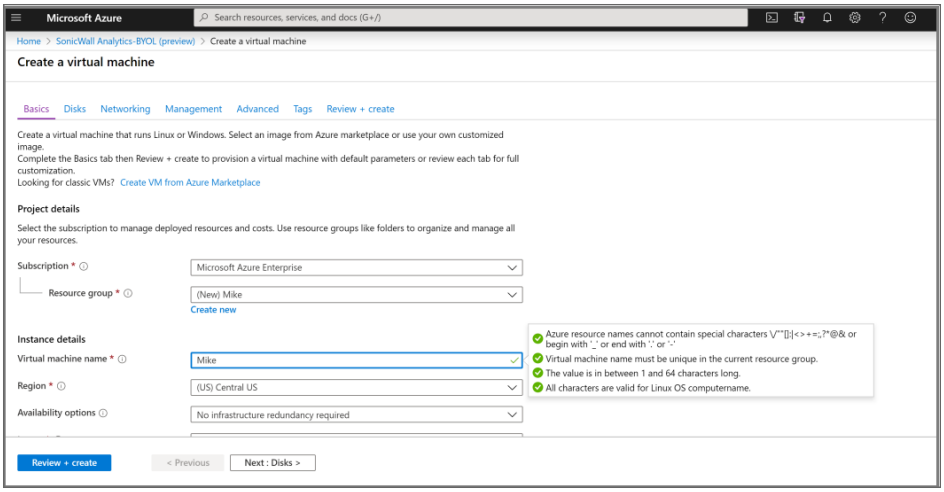
3. In the **Basics** page,

   - Click **Create new** for **Subscription > Resource group**, enter the **Name** of the Resource group, and click **Ok**.

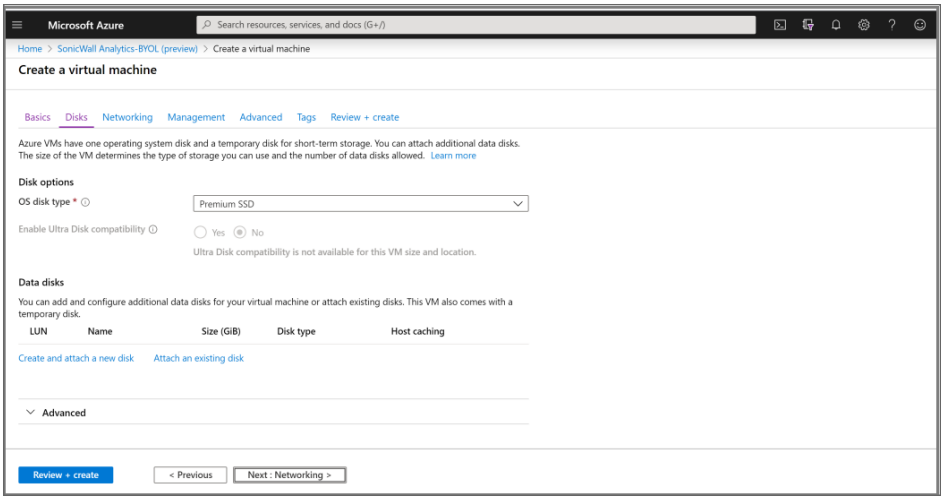


   - Enter a **Virtual machine name**.
   - Select a region, an image, and size of the VM. Refer IPFIX-based VM Sizing and Syslog-based VM Sizing for size of the VM.

- Enter the username as **management** and password for the VM.

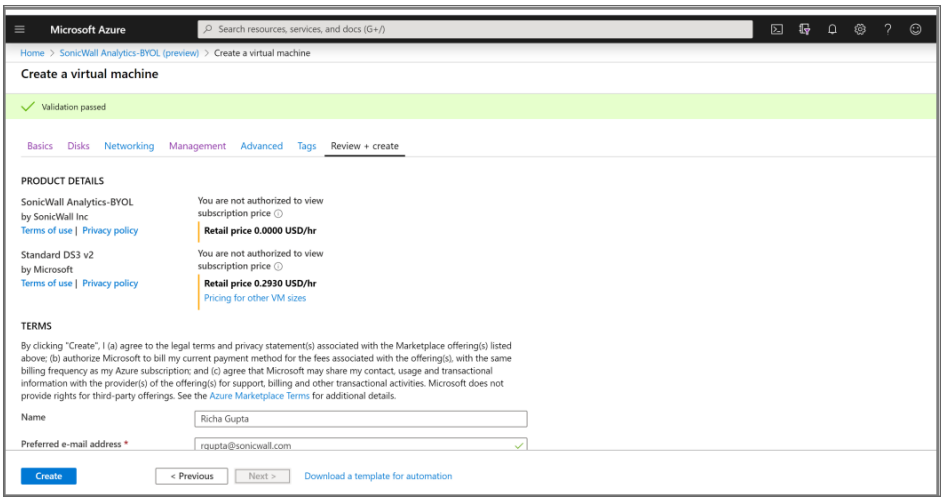


4. Click **Next:Disk**.
5. In the Disk page, Setup the amount of persistent memory to allocate to the VM. Refer to IPFIX Based Licensing Model for guidance on the amount of memory required.



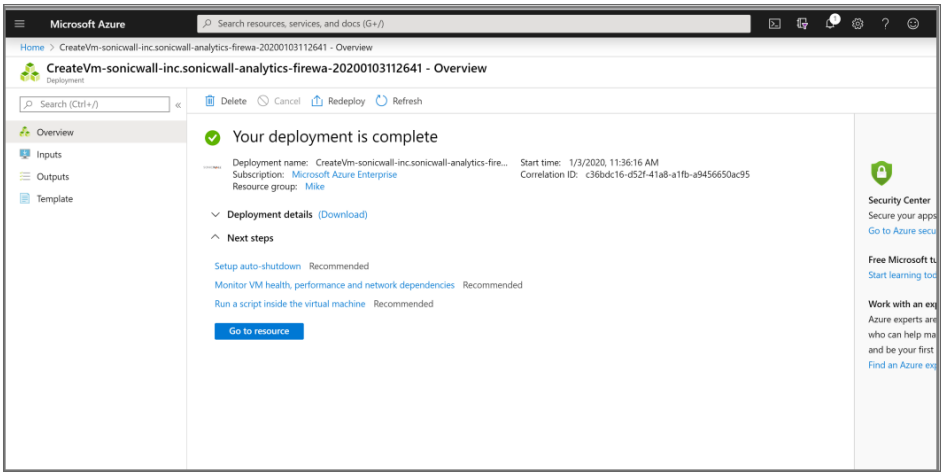
6. Click **Next:Networking**. Review the default settings and update as per your requirement or proceed with the default settings.
7. Click **Next:Management**. Review the default settings and update as per your requirement or proceed with the default settings.
8. Click **Next:Advanced**. Review the default settings and update as per your requirement or proceed with the default settings.
9. Click **Next:Tags**. Review the default settings and update as per your requirement or proceed with the default settings.

10. Click **Next:Review + create**. In this page the system will check that the VM configuration is valid before allowing deployment to the cloud. The system displays **Validation passed** for valid configuration.

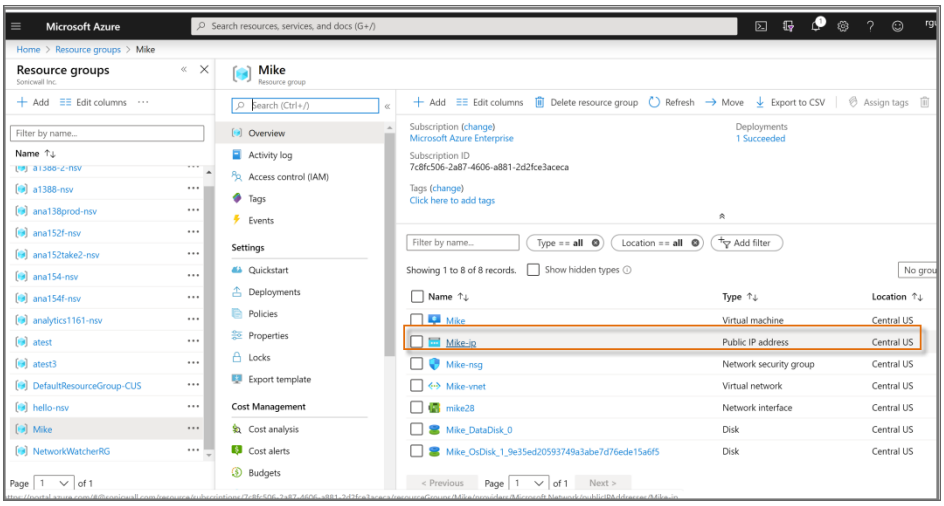


ⓘ | **NOTE:** VM deployment will take several minutes.

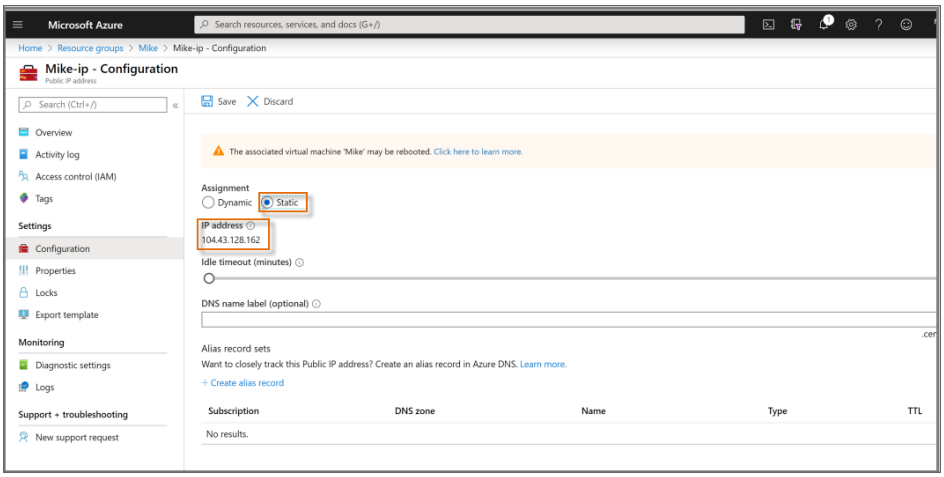
11. Azure indicates once the deployment is successfully completed.



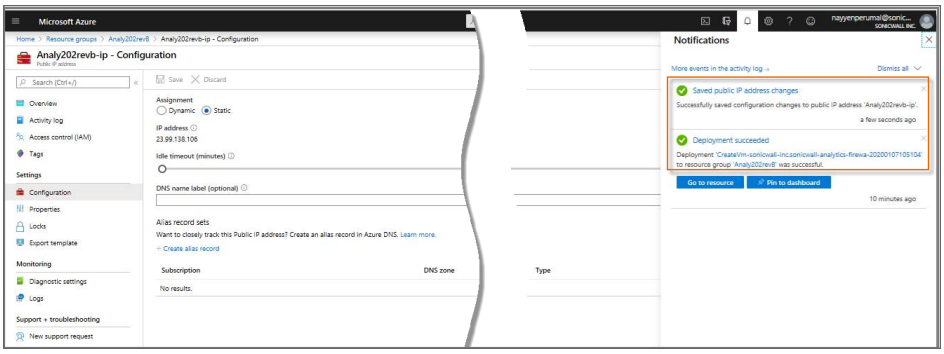
12. Navigate to **Home > Resource Groups >** created resource group and select the .ip file.



13. Double-click on the .ip file to know the assigned IP address for the VM. Record the IP address.
14. Navigate to **Settings > Configuration**.
15. Set **Assignment** to **Static**.



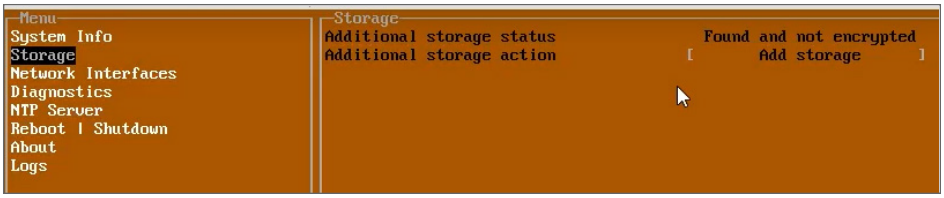
16. Click **Save**.
17. Click the notifications icon on the top right corner. **Saved public IP address changes** and **Deployment succeeded** notifications will be displayed.



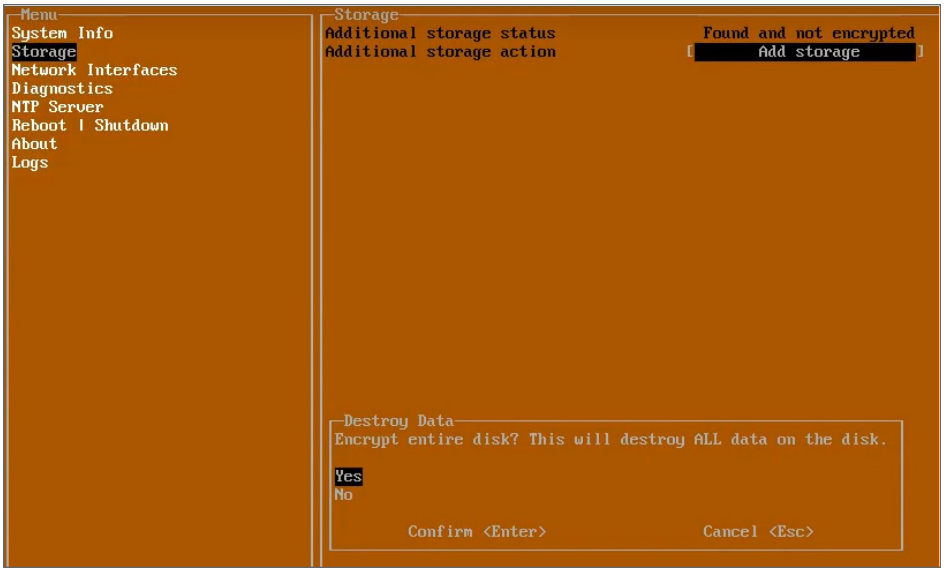
Configuring On-Premises Analytics on Azure

To configure On-Premises Analytics on Azure:

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



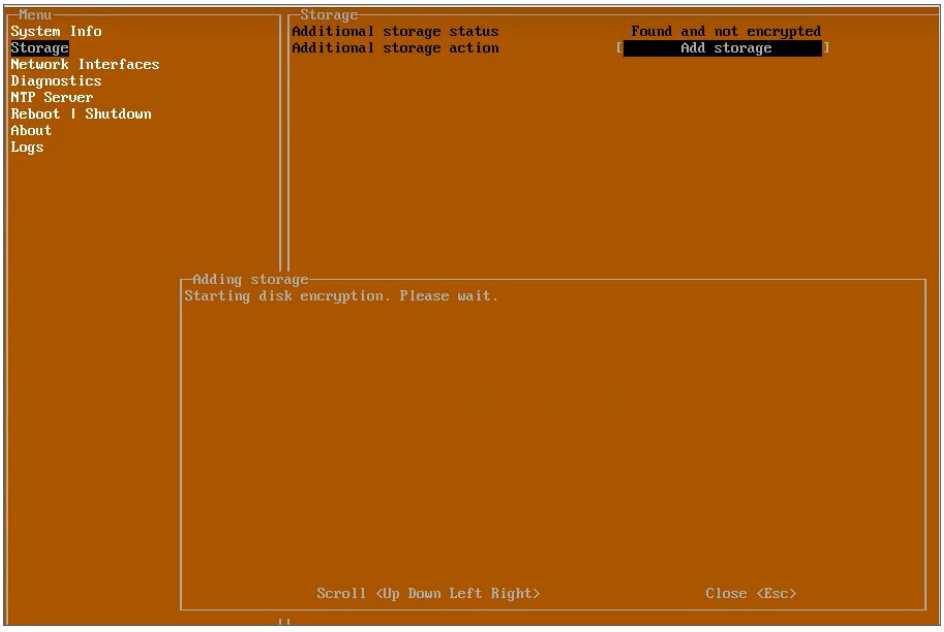
3. Select **Add Storage**, select **Yes** and press enter to confirm.



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.

ⓘ **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.

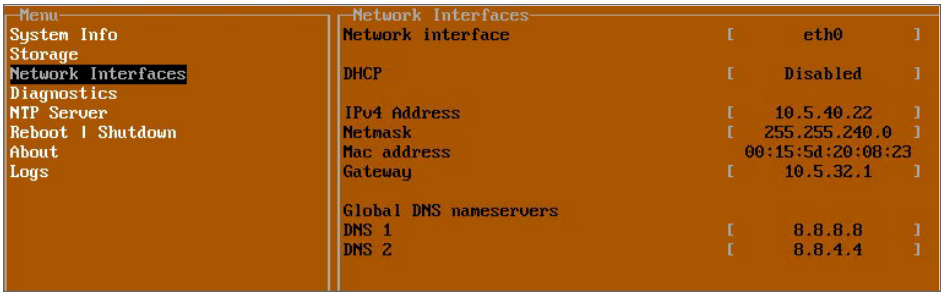


6. Click enter to reboot. You will have to enter the encryption key.

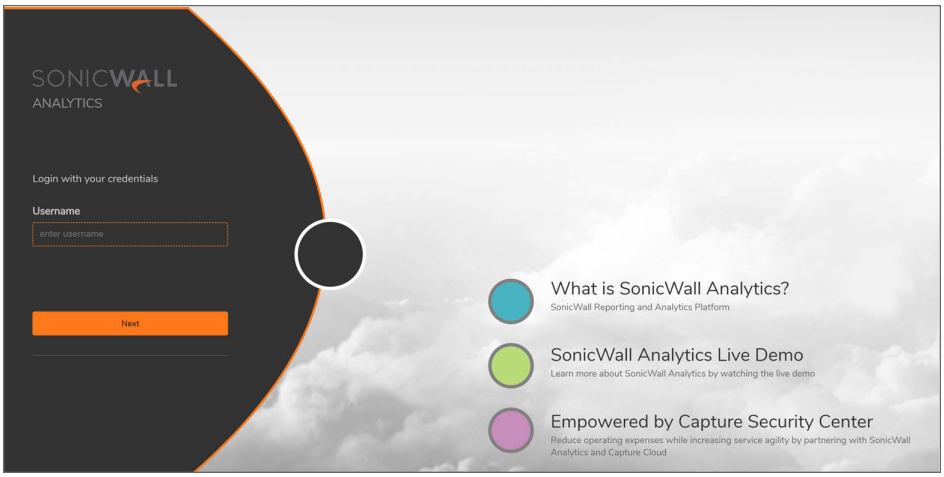
7. Navigate to the Network Interface setting, press Enter and select eth0. The system will use DHCP, if available, to assign an IP address.

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

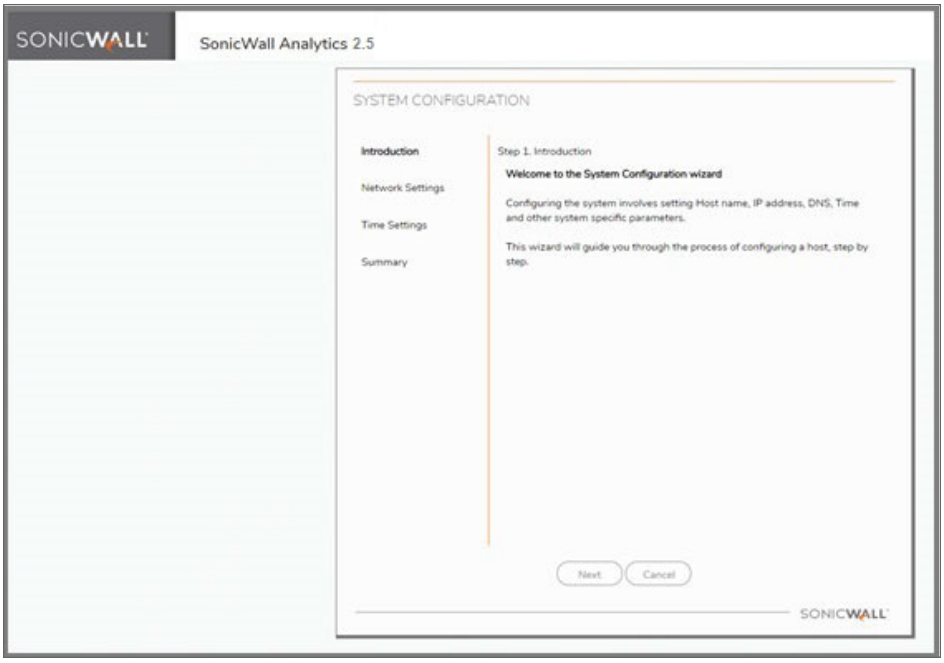
   ⓘ **NOTE:** Without DHCP, you will enter a static IP address along with associated Netmask, Mac address, Gateway entries.



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

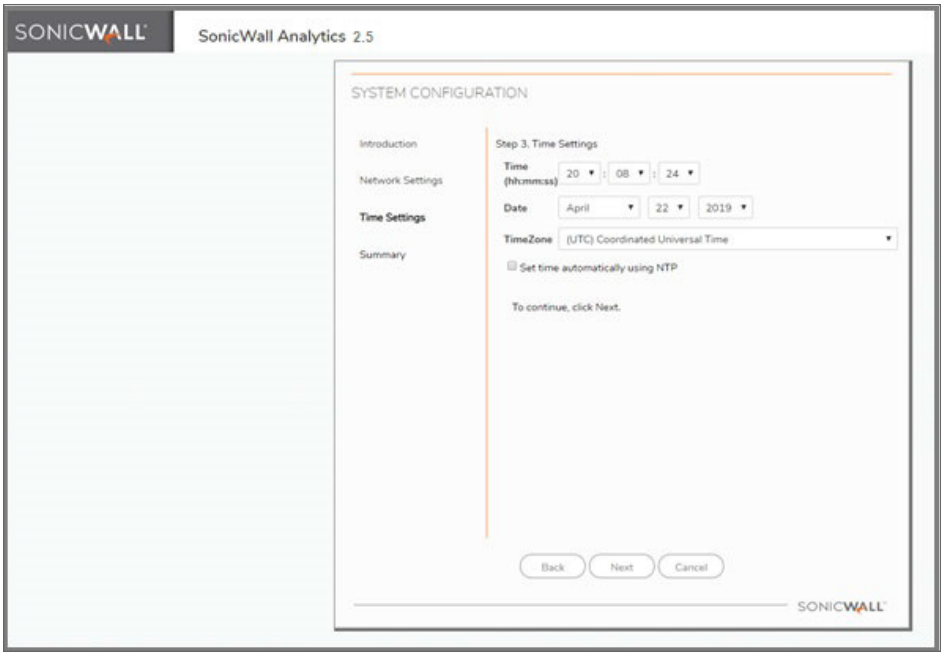


10. For initial access, use admin and password.
11. The first time up, the instance presents an initialization wizard. Use the Serial Number and Authorization Code. For this information, refer to Registering the On-Premises Analytics Instance.
12. The initialization wizard will be displayed. Click **Next**.

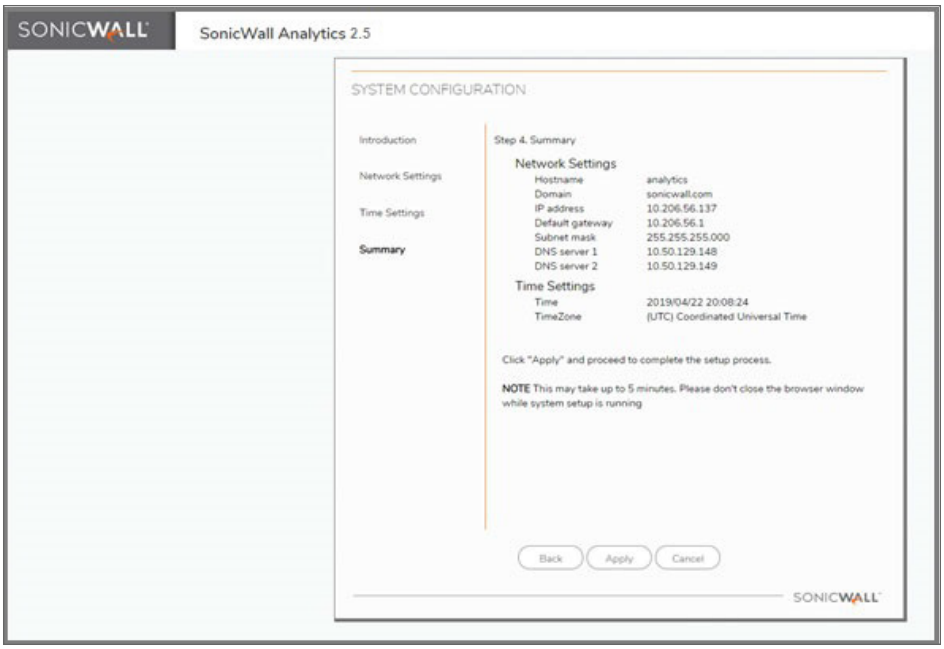


13. In **Network Settings** screen, you may choose to change the settings. Then click **Next**.

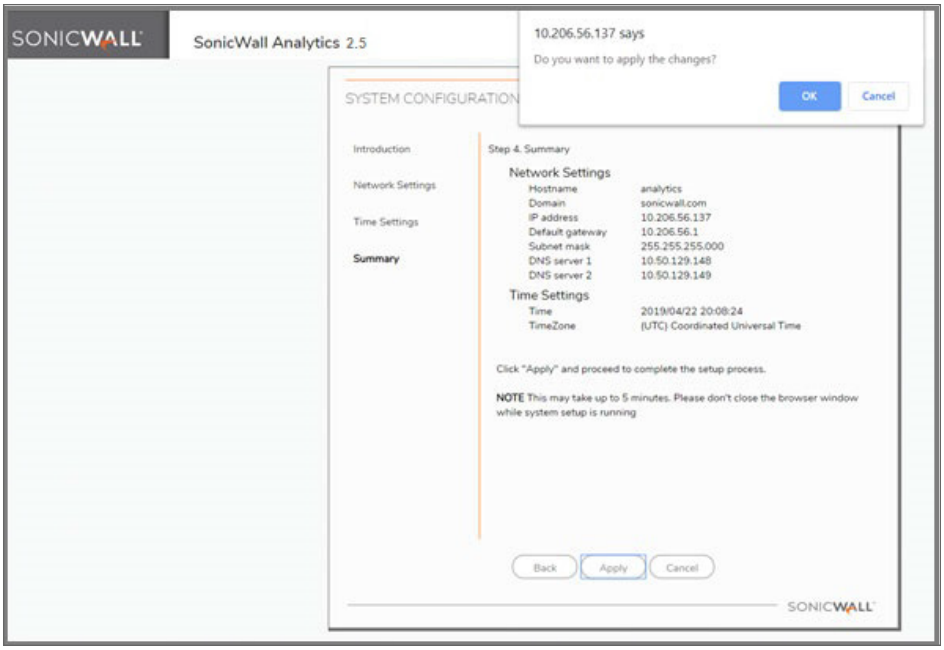
14. In **Time Settings** screen, make adjustments, if necessary, and click **Next**.



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

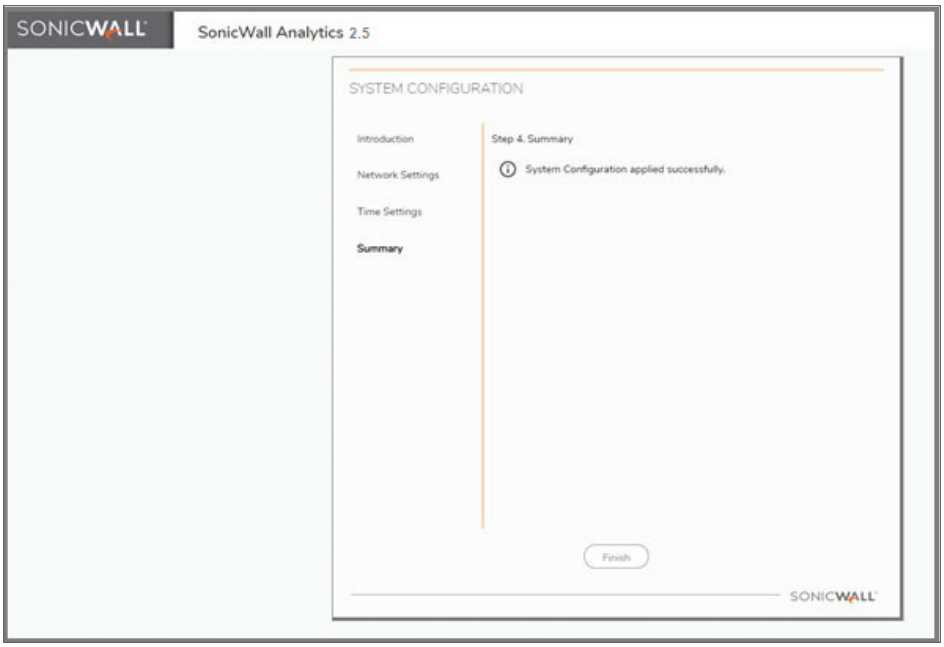


16. Click **OK**, when prompted to confirm.

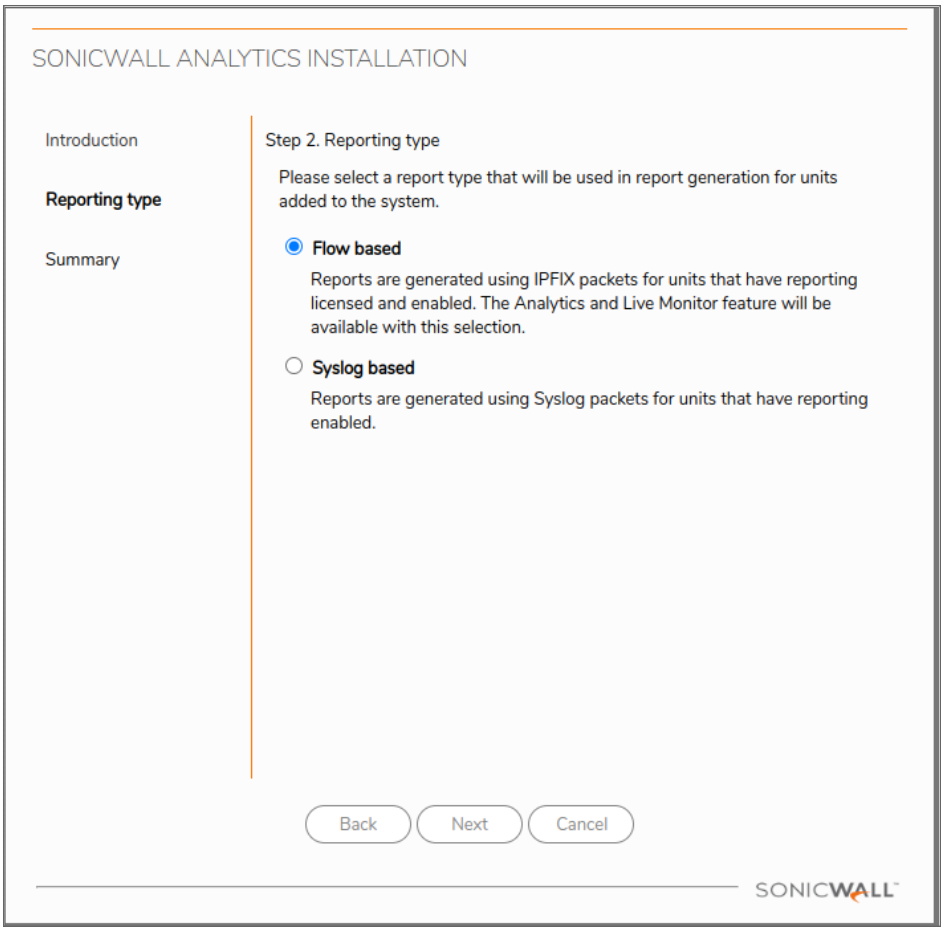


17. Success message will be displayed. Click **Finish**.

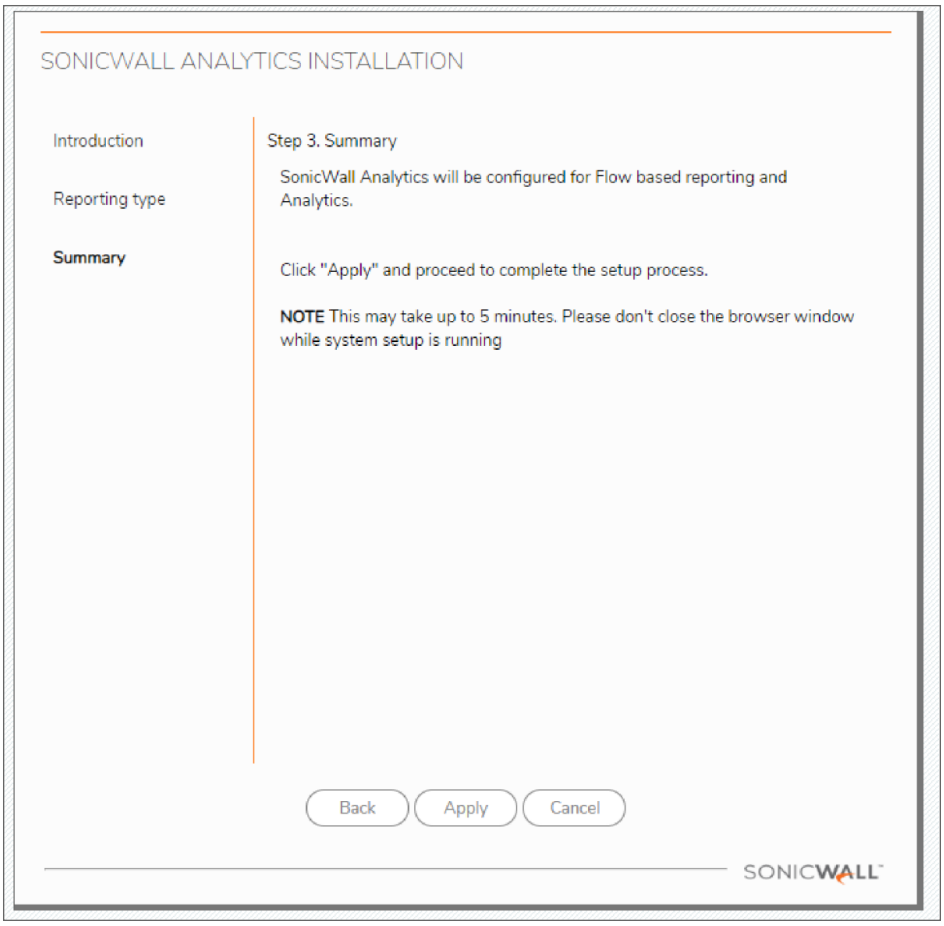
ⓘ | **NOTE:** The On-Premises Analytics instance will restart on clicking Finish.



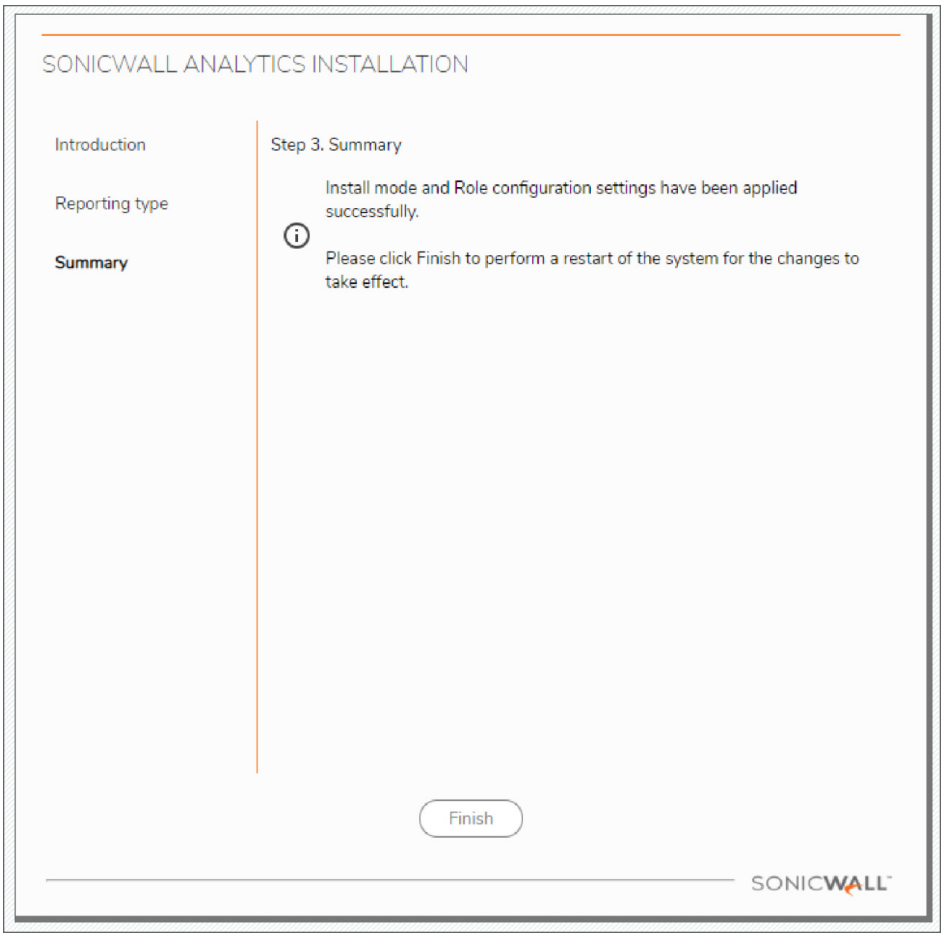
18. When the login screen reappears, enter admin in **Username**, click **Next** and enter password in **Password** to login.
19. When the installation wizard appears, click **Next**.
20. Choose **Flow based** or **Syslog based** to depending the use case for your deployment and click **Next**.



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

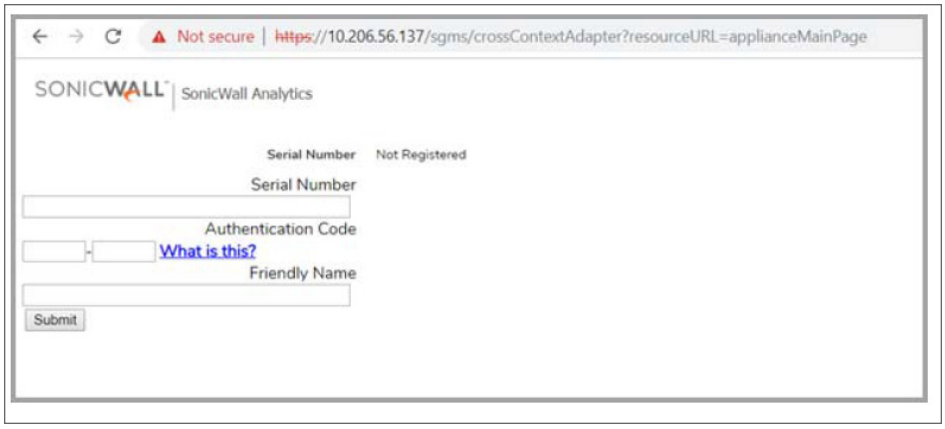


22. When the system indicates that the configuration is complete, click **Finish**.

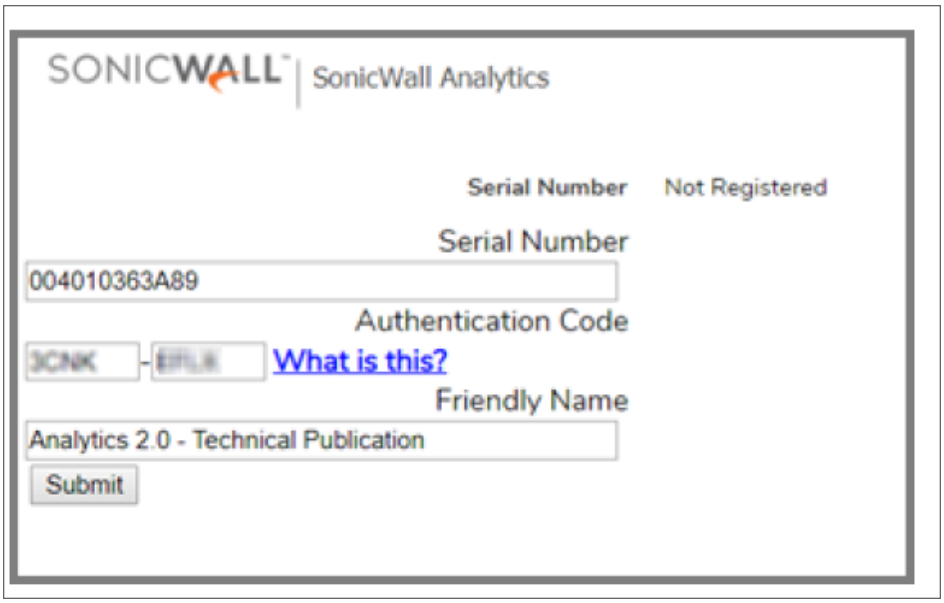


23. You will be prompted to link to your MySonicWall account.

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.

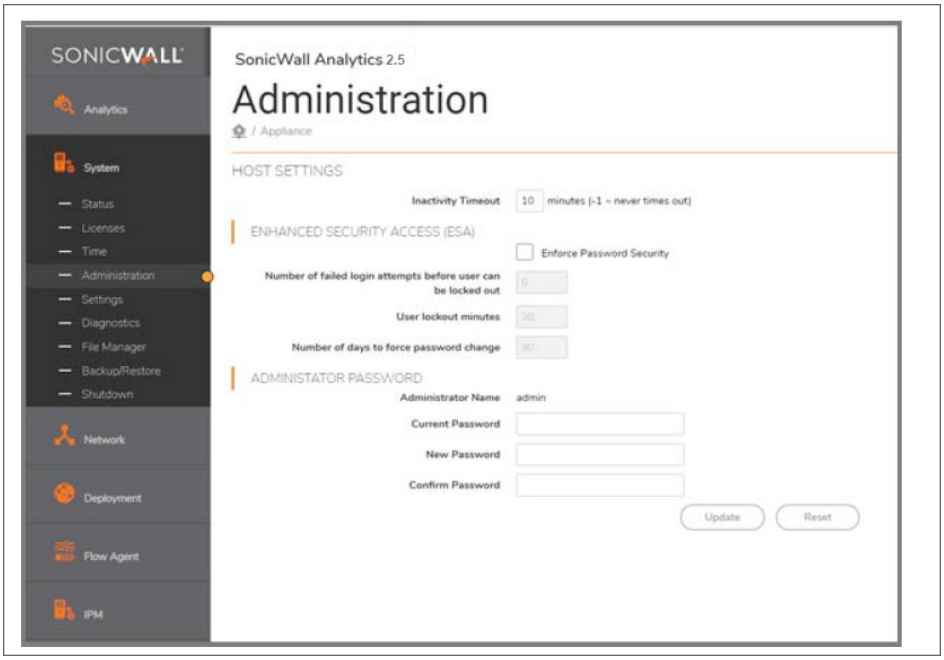


26. Click **Submit**.



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

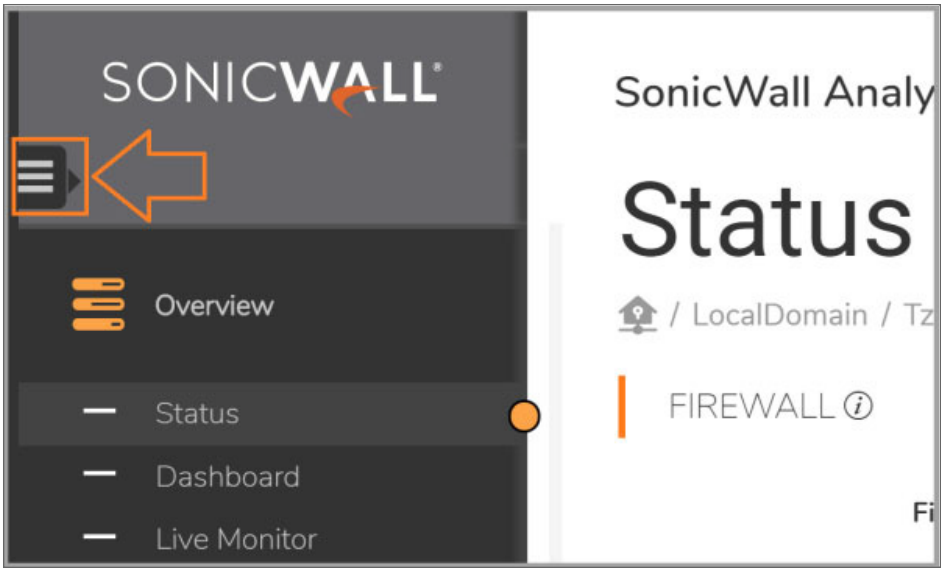
28. Navigate to **System > Administration** and set new login credentials.



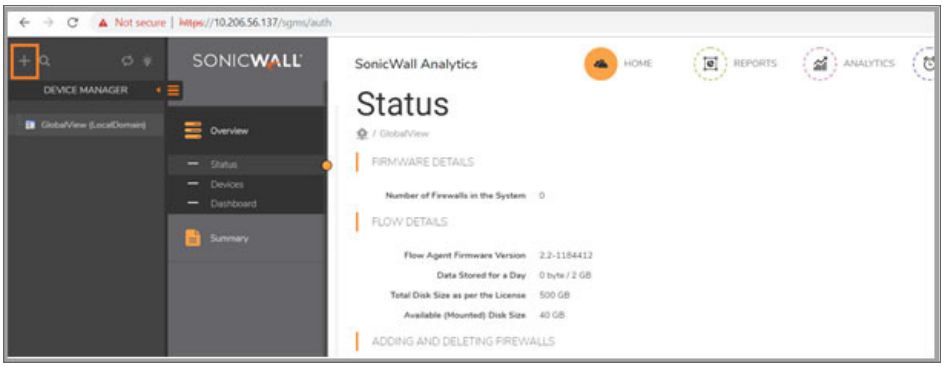
Adding Firewalls to On-Premises Analytics

To add firewalls to On-premises Analytics:

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



2. Click add icon **+**.



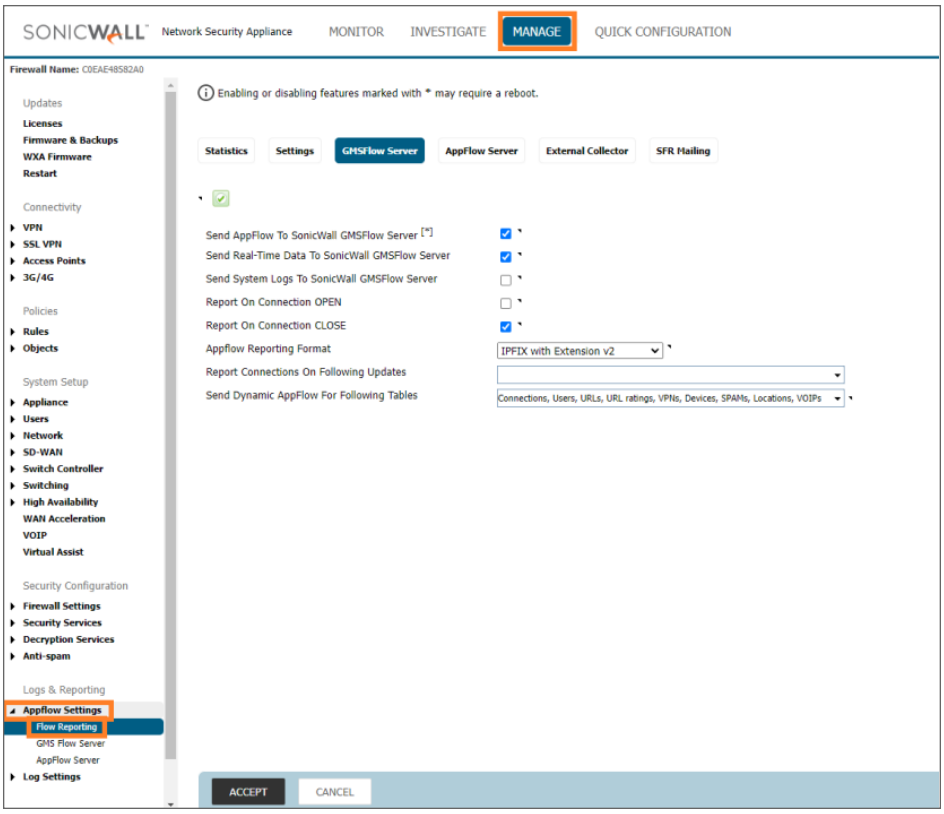
3. Enter the **Friendly Name**, the **Serial Number**, and the **Model** of the firewall.

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

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

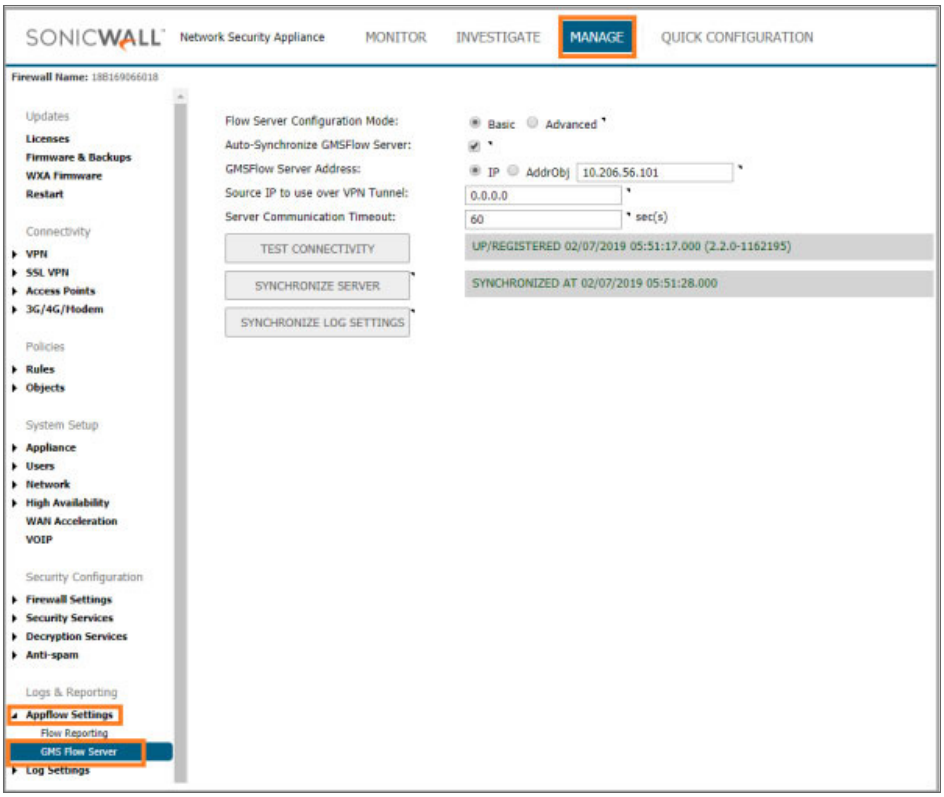
   For Syslog-based instances, go to Step 11.

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.

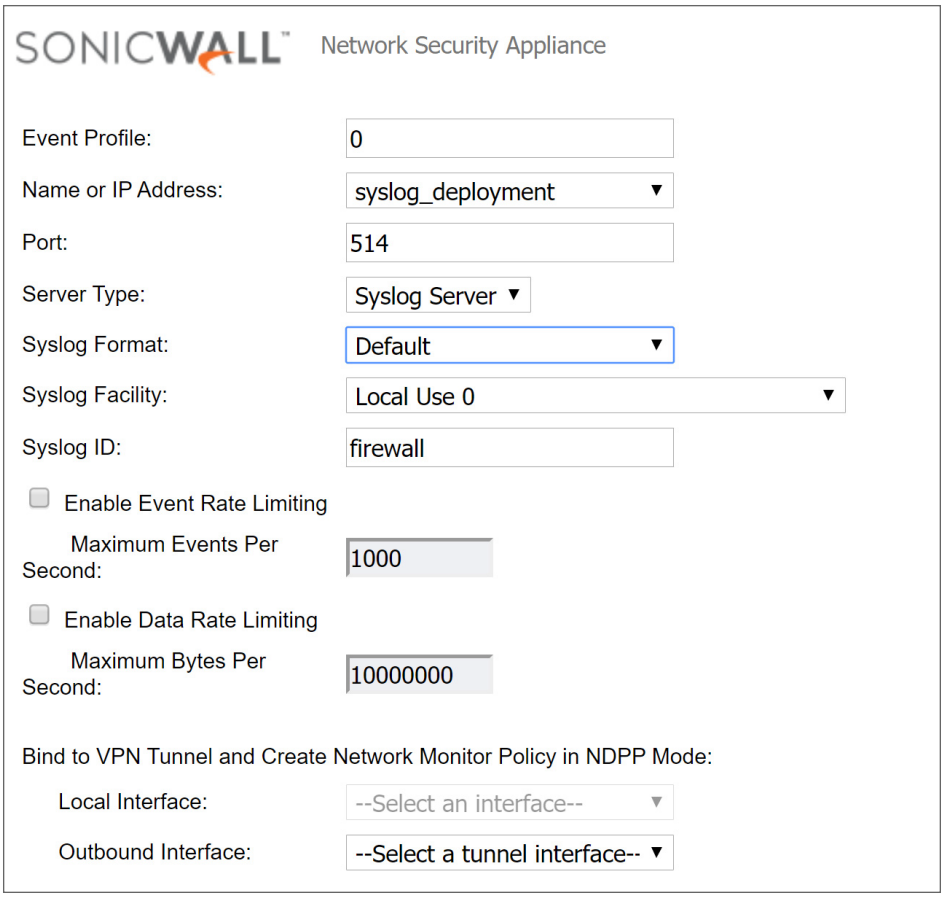
       If connectivity with the Analytics instance is a problem, go to MySonicWall and check that the firewall and Analytics instance are in the same Group or tenancy.
    c. When configuration in this panel is complete, click **Accept** at the bottom of the page.



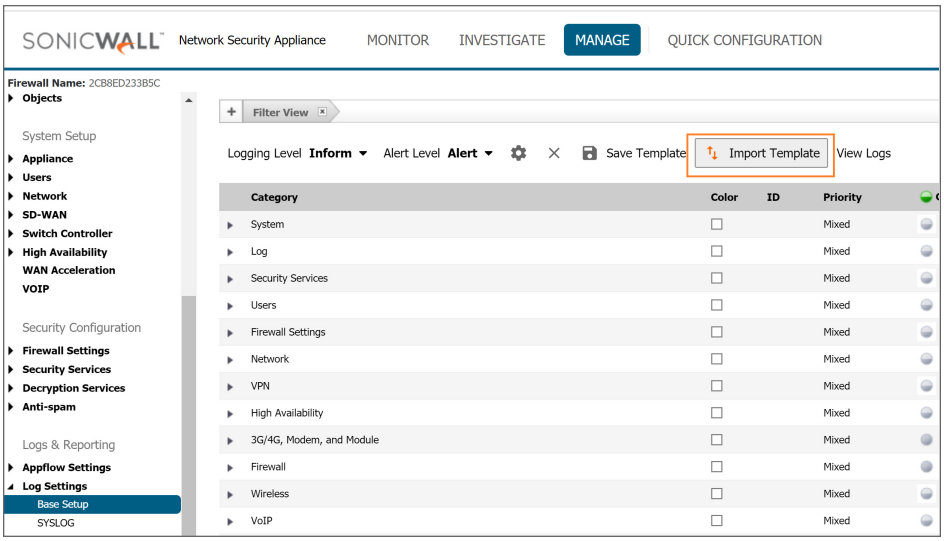
10. Repeat **Step 2** to **Step 9** for each firewall in the Group that you want to analyze IPFIX data from.

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.



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



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

4

Licensing and Registering Your On-Premises Analytics Instance

Topics:

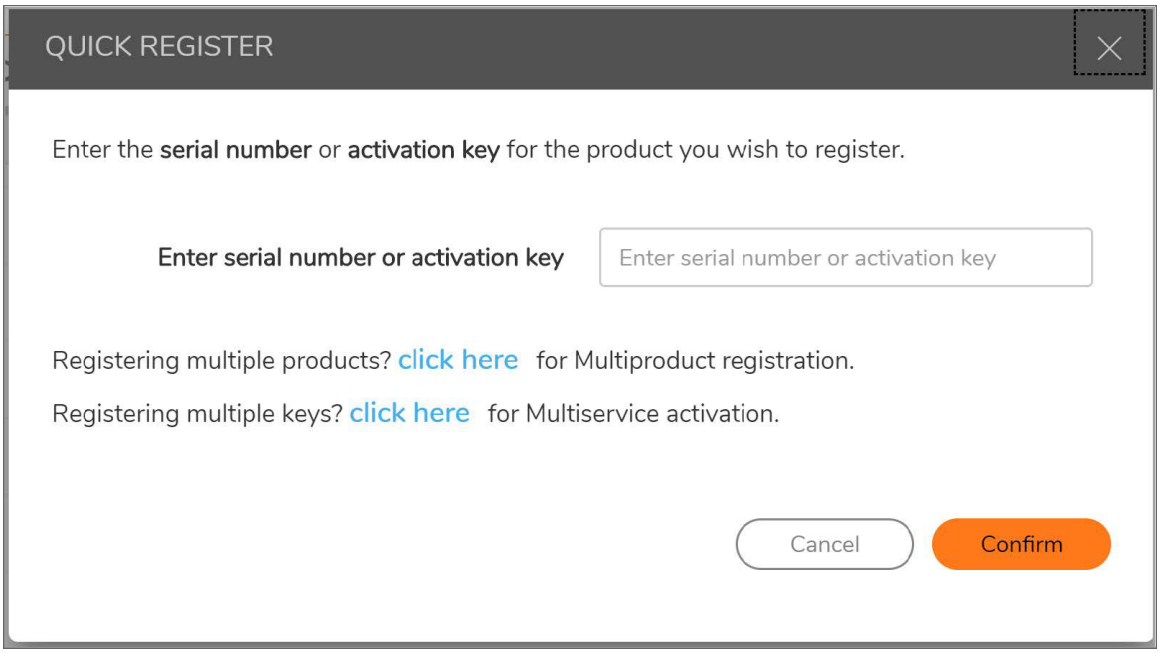
- Registering the On-Premises Analytics Instance
- Activating Firewall Licensing for Syslog-Based On-Premises Analytics
- Deregistering Your On-Premises Analytics Instance

Registering the On-Premises Analytics Instance

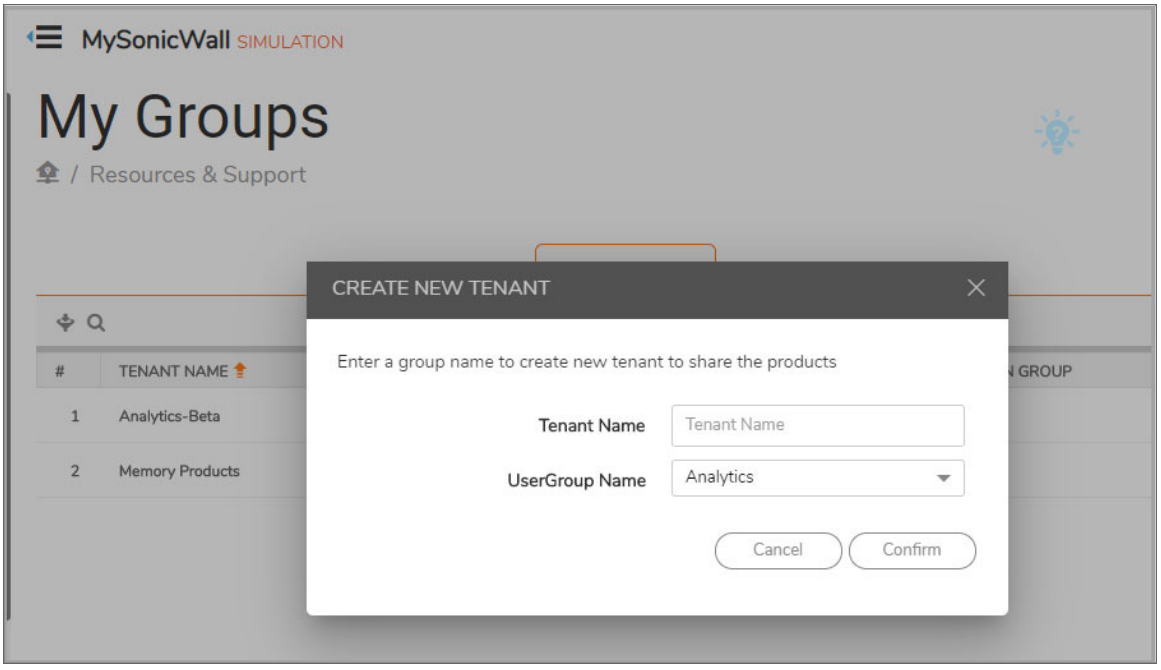
Once you have purchased a license for a SonicWallOn-Premises Analytics instance, you will receive an Activation Key code. Use the Activation Key to register your product on MySonicWall. You will get the product serial number and authorization code from MySonicWall, these can be used to register the instance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

To register your On-Premises Analytics appliance:

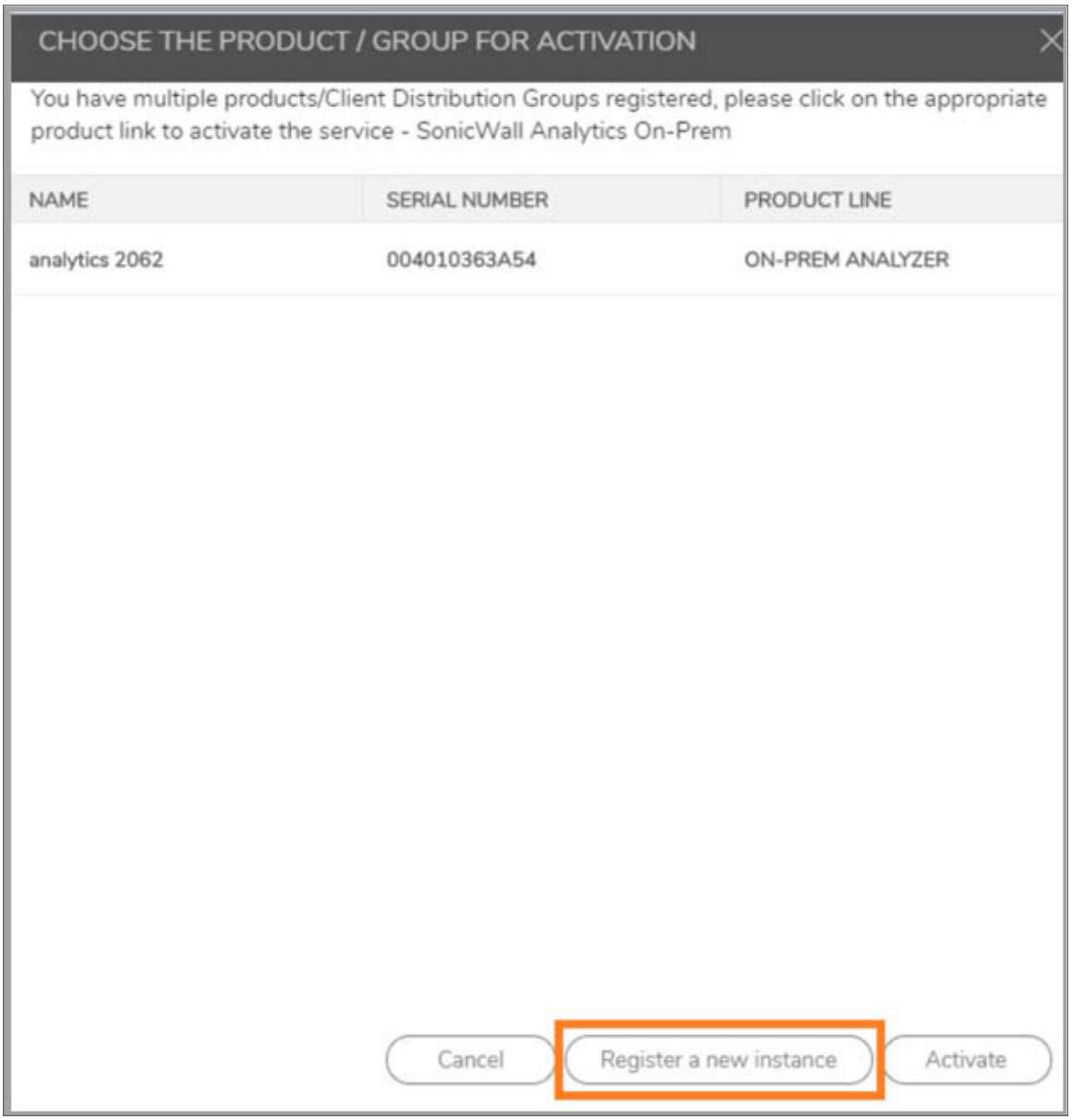
1. Log into MySonicWall, navigate to **Product Management > My Products** and click on the add products icon at the upper right :
2. Enter your **activation key**.



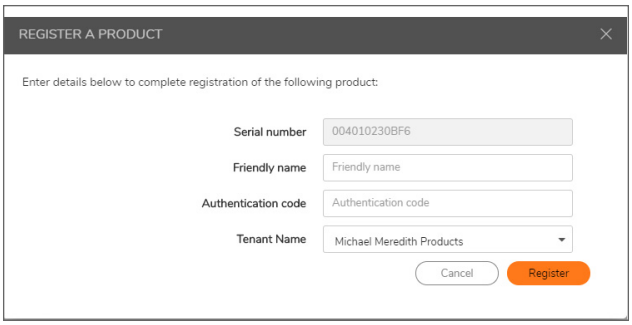
3. Select a product group into which you will deploy the instance.
    a. Navigate to **My Groups**, either create a new group or tenancy.



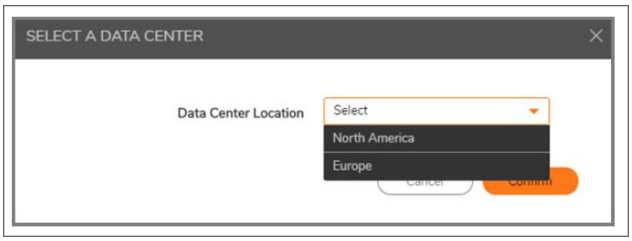
b. Or choose the group for your On-Premises Analytics instance and click **Register a new instance**.



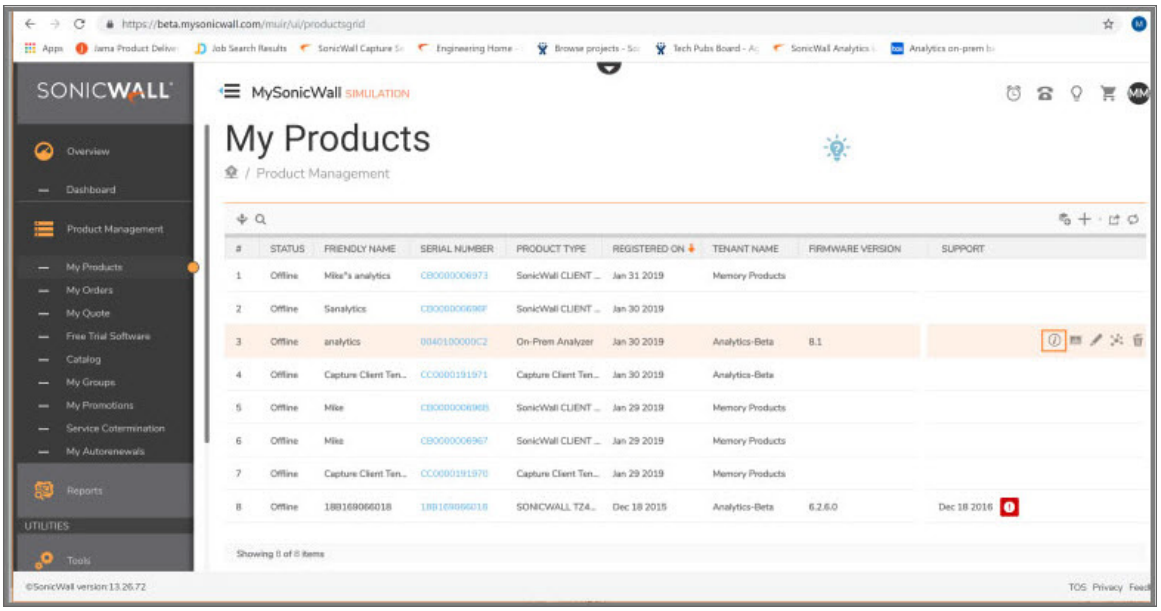
4. Establish a **Tenant Name** and a **Friendly name** for the product.



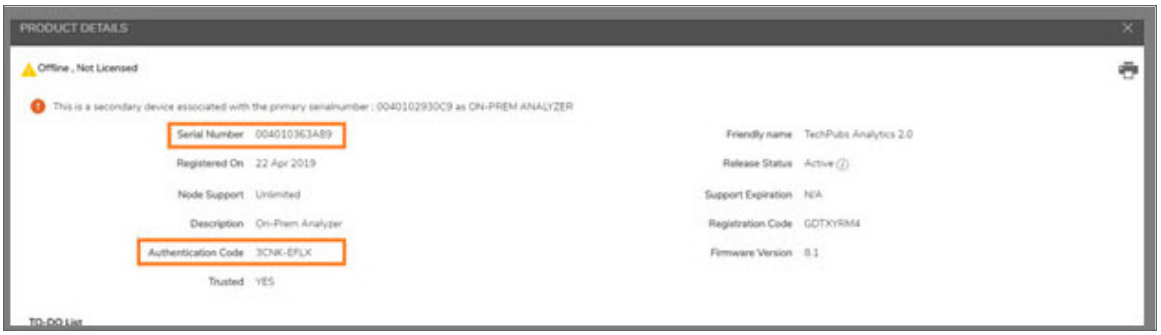
5. Select a **Data Center Location**.



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



7. Note down the **Authorization Code** and **Serial Number**.



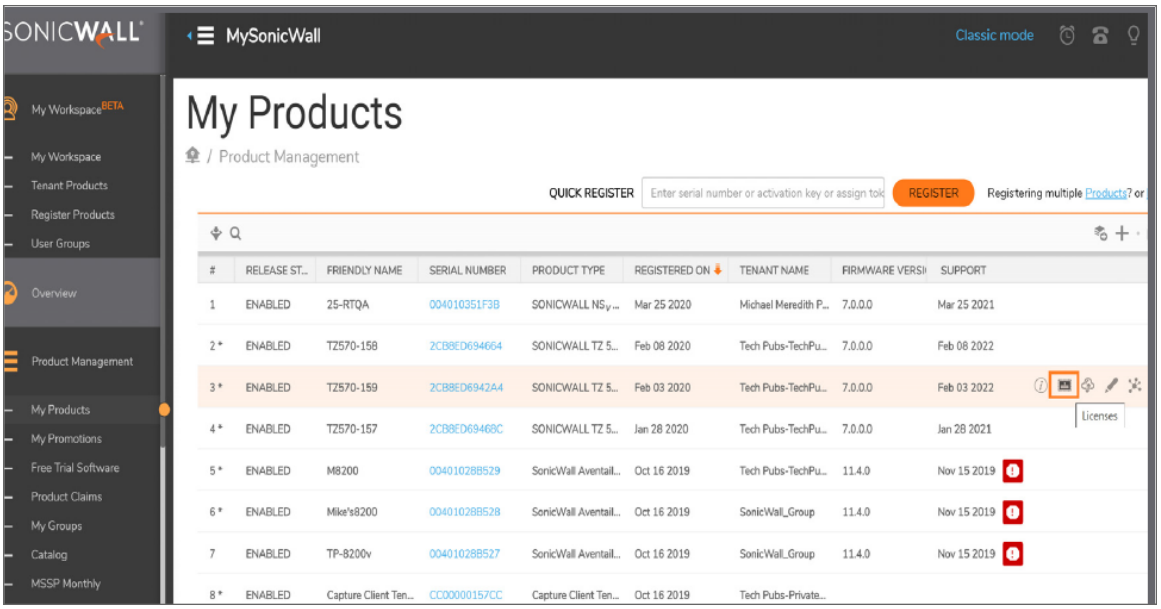
NOTE: The Serial Number and Authorization Code is needed when you bring up the On-Premises Analytics instance for the first time.

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.

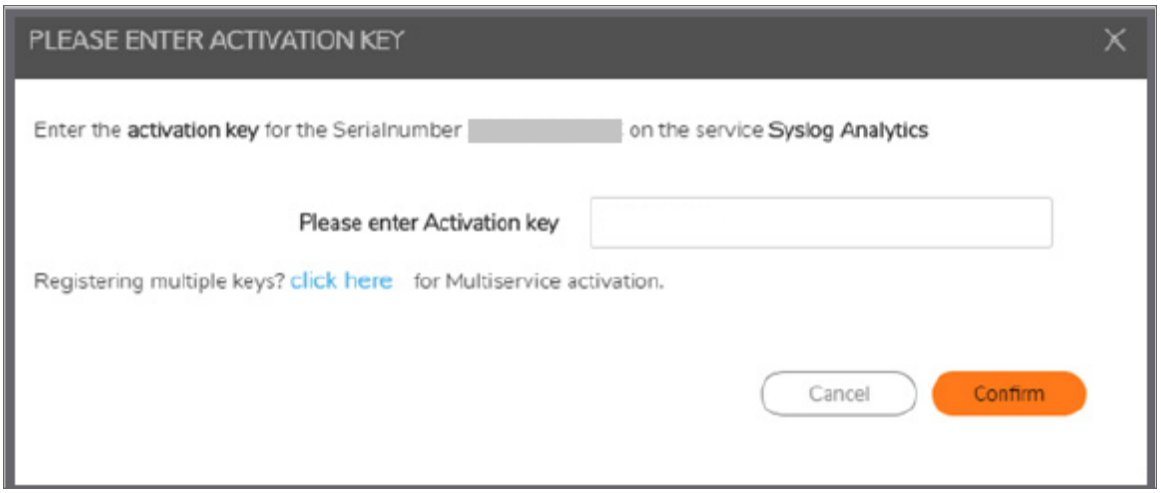
To activate license for a firewall added to a new Syslog Analytics tenant:

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



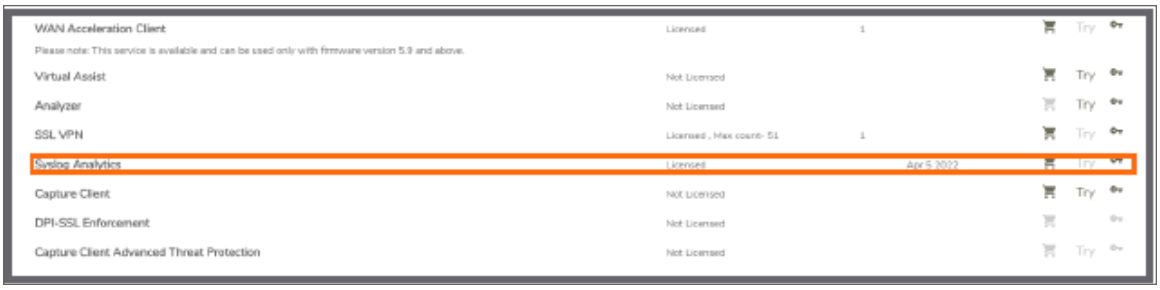
3. When the licensing list appears, identify the **Syslog Analytics** row and click on the key icon.

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

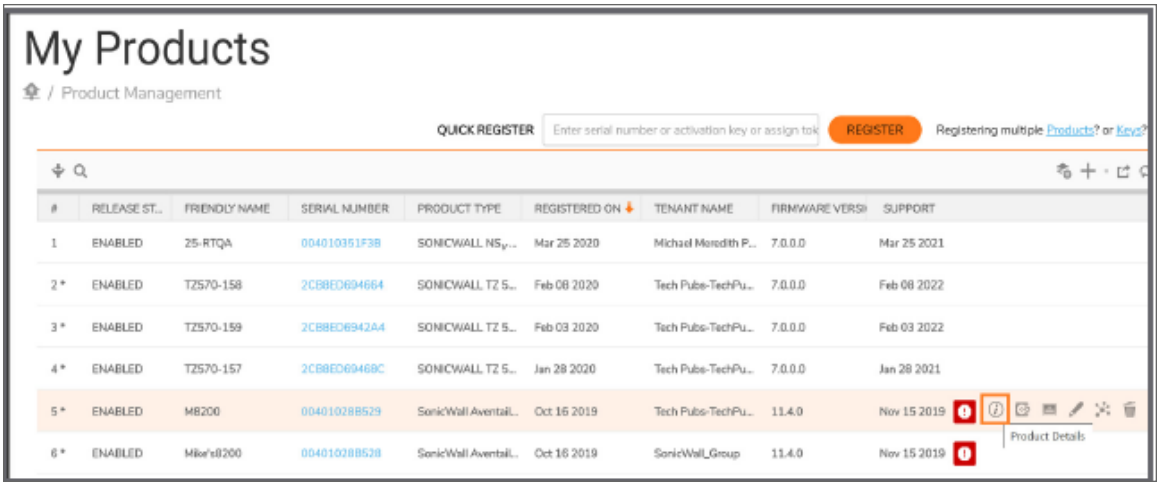


5. The system will now ask if the firewall will be licensed to serve a new or existing tenant.

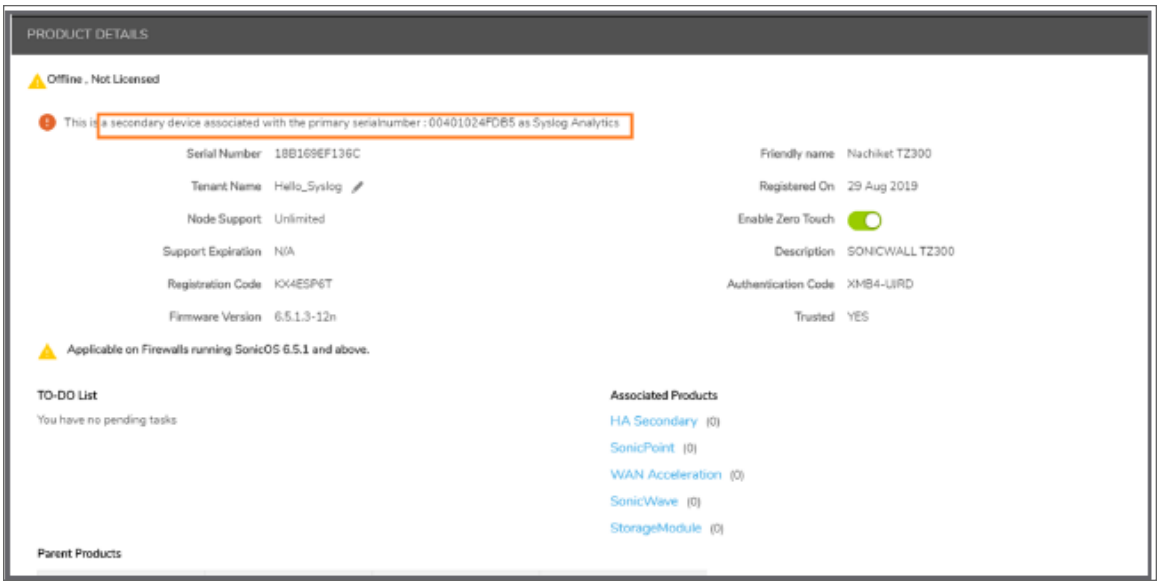
6. Return to the licensing list page and check that licensing is complete.



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



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



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.

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

5

Upgrading On-Premises Analytics

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

ⓘ | **NOTE:** SWI upgrade to Analytics 2.5.5 is not supported.

ⓘ | **NOTE:** In the event the Analytic GUI is unavailable, upgrades and hotfixes may be applied through the remote web interface in Azure. 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 2.5.5
- Upgrading Analytics using SWI file

Upgrading Analytics 2.5.5

Users can upgrade to Analytics 2.5.5 from 2.5.4 or 2.5.3.

ⓘ | **NOTE:** It is recommended to take a backup of the external disk before proceeding to any upgrade process.

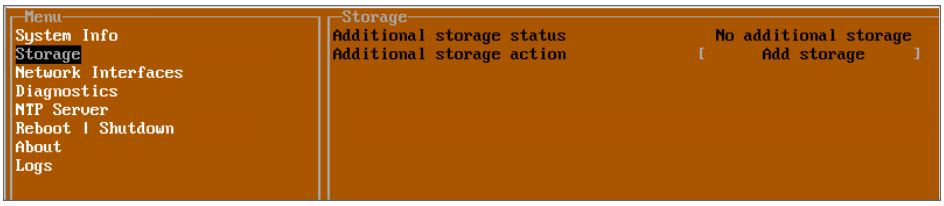
ⓘ | **NOTE:** For customers on any Analytics version older than Analytics 2.5.3, please contact support for upgrade. To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

The following table summarizes the various ways to upgrade to Analytics 2.5.5:

Current Analytics Version	Upgrade Procedure
Analytics 2.5.4 with data in external disk	Follow the steps under Upgrading Analytics with data in external disk
Analytics 2.5.4 with data in internal disk	Follow the steps under Upgrading Analytics with data in internal disk
Analytics 2.5.3 with data in external disk	Follow the steps under Upgrading Analytics with data in external disk
Analytics 2.5.3 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.



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 2.5.5, for customers with systems configured with the Analytics 2.5.4 or 2.5.3 and data present in external disk, the below steps summarizes the upgrade process:

- Unmount the hard disk from Analytics 2.5.4 or 2.5.3, refer Unmounting the Hard Disk from older Analytics Version.
- Mount it on Analytics 2.5.5, refer Mounting the Hard Disk on new Analytics.

ⓘ **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 to Analytics 2.5.5, for customers with the Analytics 2.5.4 or 2.5.3 configured on the system and data present in internal disk, the below steps summarize the upgrade process:

For customers on 2.5.4

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 Analytics 2.5.4. Refer Unmounting the Hard Disk from older Analytics

Version.

5. Mount it on Analytics 2.5.5. Refer Mounting the Hard Disk on new Analytics.

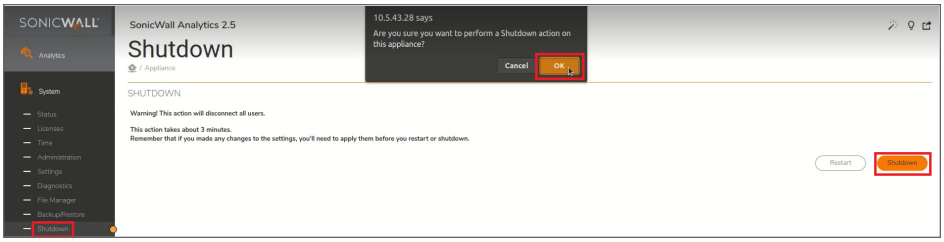
For customers on 2.5.3

1. Upgrade to Analytics 2.5.4. Refer Upgrading Analytics using SWI file.
2. Prepare the Analytics to add external disk. Refer Preparing the Analytics to Add External Disk.
3. Add external disk. Refer Adding External Disk.
4. Migrate the data from internal to external disk. Refer Migrating the Data To External Disk.
5. Unmount the hard disk from Analytics 2.5.4. Refer Unmounting the Hard Disk from older Analytics Version.
6. Mount it on Analytics 2.5.5. Refer Mounting the Hard Disk on new Analytics.

Unmounting the Hard Disk from older Analytics Version

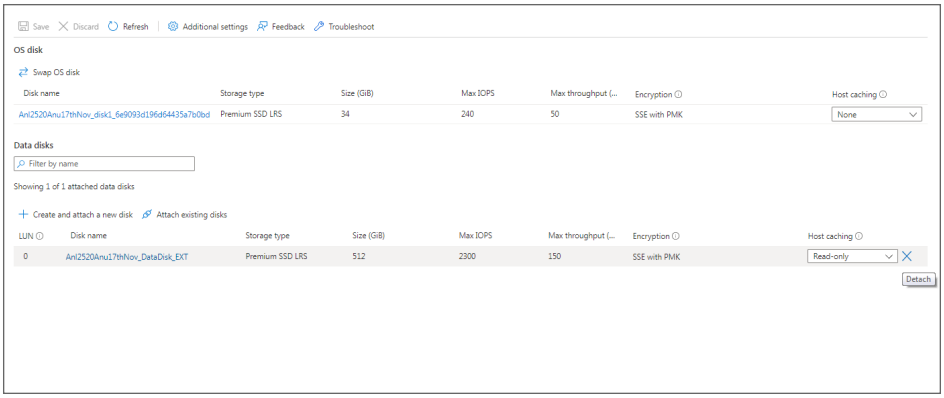
To unmount the hard disk from old Analytics version:

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, in Azure portal, navigate to **Disks > Settings**.

4. Unmount the Hard disk, under **Data Disks**, by clicking **X** button on right corner of the Hard disk in Azure.



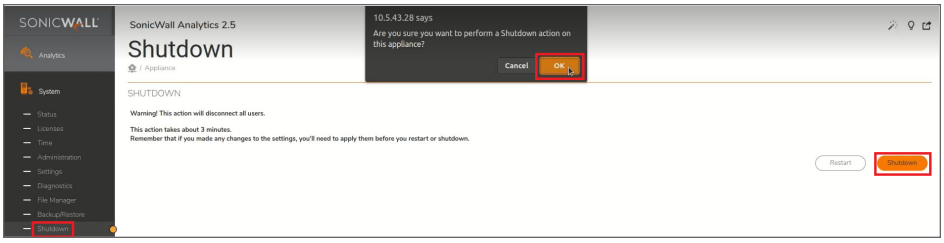
Mounting the Hard Disk on new Analytics

To mount the hard disk on new Analytics version:

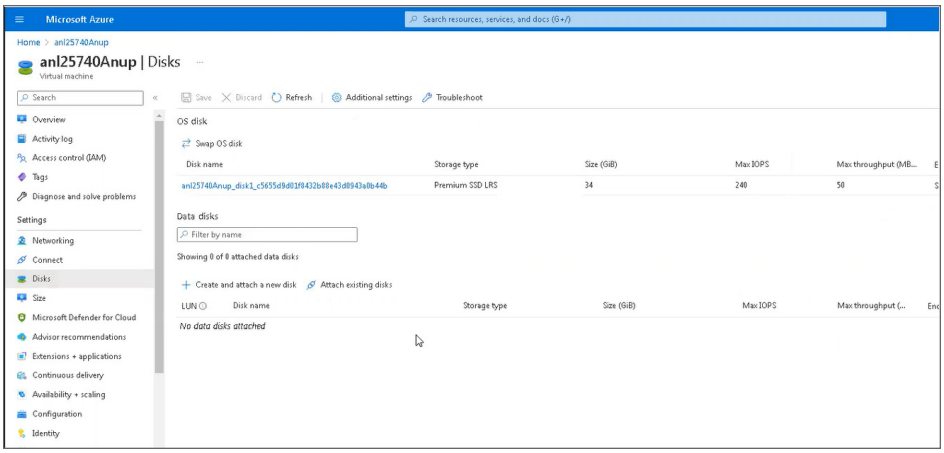
1. Install a fresh Analytics 2.5.5 VM using latest 2.5.5 VHD file and steps from Installing On-Premises Analytics on Azure and configure the VM with same IPV4 address as the older Analytics version setup following the steps under Configuring On-Premises Analytics on Azure.

   ⓘ **NOTE:** There will be a downtime while unmounting older version Analytics and mounting new version Analytics.

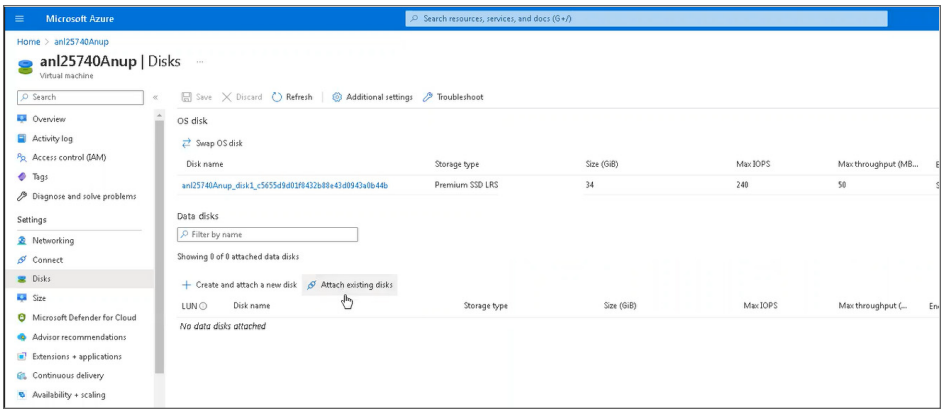
2. Login to the Analytics UI using the IPV4 address, username and password.
3. Navigate to **System > Shutdown**. Click **Shutdown**. On prompting for confirmation, click **OK**.



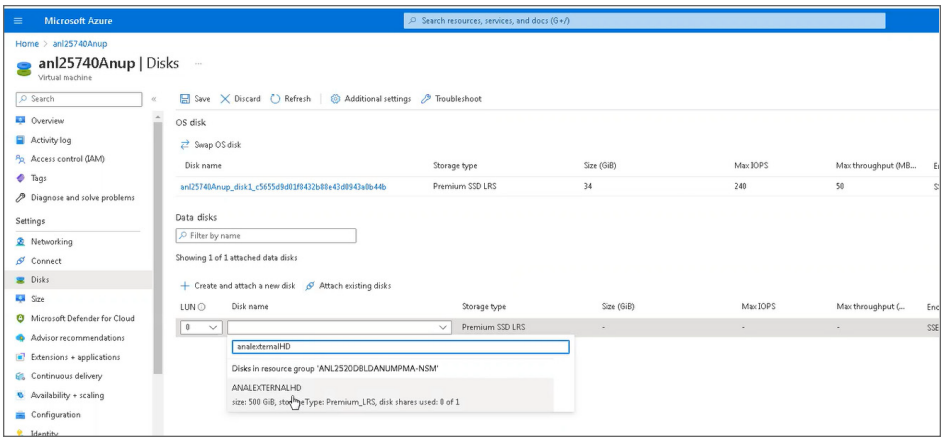
4. In Azure portal, navigate to **Disks > Settings**.



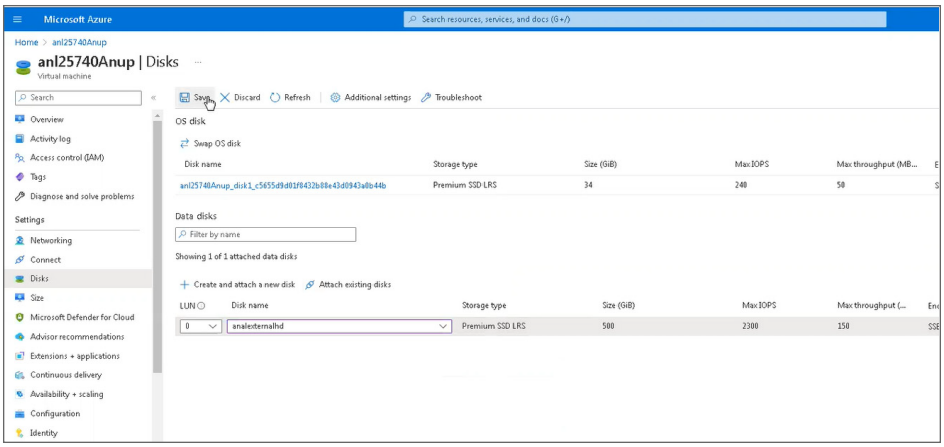
5. Click **Attach existing disk**.



6. Type the Name of the Hard disk that you had removed from the previous Analytics VM.

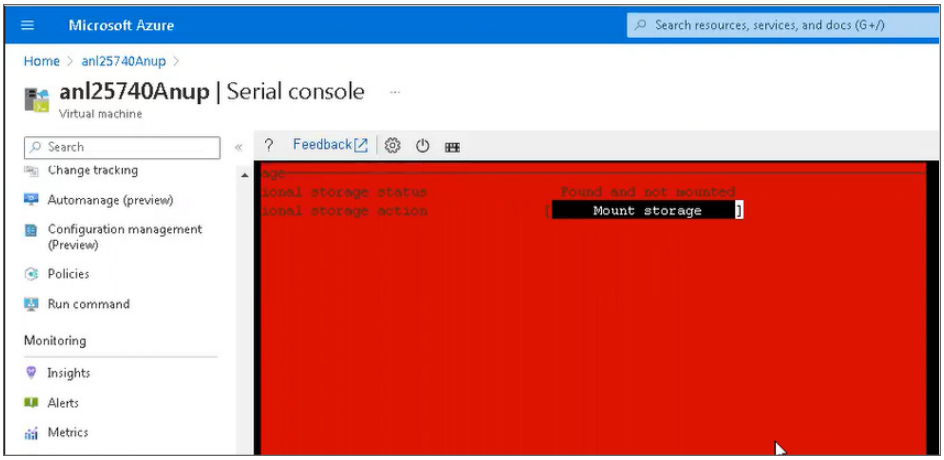


7. Click **Save**.

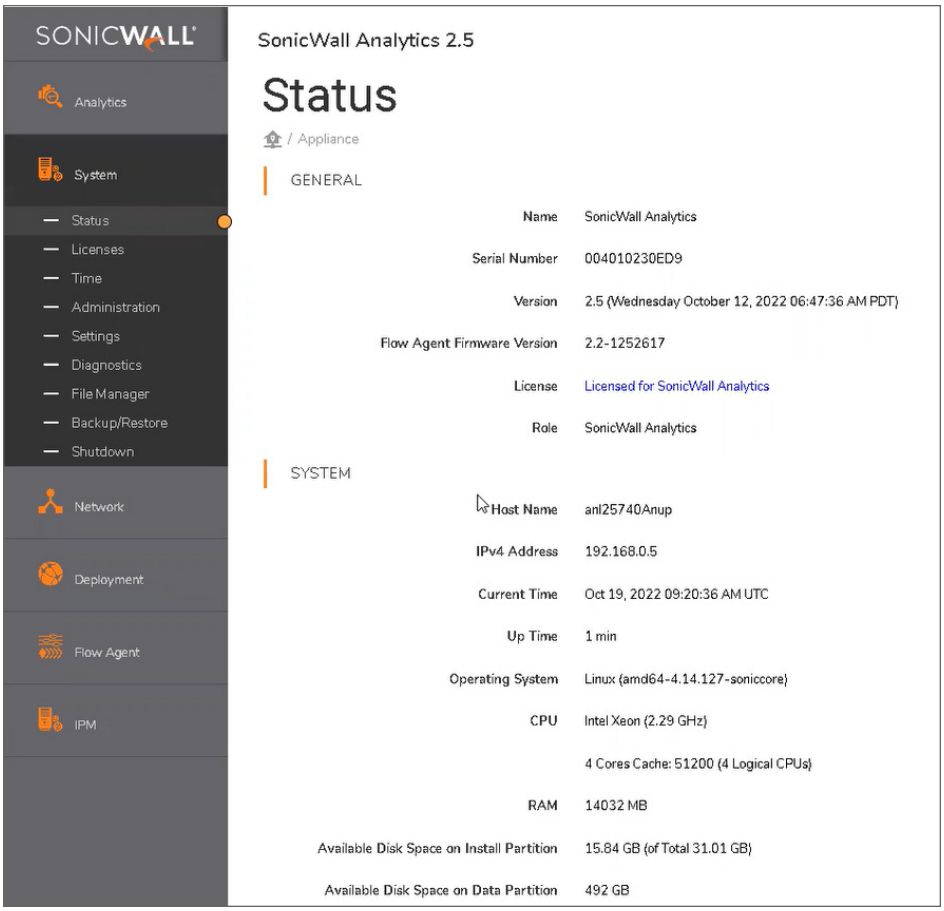


8. Power on the Analytics 2.5.5 and mount the storage.

   ⓘ **IMPORTANT:** 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.



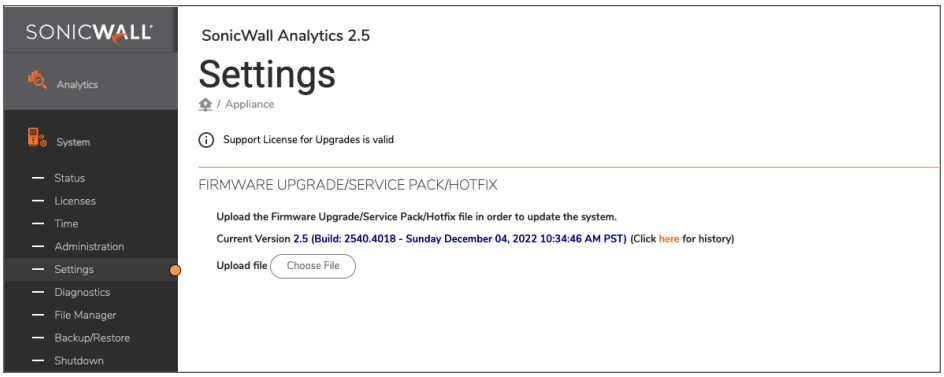
9. Login to the Analytics UI using the IPV4 address, username and password.
10. Navigate to **System > Status**. The page displays the details of the installed Analytics.



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**.

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

6

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.

ⓘ **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

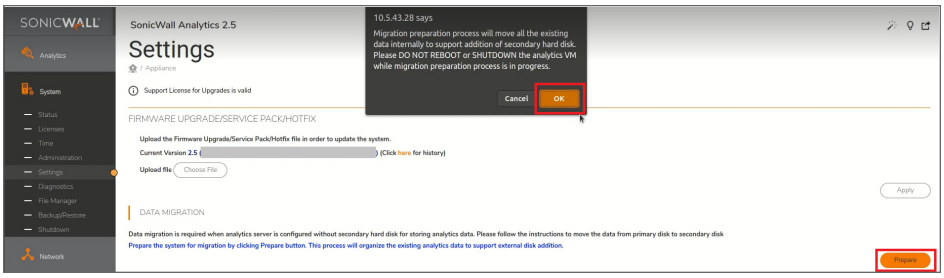
Preparing the Analytics to Add External Disk

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**.

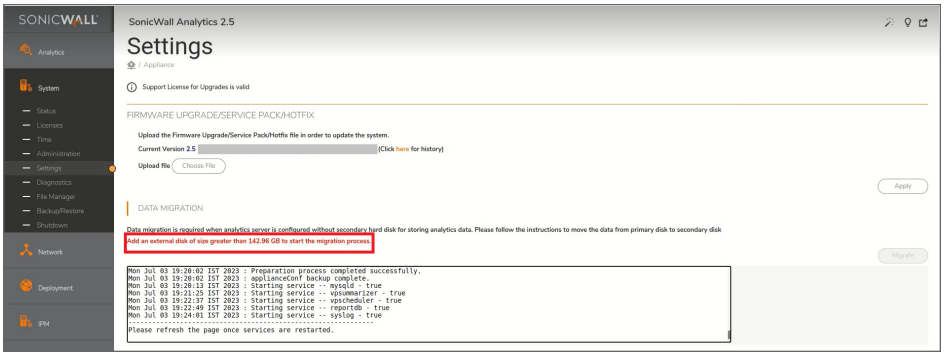


ⓘ | **NOTE:** This process will take some time to complete. Refresh the page at regular intervals.

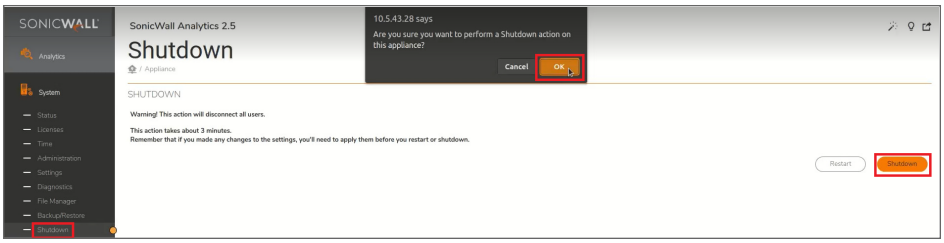
Adding External Disk

To add external disk:

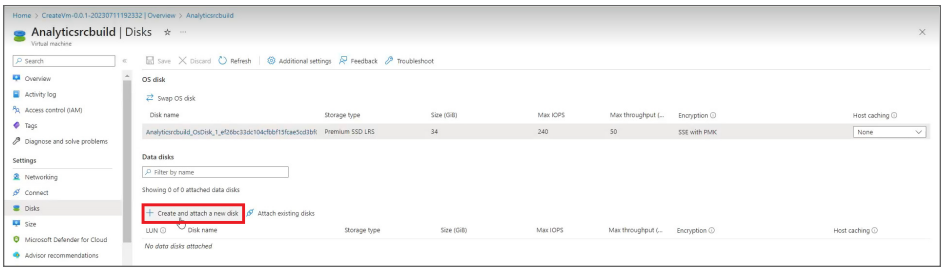
1. Navigate to **System > Settings**. On successfully preparing the system to support external disk, the Settings page will display a message to add external disk.



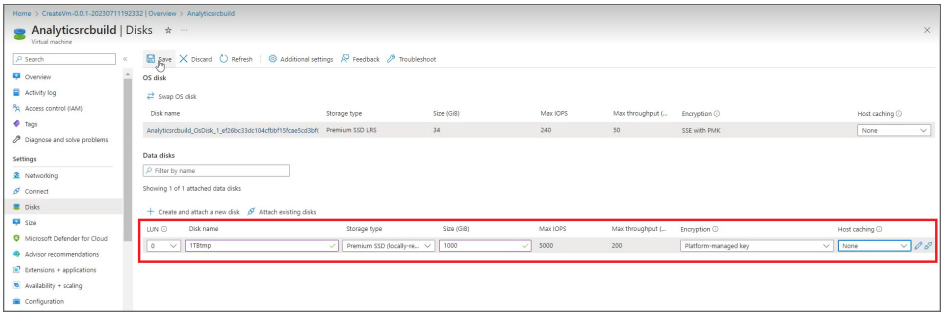
2. Navigate to **System > Shutdown**. Click **Shutdown**. On prompting for confirmation, click **OK**.



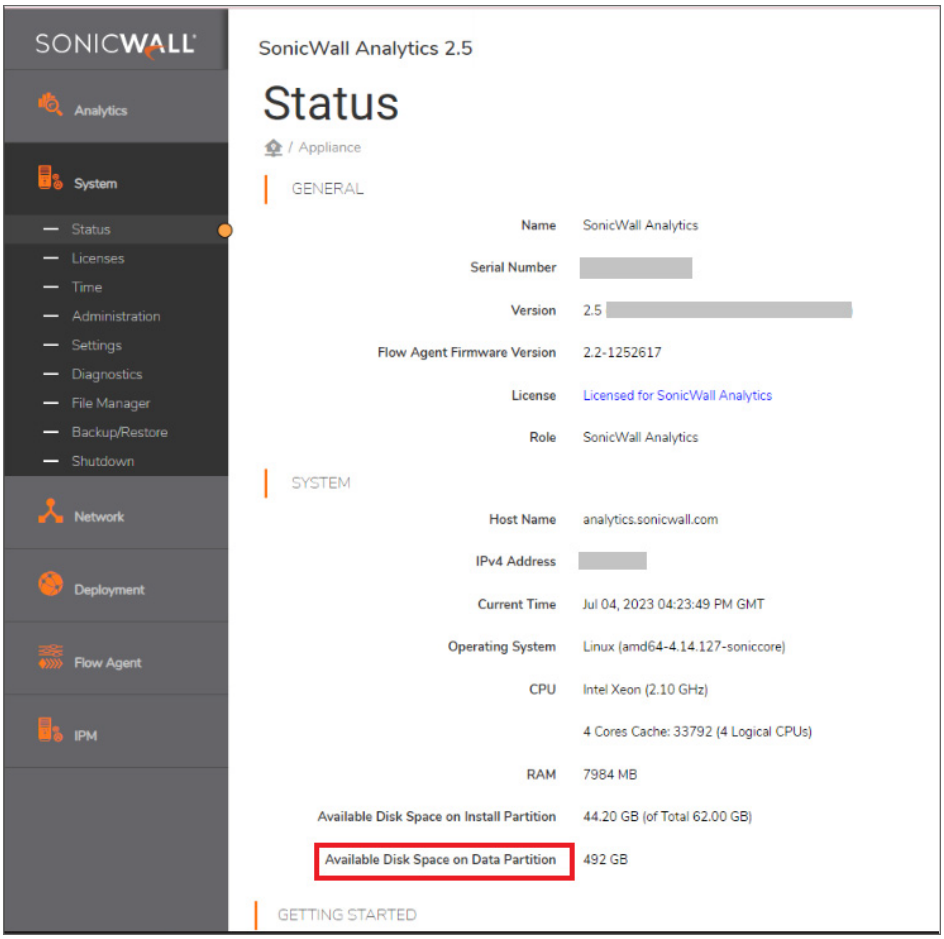
3. Bring up the Azure Portal, navigate to **Disks > Settings**.
4. Click **Create and attach a new disk**.



5. Enter the **Disk name**, **Storage type**, **Size** of the new data disk. Refer to IPFIX Based Licensing Model on recommendations in size.



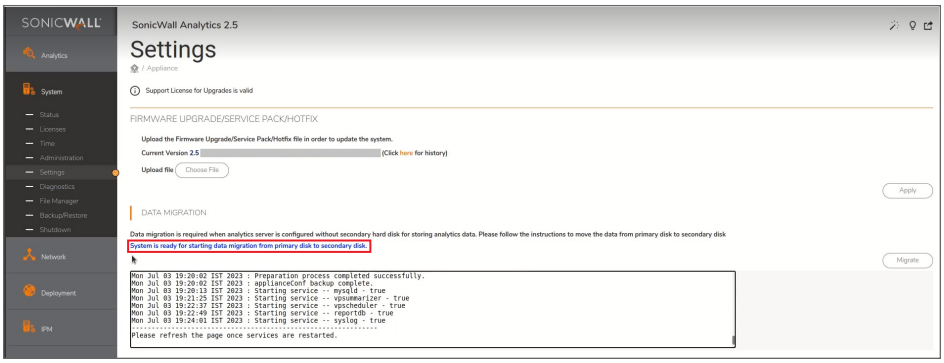
6. Click **Save**.
7. Add and mount the storage. Follow **steps 1 to 6** under Configuring On-Premises Analytics on Azure.
8. Login to the Analytics UI using the IPV4 address, username and password.
9. Navigate to **System > Status**. Verify that the added storage is displayed in **Available Disk Space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



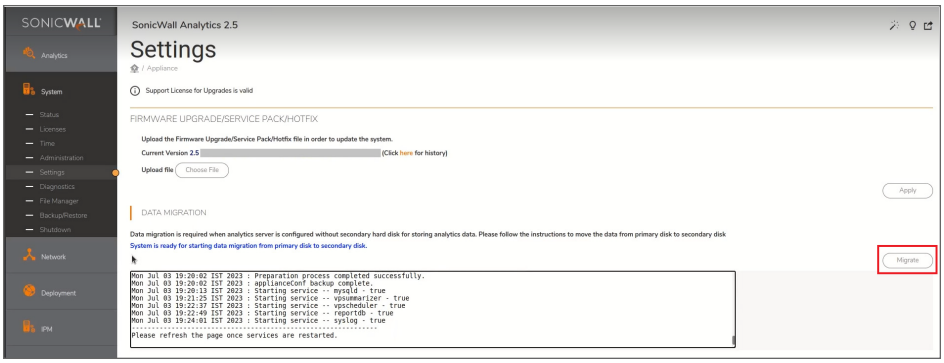
Migrating the Data To External Disk

To migrate the data:

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



2. Click **Migrate**.



ⓘ | **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.

7

Using the Management Console

Topics:

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

Connecting to the Console

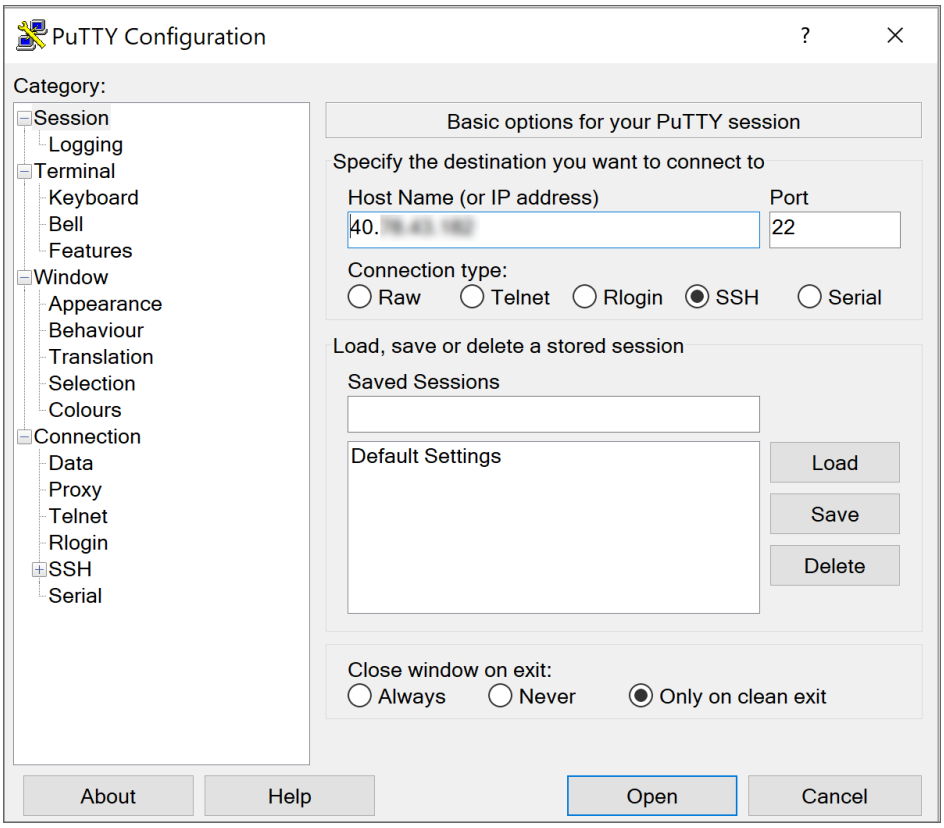
There are two ways to connect to the Management Console:

1. Use SSH or PuTTY to access the public IP address of the On-Premises Analytics instance.
2. Use the Azure remote console to access the On-Premises Analytics command line interface.

   ⓘ **NOTE:** The public IP address is the WAN IP address appearing in the Azure Virtual Machine Connection.

To connect to the management console using SSH:

1. Launch PuTTY and type in the public IP address of the On-Premises Analytics instance on Azure.

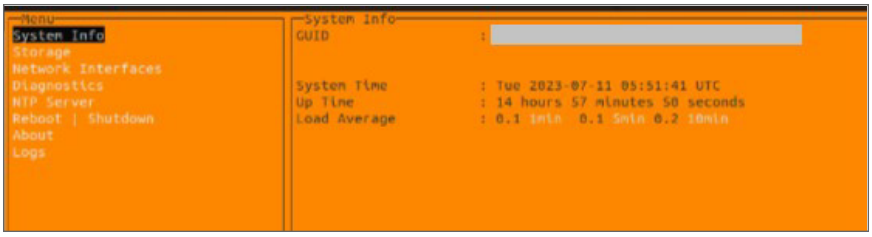


2. For **Port**, type in **22** if it is not already set.
3. For **Connection type**, **SSH** should already be selected by specifying port 22.
4. Click **Open** to open a console connection.
5. When you are prompted to log in at the **User** prompt, enter the SonicOS administrator credentials **(default: admin / password)**.

To connect to the management console through Azure:

1. Bring up the Azure Manager, select the On-Premises Analytics instance with a left-click and then right-click to select Connect.
2. Wait for the On-Premises Analytics instance to boot to the command line in the Azure Virtual Machine Connection window and then login as admin with the password: password.
3. Press Ctrl+s and then press the spacebar to toggle between the Azure remote console and the Management Console. That is, press the Ctrl key and ‘s’ key together, then release and press the spacebar.

The Management Console will appear:

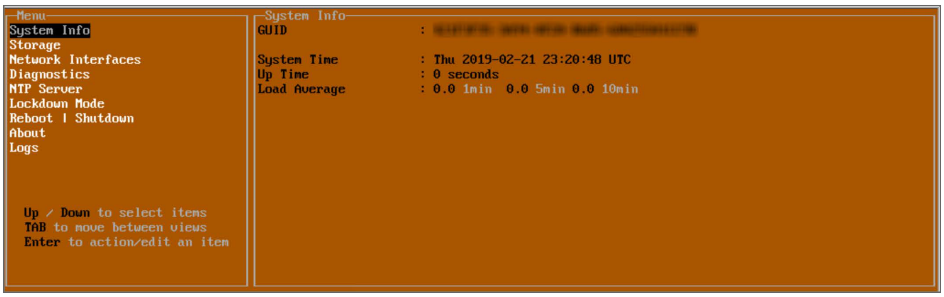


Management Console Operations

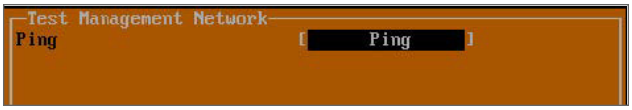
The Management Console provides options for viewing and changing system and network settings, running diagnostics, rebooting the system, and other functions.

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.

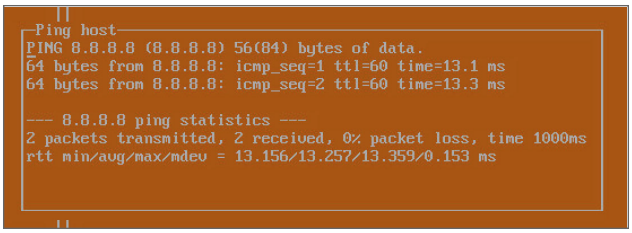


3. Press the Tab key to move the focus from left side menu to the main view (right pane), or vice versa.
4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.

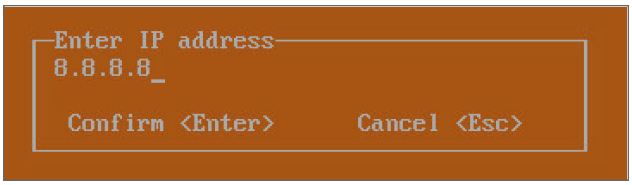


5. To select an option for editing or to choose the associated action, use the up/down arrow keys to move the focus to the editable/actionable items and press the Enter key.

   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.

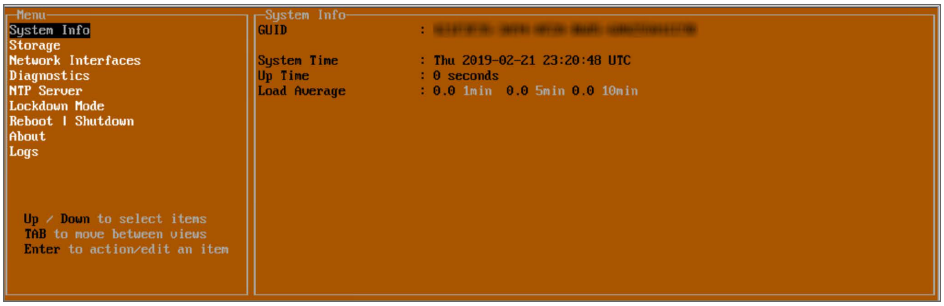


6. Use the arrow keys as needed to move between selections in the dialog. To change a value, press **Backspace** to erase each character, then type in the new value. When ready, press **Enter** to commit the change or perform the selected action. You can dismiss the dialog by pressing **Esc**.

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



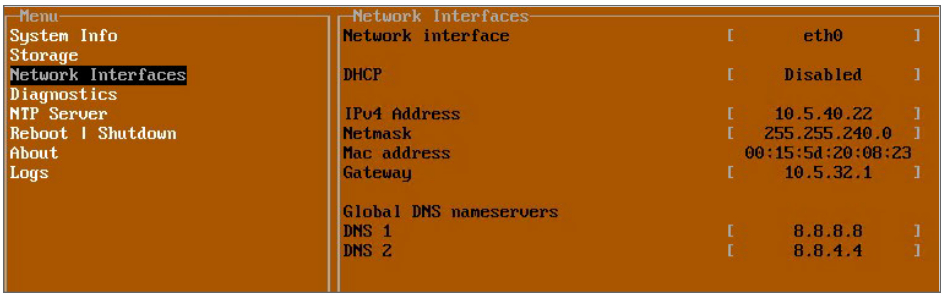
Some of the information in the System Info screen is dynamic. The following information is displayed:

- **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

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

Network Interfaces

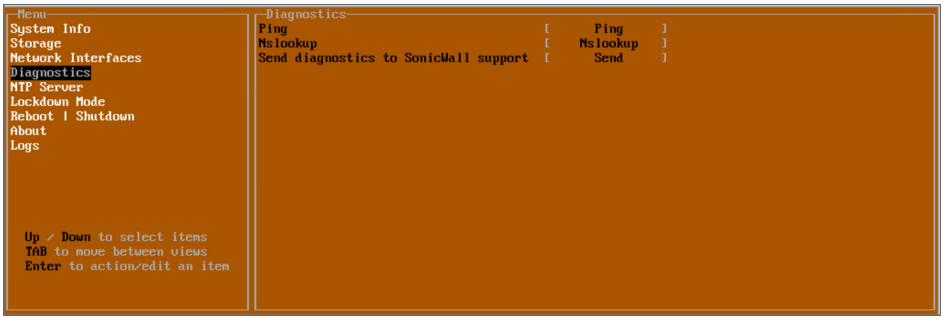


In the **Network Interface** screen, you can configure these settings.

- **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.

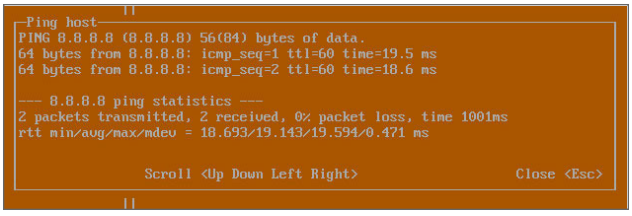
Diagnostics



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.



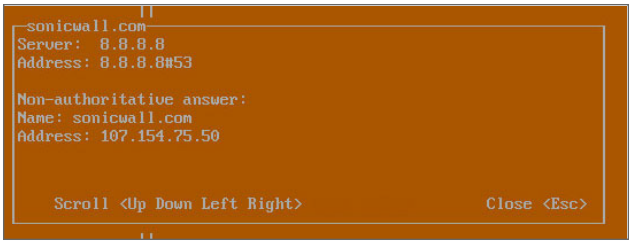
5. Press the **Esc** key to close the dialog.

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**.

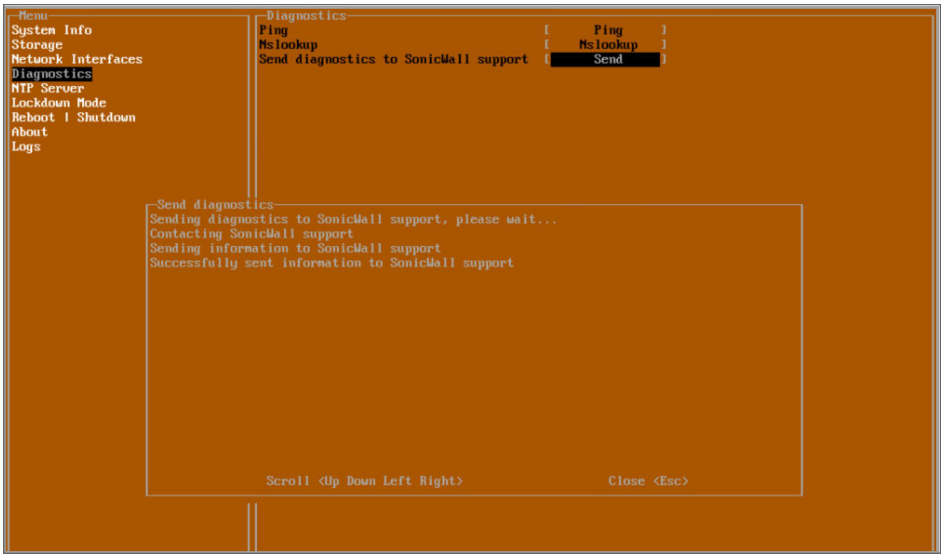
   The Nslookup query results are displayed in an information dialog. You can scroll up and down within the dialog by using the up/down arrow keys.



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.



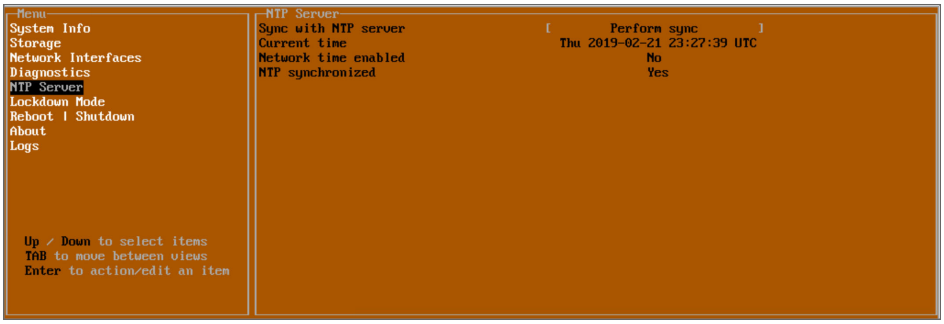
4. Press the **Esc** key to close the dialog.

   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

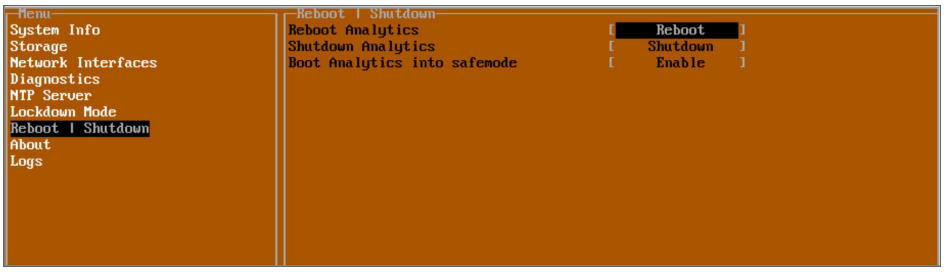


In the **NTP Server** screen, you can synchronize with an NTP server. For complete NTP Server configuration options, log into the SonicOS management interface and navigate to the **MANAGE | Appliance > System Time** page.

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.

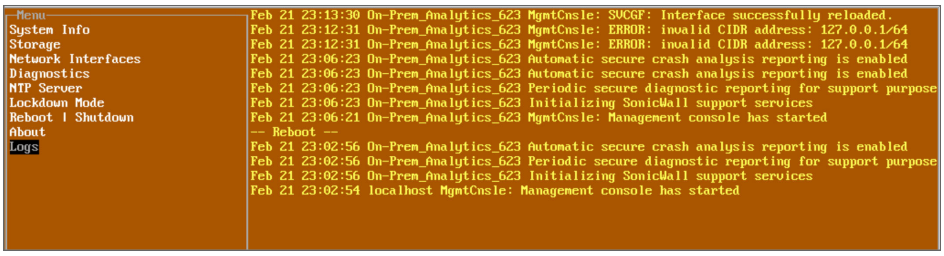
The actions available on the Reboot | Shutdown screen are:

- **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

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

Logs



The **Logs** screen displays log events for the instance.

Using SafeMode on the Management Console

ⓘ | **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.

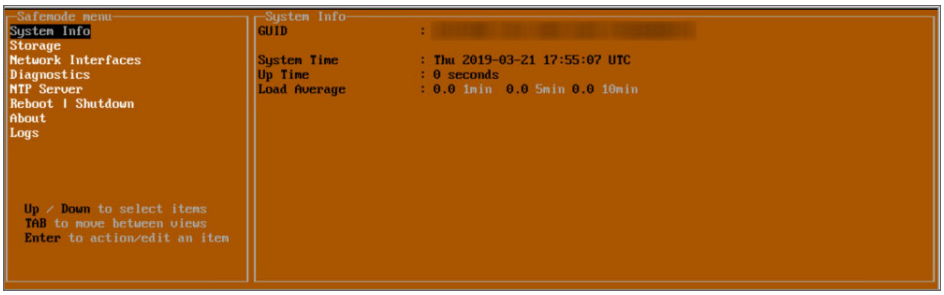
In SafeMode, some of the features the management console provides are different in the following ways:

- Configurable interfaces
- Configurable default gateway

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

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

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



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

Topics:

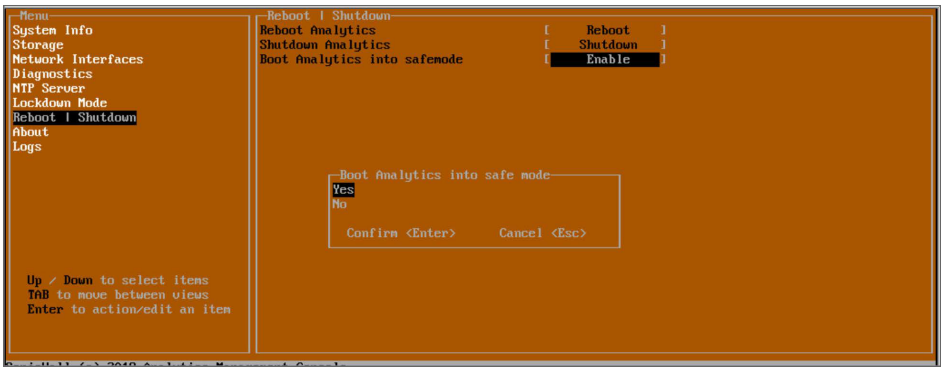
- Enabling SafeMode
- Disabling SafeMode
- Configuring the Network Interfaces in SafeMode
- Installing a Software Upgrade in SafeMode
- Downloading Logs in SafeMode

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**.



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

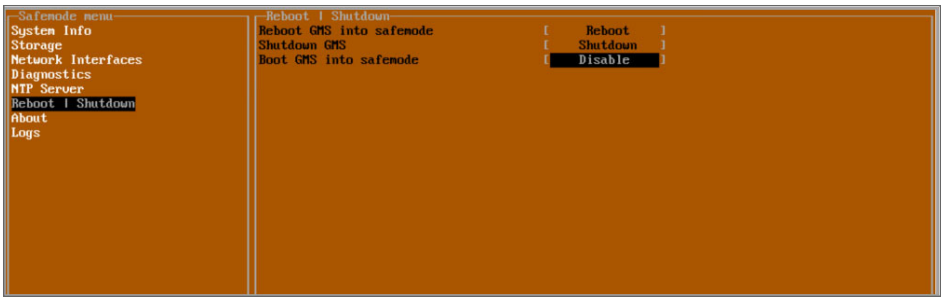
   The On-Premises Analytics instance immediately reboots and comes back up in SafeMode.

   ⓘ **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**.



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 Analtyics 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.

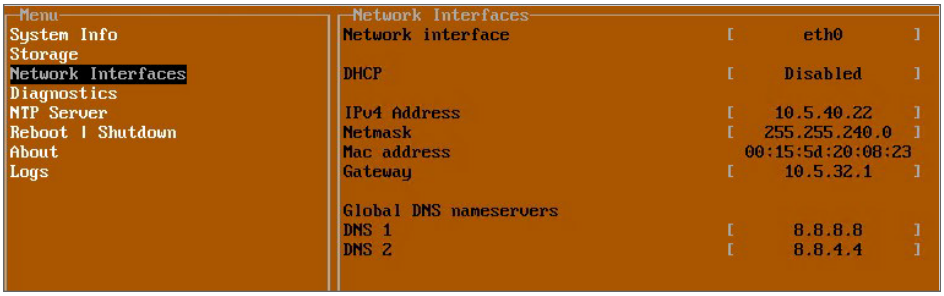
ⓘ | **NOTE:** Changes made to interfaces in SafeMode are not persistent between reboots.

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.



To edit an interface:

1. 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.
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.
3. 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.

ⓘ **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.

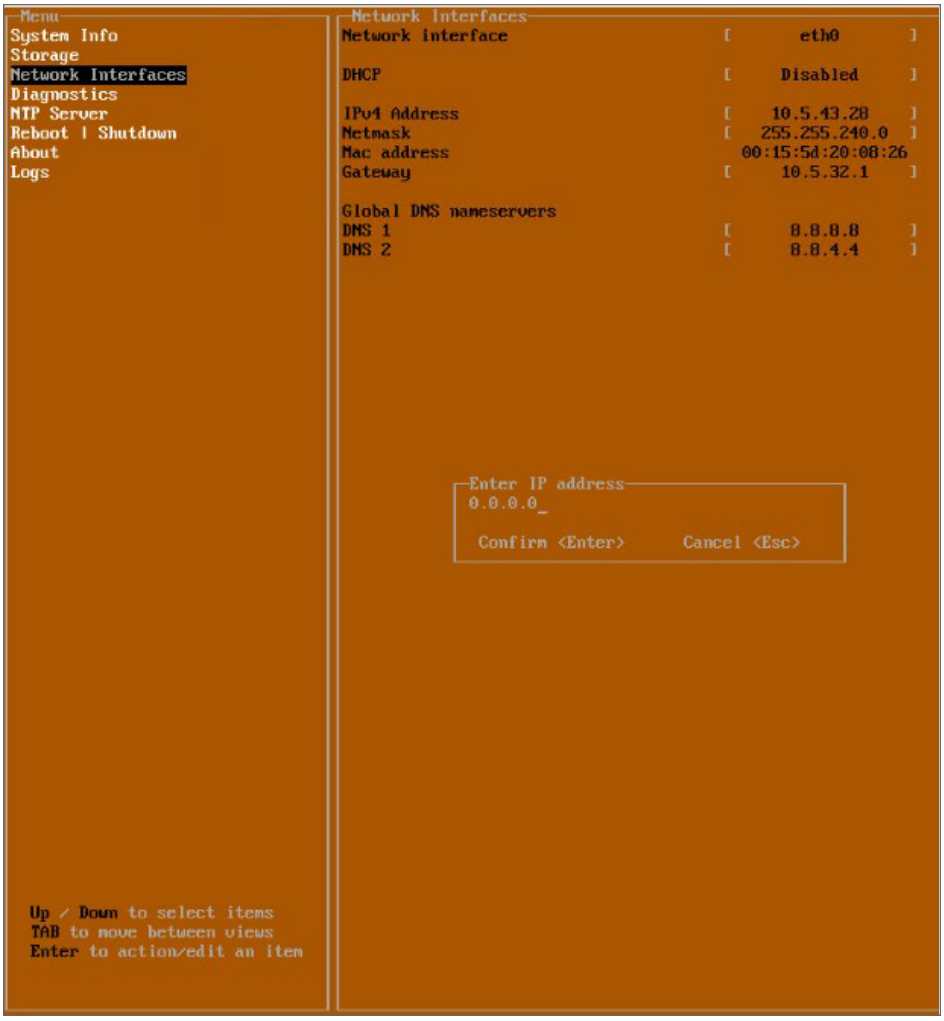
To disable an interface:

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**.



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

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

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.

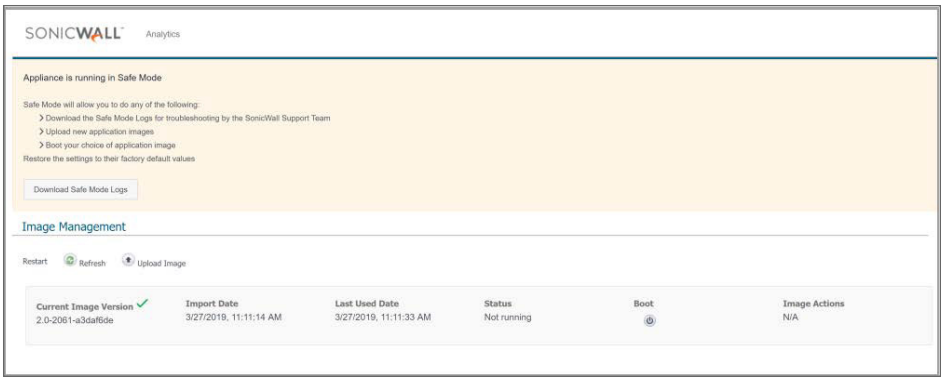
In SafeMode, you can upload a new SWI image and apply it to the On-Premises Analytics instance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the Management Console. When viewing the Management Console in SafeMode, the URL for the SafeMode web interface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

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

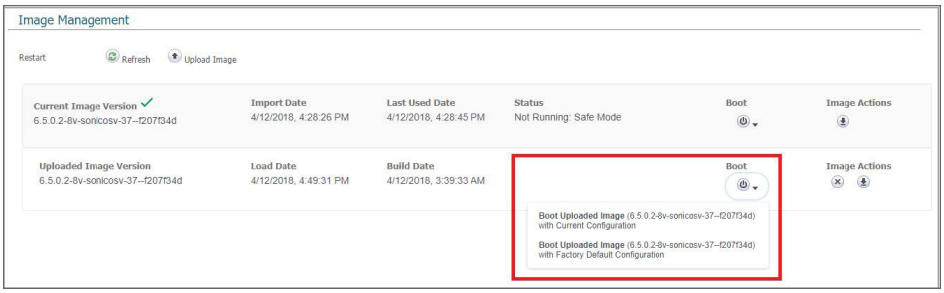
To install a new system image from SafeMode:

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.



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**



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

Downloading Logs in SafeMode

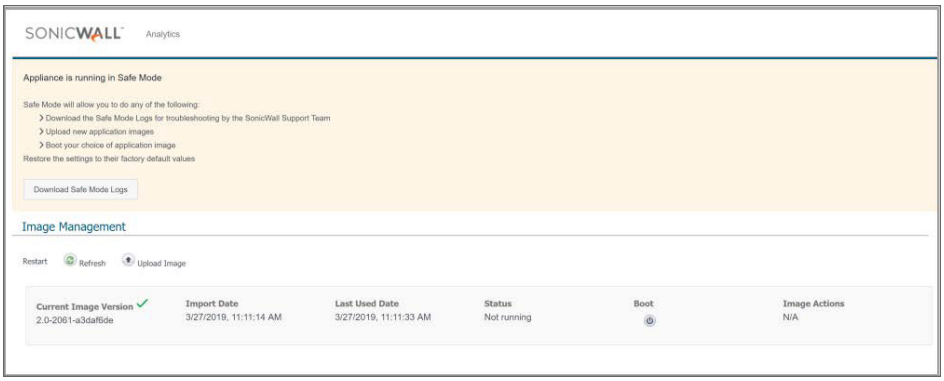
When the On-Premises Analytics instance is in SafeMode, extra logging information is kept that can be downloaded. The logs are available from the SafeMode web management interface, which can be accessed via the URL provided at the bottom of the Management Console screen.

ⓘ | **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.



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.

8

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 Azure
Updated - April 2024
232-004741-00 Rev J

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