SonicWall® On-Premises Analytics

Azure Deployment Guide
Contents

Before Beginning ......................................................... 4
Supported Firewalls .................................................... 5
Additional Firewall Requirements ................................. 5
Azure Requirements .................................................... 5
Licensing Model ........................................................ 6
Capacity Planning ....................................................... 6
Scaling Up ............................................................... 8
Integration with Capture Security Center ......................... 8
Backup and Recovery Information ................................. 9
Best Practices and Recommendations ............................ 9
Creating a MySonicWall Account .................................... 9

Installing On-Premises Analytics on Azure ....................... 11
Task List for On-Premises Analytics ............................... 11
Azure VM Setup ....................................................... 11
Installing On-Premises Analytics on Azure ....................... 12
Configuring On-Premises Analytics on Azure .................... 18
Adding Firewalls to On-Premises Analytics ....................... 32

Licensing and Registering Your On-Premises Analytics Instance ................................. 35
Registering the On-Premises Analytics Instance ................ 35
Deregistering Your On-Premises Analytics Instance .............. 37

Upgrading On-Premises Analytics ..................................... 38

Using the Management Console ..................................... 39
Connecting to the Console ............................................. 39
Management Console Operations .................................... 40
  System Info ....................................................... 42
  Storage .......................................................... 42
  Network Interfaces .............................................. 43
  Diagnostics ....................................................... 43
  NTP Server ...................................................... 45
  Reboot | Shutdown .............................................. 46
  About ........................................................... 46
  Logs .............................................................. 47
Using SafeMode on the Management Console ..................... 47
  Enabling SafeMode .............................................. 48
  Disabling SafeMode ............................................. 48
  Configuring the Network Interfaces in SafeMode .............. 49
  Configuring Interface Settings .................................. 49
  Disabling an Interface .......................................... 51
  Installing a Software Upgrade in SafeMode ...................... 52
Contents

Downloading Logs in SafeMode ................................................................. 53
SonicWall Support ..................................................................................... 54
About This Document ............................................................................. 55
Before Beginning

The SonicWall® Azure Environment for On-Premises Analytics describes how to install SonicWall On-Premises Analytics on Microsoft Azure and provides basic configuration information.

To jump directly to the installation instructions, go to Installing On-Premises Analytics on Azure on page 11.

On-Premises Analytics collects data from firewalls, analyzes it, and presents it as actionable intelligence. For an overview of product features, refer to the SonicWall® On-Premises Analytics Getting Started Guide.

Read this chapter to answer basic questions about installing and managing On-Premises Analytics in an Azure environment.

Chapter 2, Installing On-Premises Analytics on Azure on page 11, details the installation process.

Licensing and Registering Your On-Premises Analytics Instance on page 35 tells how to access serial numbers and authorization codes and how to use them.

For details on upgrading the data handling capacity of your instance, see Upgrading On-Premises Analytics on page 38.

Chapter 4, Management Console Operations on page 40, goes over steps to configure the software and diagnose problems.

This introductory chapter includes:

- Supported Firewalls on page 5
- Additional Firewall Requirements on page 5
- Azure Requirements on page 5
- Backup and Recovery Information on page 9
- Best Practices and Recommendations on page 9
- Creating a MySonicWall Account on page 9
Supported Firewalls

On premises analytics can collect data from the following firewalls:

<table>
<thead>
<tr>
<th>Firewall Type</th>
<th>Models</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entry-Level Firewalls</td>
<td>SOHO W</td>
</tr>
<tr>
<td></td>
<td>TZ Series</td>
</tr>
<tr>
<td></td>
<td>NSv 10 — 100</td>
</tr>
<tr>
<td>Mid-Range Firewalls</td>
<td>NSA 2500—6600</td>
</tr>
<tr>
<td></td>
<td>NSA 2650—6650</td>
</tr>
<tr>
<td></td>
<td>NSv 200 — 400</td>
</tr>
<tr>
<td>High-End Firewalls</td>
<td>SuperMassive 9000 Series</td>
</tr>
<tr>
<td></td>
<td>NSA 9250—9650</td>
</tr>
<tr>
<td></td>
<td>NSv 800—1600</td>
</tr>
</tbody>
</table>

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.
- The firewalls connected to the On-Premises Analytics instance must not be associated with a Cloud GMS 1.0 implementation.
- Firewalls must be added manually, Zero Touch is not supported.
- 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.

Azure Requirements

Hardware settings with Azure for an On-Premises Analytics instance:

- 4 CPUs
- 8 GB Memory
- 68.41 GB disk size (preferably SSDs)
- 2 virtual NICs

An additional external mount of 500 GB of storage is recommended for logs storage. Refer to Configuring On-Premises Analytics on Azure on page 18.

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

**IMPORTANT:** To choose when the day starts, regardless of the deployment location, refer to Azure documentation: [https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview](https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview)

The following table summarizes currently available licensing levels.

<table>
<thead>
<tr>
<th>Storage (based on licenses)</th>
<th>Flows/logs per second or day</th>
<th>Storage Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 GB/day</td>
<td>5 GB/day — 750 logs/sec and 50 million logs/day</td>
<td>1 TB</td>
</tr>
<tr>
<td>15 GB/day</td>
<td>15 GB/day — 2250 logs/sec and 150 million logs/day</td>
<td>5 TB</td>
</tr>
<tr>
<td>30 GB/day</td>
<td>30 GB/day — 4500 logs/sec and 300 million logs/day</td>
<td>10 TB</td>
</tr>
<tr>
<td>100 GB/day</td>
<td>100 GB/day — 15000 logs/sec and 1000 million logs/day</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

1. This is the maximum amount of analyzed data that can be stored, not the maximum amount of external storage supported by the VM.

The following section, **Capacity Planning**, provides capacity planning guidelines and walks through an example.

### Capacity Planning

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

<table>
<thead>
<tr>
<th>Typical Installations</th>
<th>Storage (based on licenses)</th>
<th>Flows/logs per second or day</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 Core, 16 GB</td>
<td>5 GB/day</td>
<td>5 GB/day — 750 logs/sec and 50 million logs/day</td>
</tr>
<tr>
<td>16 Core, 32 GB</td>
<td>15 GB/day</td>
<td>15 GB/day — 2250 logs/sec and 150 million logs/day</td>
</tr>
<tr>
<td>32 Core, 64 GB</td>
<td>30 GB/day</td>
<td>30 GB/day — 4500 logs/sec and 300 million logs/day</td>
</tr>
<tr>
<td>64 Core, 64 GB</td>
<td>100 GB/day</td>
<td>100 GB/day — 15000 logs/sec and 1000 million logs/day</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>VM Hardware Configuration</th>
<th>TZs / SOHOs / NSv low capacity (number of firewalls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Core, 8 GB - default</td>
<td>10&lt;sup&gt;1&lt;/sup&gt;</td>
</tr>
<tr>
<td>8 Core, 16 GB</td>
<td>50</td>
</tr>
<tr>
<td>16 Core, 32 GB</td>
<td>100</td>
</tr>
<tr>
<td>32 Core, 64 GB</td>
<td>200</td>
</tr>
<tr>
<td>64 Core, 64 GB</td>
<td>500</td>
</tr>
</tbody>
</table>

1. Includes all TZ and SOHO models along with NSv models 10 to 100.
The following table shows recommended guidelines for main memory to support different numbers of firewalls.

<table>
<thead>
<tr>
<th>VM Hardware Configuration</th>
<th>NSa / NSv medium capacity (number of firewalls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Core, 8 GB - default</td>
<td>2¹</td>
</tr>
<tr>
<td>8 Core, 16 GB</td>
<td>4</td>
</tr>
<tr>
<td>16 Core, 32 GB</td>
<td>8</td>
</tr>
<tr>
<td>32 Core, 64 GB</td>
<td>16</td>
</tr>
<tr>
<td>64 Core, 64 GB</td>
<td>32</td>
</tr>
</tbody>
</table>

1. Includes NSa 2600-6600, NSv 200-400.

<table>
<thead>
<tr>
<th>VM Hardware Configuration</th>
<th>SM / NSa / NSv high capacity (number of firewalls)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 Core, 8 GB - default</td>
<td>1¹</td>
</tr>
<tr>
<td>8 Core, 16 GB</td>
<td>2</td>
</tr>
<tr>
<td>16 Core, 32 GB</td>
<td>4</td>
</tr>
<tr>
<td>32 Core, 64 GB</td>
<td>8</td>
</tr>
<tr>
<td>64 Core, 64 GB</td>
<td>16</td>
</tr>
</tbody>
</table>

1. Includes SuperMassive 9000 series, NSa 9200-9800, NSv 800-1600.

<table>
<thead>
<tr>
<th>Number of Firewalls</th>
<th>Recommended Amount of Main Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>8 GB</td>
</tr>
<tr>
<td>50</td>
<td>16 GB</td>
</tr>
<tr>
<td>100</td>
<td>32 GB</td>
</tr>
<tr>
<td>500</td>
<td>64 GB</td>
</tr>
</tbody>
</table>

**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.

Likewise, we see that a 4 core, 8 GB can handle IPFIX flows from a single high-capacity firewall such as the NSa 9450.

So, it makes sense to choose the license level associated with 8 cores 16 GB VM. This will support 50 million log entries per day and should cover these six firewalls. 6 cores may suffice, but 8 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 your SonicWall sales representative for further guidance.

Scaling Up

It works well to have one On-Premises Analytics instance supporting all the firewalls in a single product group or tenancy.

However, IPFIX flows can be redirected from an existing instance to an additional one, so multiple On-Premises Analytics instances can support a large single group or tenancy.

Firewalls from different groups or tenancies can send IPFIX data to the same instance, however this may become a problem if there is a future move to integrate firewall management with Capture Security Center. Refer to the following section, Integration with Capture Security Center.

Integration with Capture Security Center

As shown below, Analytics capabilities can be included within a cloud-based Capture Security Center implementation.

NOTE: Contact your SonicWall sales representative for further information.
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 Azure console remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall Technical 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 on page 37 for information.
- If On-Premises Analytics fails to boot, it may still allow access to the Management Console through the Azure remote console. Check the Azure 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 on page 43), and contact SonicWall Technical Support for assistance. For details on using the Management Console, refer to Management Console Operations on page 40.

Best Practices and Recommendations

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

Creating a MySonicWall Account

A MySonicWall account is required for product registration to enable full functionality of SonicOS features, and for access to licensed security services.

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 Complete the account information, including email and password.

4 Follow the prompts to finish creating your account.

5 Click **Finish**.

6 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.

7 Click **Done**. You are returned to the login window so you can log into MySonicWall with your new account.

**Next Steps**

- [Installing On-Premises Analytics on Azure](#) on page 11
- [Licensing and Registering Your On-Premises Analytics Instance](#) on page 35
Installing On-Premises Analytics on Azure

Topics:
- Task List for On-Premises Analytics Azure VM Setup on page 11
- Installing On-Premises Analytics on Azure on page 12
- Configuring On-Premises Analytics on Azure on page 18
- Configuring On-Premises Analytics on Azure on page 18
- Adding Firewalls to On-Premises Analytics on page 32

Task List for On-Premises Analytics Azure VM Setup

The process for setting up an On-Premises Analytics instance on Azure is summarized in three main tasks:

1. Install the On-Premises Analytics instance on Azure
   - Installing On-Premises Analytics on Azure on page 12
2. Register the On-Premises Analytics instance on MySonicWall
   - Registering the On-Premises Analytics Instance on page 35
3. Configure On-Premises Analytics and add firewalls for data collection
   - Configuring On-Premises Analytics on Azure on page 18
Installing On-Premises Analytics on Azure

Once SonicWall’s Analytics product is identified in the marketplace, installing it on your Azure instance is simple.

**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 Analytics from the Azure Market Place.

1. Login into Azure and Navigate to the SonicWall Analytics page in Marketplace. The page appears:

2. Choose to create this application and agree with the End User license agreement as shown
3 Create a Resource Group:

4 Define a Virtual machine name:

5 Continue down the Create a virtual machine page, select region, image, size of VM, and set up a login and password for the VM. Refer to the following table to select VM size.

<table>
<thead>
<tr>
<th>VM Size in Azure</th>
<th>License Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard_D2_v2</td>
<td>5 GB/day</td>
</tr>
<tr>
<td>Standard_D3_v2</td>
<td>15 GB/day</td>
</tr>
<tr>
<td>Standard_D4_v2</td>
<td>30 GB/day</td>
</tr>
<tr>
<td>Standard_D5_v2</td>
<td>100 GB/day</td>
</tr>
</tbody>
</table>
Enter the username as `management` and password for the VM.

6. Click on **Next: Disk** to go on to the Disk page. Setup the amount of persistent memory to allocate to the VM. For guidance on the amount of memory required, refer to **Licensing Model** on page 6.

7. Once an appropriate virtual disk size is defined, go on to the **Networking**, **Management**, and **Advanced** screens. Depending on your Azure application, you may choose to leave the settings on these pages in default values, or use them to meet the requirements of your cloud.
8 When you reach the Review + create screen the system will check that the VM configuration is valid before allowing deployment to the cloud. The system responds with the green band shown below.

9 Deploying the VM will take several minutes. Meanwhile, Azure will indicate:
10. Azure will then indicate deployment complete:

11. Now navigate through **Home> Resource Groups** to the new VM and select the ip parameter file:

Double-click on the .ip file to learn the assigned IP address for the VM. Note it.
12 Click configuration under settings Tab. Be sure to change the address mode from Dynamic to Static. Then click Save.

13 Notifications will now appear to the right of the screen: “Saved public IP address changes” and “Deployment succeeded.”

**IMPORTANT:** Be sure to set the IP address assignment as Static.
Configuring On-Premises Analytics on Azure

1. Setup PuTTY for SSH communication and go to the public IP address noted at the end of the previous section.

   ![PuTTY Configuration](image)

   **NOTE:** The initial boot process may take 10 to 15 minutes.

2. Wait for the software to boot to the command line in the **Virtual Machine Connection** window and then username **management** and the password as determined in **Step 5** in the previous section.
3 When the Management Console appears, go to the **Storage** screen:
4 After selecting **Add Storage**, select Yes and press enter to confirm:

5 Enter the key for encryption and write it down for later reference.
**IMPORTANT:** Be sure to securely store your storage encryption key, you will probably need it to re-configure storage at some point.

6. Click enter to start disk encryption as shown:
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.

**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 of the instance in a web browser. The instance login screen will appear:
10 For initial access, use admin and password.

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 on page 35.

The initialization wizard guides you through the remaining process. It first appears:

---

11 Click on Next.

12 When the Network Settings screen comes up you may choose to change settings.

---

13 Then click on Next.
14 When the **Time Settings** comes up make adjustments if necessary and click **Next**.

![Time Settings screenshot](image1.png)

15 Click **Next** and the system displays a summary screen:

![Summary screenshot](image2.png)

16 To adjust, click on **Back**. Otherwise click **Apply**.
17 When the system asks you to confirm, click on **OK**.
18 The system will indicate success:

19 Click on **Finish** to restart the On-Premises Analytics instance.
20 When the login screen reappears, again use admin and password for access.

21 When the installation wizard appears, click on Next.
22 Click on **Apply** to start configuration.

23 When the system asks for confirmation, click **OK**.
24 Wait for configuration to complete.

The system reports when configuration is complete:
25 Click on **Finish** to restart the system.

You are asked to link to your MySonicWall account:

26 After linking to MySonicWall, provide the Serial Number and Authorization Code from Use a Friendly Name to distinguish from other instances of On-Premises Analytics.
27. After you enter the data as shown below, click **Submit**.

![Registration Form]

28. To confirm your completion of the registration process as below, click **Continue**.

![Registration Success]

29. Now navigate to **System > Administration** to set new login credentials.

![Administration Settings]

---

On-Promises Analytics Azure Deployment Guide

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

To add firewalls:

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

2. Once the Device Manager panel appears, click on the ‘+’ sign to show the Add Firewall dialog box.

3. Fill in the “Friendly name” of the firewall, the serial number and model designation. Click on OK.
4. In another browser window, log into the firewall and then go to **Manage > Appflow Settings | Flow Reporting**:

![Flow Reporting panel](image)

5. In the **Flow Reporting** panel take these steps:
   - Enable **Send AppFlow to SonicWall GMSFlow Server**.
   - Enable **Send Real-Time Data To SonicWall GMSFlow Server**.
6 Now go to Manage > AppFlow Settings | GMS Flow Servers:

![SONICWALL Network Security Appliance](image)

7 In the GMS Flow Server panel take these steps:
   a Enter the IP address of the Analytics instance as the **GMSFlow Server Address** (this is your Analytics deployment IP adress).
   b **IMPORTANT**: When configuration in this panel is complete, click on the Accept button at the bottom of the page.
   c Click on the Test Connectivity button 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.
   8 Repeat Step 2 through Step 7 for every firewall in the **Group** that you wish to analyze data from.
Licensing and Registering Your On-Premises Analytics Instance

Topics:
- Registering the On-Premises Analytics Instance on page 35
- Deregistering Your On-Premises Analytics Instance on page 37

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

![Quick Register Screen](image)
3 If necessary, establish a new product group to support the Analytics instance:

4 Once the product appears in your My Products listing, click on the information icon:

5 When the Product Details box comes up, record the Serial Number and Authorization Code.

6 Enter the Serial Number and Authorization Code into the initialization wizard as you bring up the On-Premises Analytics instance for the first time.
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.
Upgrading On-Premises Analytics

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

**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 on page 52. In the event this step is necessary, please contact SonicWall Technical Support for assistance.

**To upgrade On-Premises Analytics software:**

1. Navigate to Console > Appliance and click on Appliance.

2. Then select System > Settings:

3. Choose the hotfix or service pack and click apply.
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:

- Use SSH or PuTTY to access the public IP address of the On-Premises Analytics instance.
- 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 in Step 2.

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. The Management Console can be accessed by logging into the **Azure Virtual Machine Connection**.
To access and navigate the Management Console:

1. Log into the Azure manager, select your On-Premises Analytics, and right-click on Connect. Use Ctrl and S keys with the space bar to bring up the console. See Step 3 above.

2. The Management Console will appear:

3. The main menu is displayed in the side menu (left 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.

4. Press the Tab key to move the focus from side menu to the main view (right pane), or vice versa.

5. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.

6. 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:

7. 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
- 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.
Network Interfaces

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

- **Network Interface** – This is the current interface serving as the management interface. This defaults to ens160.
- **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.

```
Ping host
PING 0.0.0.0 (0.0.0.0) 56(84) bytes of data.
64 bytes from 0.0.0.0: icmp_seq=1 ttl=60 time=19.5 ms
64 bytes from 0.0.0.0: icmp_seq=2 ttl=60 time=18.6 ms
--- 0.0.0.0 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 18.653/19.143/19.594/0.471 ms
```

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.

```
sonicwall.com
Server: 0.0.0.0
Address: 0.0.0.0

Non-authoritative answer:
Name: sonicwall.com
Address: 10.7.154.75.50
```

5 Press the Esc key to close the dialog.

**To send Diagnostic Report**

In the Diagnostics screen, you can send diagnostics to SonicWall Technical Support.

**NOTE:** Your On-Premises Analytics instance must have internet access to send the diagnostics report to SonicWall Support.
To send the diagnostics report, 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.

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-Premises Analytics instance is currently synchronized with the configured NTP server(s).

### Reboot | Shutdown

![Reboot | Shutdown screen](image)

The **Reboot | Shutdown** screen provides functions for rebooting the instance, returning to factory defaults, and enabling SafeMode. To perform an action, position the focus 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 GMS** – Restarts the instance with current configuration settings.
- **Shut down GMS** – Powers off the instance.
- **Boot with factory default settings** – Restarts the instance using factory default settings. All configuration settings will be erased.
- **Boot GMS into safemode** – Puts the On-Premises Analytics instance into SafeMode. In this product, SafeMode does not offer additional functionality.

### About

![About screen](image)

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 On-Premises Analytics 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 Disabling SafeMode on page 48 for more information.
Topics:

- Enabling SafeMode
- Disabling SafeMode
- Configuring the Network Interfaces in SafeMode

## Enabling SafeMode

SafeMode can be enabled from the management console.

**To enable SafeMode:**

1. Access the On-Premises Analytics Management Console through the Azure remote console.
2. In the console, select the **Reboot | Shutdown** option and then press **Enter**.
3. Navigate down to the **Boot SonicWall 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 SonicWall 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 Analytics interfaces:

- **Network Interface** – This is the currently selected interface. This defaults to `ens160`. Use this to select any of the On-Premises Analytics interfaces.
- **D H C P** – Determines whether addressing is static or handled automatically and dynamically by a DHCP server.
- **I P v 4 A d d r e s s** – The current IPv4 address currently assigned to the Management Interface.
- **N e t m a s k** – The current Netmask assigned to the Management Interface.
- **M a c A d d r e s s** – The MAC address of the Management Interface.
- **I P v 6 A d d r e s s** – The currently assigned IPv6 address of the Management Interface.
- **G a t e w a y** – The current Default Gateway currently in use by the On-Premises Analytics instance.
- **D N S** – 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.

### 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.
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 interfaces 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.
3. For example, select IPv4 Address and press Enter.
   
   The on-screen dialog displays the current IP address.
4. Navigate into the dialog and change the IP address to 0.0.0.0, then press Enter.
   
   The Save changes button is displayed.
5. Press Tab to navigate to the Save changes button and then press Enter.
The interface is disabled:

![On-Premises Analytics Azure Deployment Guide - Using the Management Console](image)

**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 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.
Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.
About This Document

Legend

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

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

💡 IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

On Premises Analytics Azure Deployment Guide
Updated - January 2020
Software version - 2.0.2
232-004741-00 Rev B

Copyright © 2020 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

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

End User Product Agreement

Open Source Code
SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035

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