SonicWall® SonicOSX 7 NSv Series on Azure

Getting Started Guide
# Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Introducing NSv Series</strong></td>
<td>4</td>
</tr>
<tr>
<td>Feature Support Information</td>
<td>5</td>
</tr>
<tr>
<td>Product Matrix and Requirements</td>
<td>7</td>
</tr>
<tr>
<td>Github Repository</td>
<td>8</td>
</tr>
<tr>
<td>Backup and Recovery Information</td>
<td>8</td>
</tr>
<tr>
<td>Exporting and Importing Firewall Configurations</td>
<td>9</td>
</tr>
<tr>
<td>Upgrading from SonicOS 6.5</td>
<td>9</td>
</tr>
<tr>
<td>Upgrading to a Higher Capacity NSv Model</td>
<td>9</td>
</tr>
<tr>
<td>Creating a MySonicWall Account</td>
<td>9</td>
</tr>
<tr>
<td><strong>Installing NSv Series on Azure</strong></td>
<td>11</td>
</tr>
<tr>
<td>Supported NSv Series Models on Azure</td>
<td>11</td>
</tr>
<tr>
<td>Task List for NSv Azure VM Setup</td>
<td>12</td>
</tr>
<tr>
<td>Installing NSv on Azure</td>
<td>12</td>
</tr>
<tr>
<td>Accessing Your NSv in the Azure Portal</td>
<td>25</td>
</tr>
<tr>
<td>Updating Your Dashboard and Accessing the NSv Resource Group</td>
<td>25</td>
</tr>
<tr>
<td>Finding the Public IP Address of Your NSv</td>
<td>26</td>
</tr>
<tr>
<td>Logging into Your NSv for SonicOS Management</td>
<td>26</td>
</tr>
<tr>
<td>Viewing and Configuring Security Rules</td>
<td>27</td>
</tr>
<tr>
<td>Forwarding Traffic to Your NSv in Azure</td>
<td>29</td>
</tr>
<tr>
<td>Testing Traffic Through Your NSv in Azure</td>
<td>33</td>
</tr>
<tr>
<td>Troubleshooting Installation Configuration</td>
<td>35</td>
</tr>
<tr>
<td><strong>Licensing and Registering Your NSv</strong></td>
<td>37</td>
</tr>
<tr>
<td>Registering the NSv Appliance from SonicOS</td>
<td>37</td>
</tr>
<tr>
<td><strong>SonicOS Management</strong></td>
<td>39</td>
</tr>
<tr>
<td>Managing SonicOS on the NSv Series</td>
<td>39</td>
</tr>
<tr>
<td>Using System Diagnostics</td>
<td>39</td>
</tr>
<tr>
<td><strong>Using the Virtual Console</strong></td>
<td>41</td>
</tr>
<tr>
<td>Connecting to the Console with SSH</td>
<td>41</td>
</tr>
<tr>
<td>Navigating the NSv Management Console</td>
<td>43</td>
</tr>
<tr>
<td>System Info</td>
<td>45</td>
</tr>
<tr>
<td>Management Network or Network Interfaces</td>
<td>46</td>
</tr>
<tr>
<td>Test Management Network</td>
<td>47</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>48</td>
</tr>
<tr>
<td>NTP Server</td>
<td>49</td>
</tr>
<tr>
<td>Lockdown Mode</td>
<td>50</td>
</tr>
<tr>
<td>System Update</td>
<td>51</td>
</tr>
<tr>
<td>Reboot</td>
<td>Shutdown</td>
</tr>
<tr>
<td>About</td>
<td>52</td>
</tr>
<tr>
<td>Logs</td>
<td>52</td>
</tr>
</tbody>
</table>

---

SonicWall NSv Series Azure Getting Started Guide

Contents | 2
### Using SafeMode on the NSv

- **Enabling SafeMode**
- **Disabling SafeMode**
- **Configuring the Management Network in SafeMode**
- **Installing a New SonicOS Version in SafeMode**
- **Downloading Logs in SafeMode**

### SonicWall Support

### About This Document
Introducing NSv Series

This SonicWall® NSv Series on Azure Getting Started Guide describes how to install SonicWall NSv on Microsoft Azure and provides basic configuration information.

To jump directly to the installation instructions, go to Installing NSv Series on Azure on page 11.

SonicWall NSv on Azure Marketplace

The SonicWall® Network Security Virtual Series (SonicWall® NSv Series) is SonicWall’s virtualized next-generation firewall appliance that provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. SonicOS running on the NSv Series offers the feature functionality and security features of a physical appliance, with comparable performance. SonicOS Virtual is a fully featured 64-bit SonicOS powered by SonicCore.

Topics:

- Feature Support Information on page 5
- Product Matrix and Requirements on page 7
- Github Repository
- Backup and Recovery Information
- Exporting and Importing Firewall Configurations on page 9
- Upgrading from SonicOS 6.5
- Upgrading to a Higher Capacity NSv Model
- Creating a MySonicWall Account on page 9
Feature Support Information

The Feature Support List table lists key SonicOS features and whether or not they are supported in deployments of the NSv Series. The SonicWall NSv Series for Azure has nearly all the features and functionality of a SonicWall NSA hardware appliance running SonicOSX 7 firmware.

For information about supported features, go to the technical publications portal. The Feature Support List of NSv for Azure table lists the key SonicOSX 7 features.

### Feature Support List

<table>
<thead>
<tr>
<th>Functional Category</th>
<th>Feature Area</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unified Security Policy</strong></td>
<td><strong>Unified Policy combining Layer 4 to Layer 3 Rules</strong></td>
<td>Source/Destination IP/Port/Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Application based Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CFS/Web Filtering</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Botnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Geo-IP/country</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single Pass Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Services enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Decryption Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DoS Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EndPoint Security Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rule Diagram</td>
</tr>
<tr>
<td></td>
<td><strong>Profile Based Objects</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Endpoint Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bandwidth Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QoS Marking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Content Filter</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intrusion Prevention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DHCP Option</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AWS VPN</td>
</tr>
<tr>
<td></td>
<td><strong>Action Profiles</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Profile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DoS Profile</td>
</tr>
<tr>
<td></td>
<td><strong>Signature Objects</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AntiVirus Signature Object</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AntiSpyware Signature Object</td>
</tr>
<tr>
<td></td>
<td><strong>Rule management</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shadow rule analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In-cell editing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group editing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Export of Rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LiveCounters</td>
</tr>
</tbody>
</table>
### Feature Support List

<table>
<thead>
<tr>
<th>Functional Category</th>
<th>Feature Area</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Managing views</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Used/un-used rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Active/in-active rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sections</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customizable Grid/Layout</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom Grouping</td>
<td></td>
</tr>
<tr>
<td><strong>TLS 1.3</strong></td>
<td>Supporting TLS 1.3 with enhanced security</td>
<td></td>
</tr>
<tr>
<td><strong>SDWAN</strong></td>
<td>SDWAN Scalability</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDWAN Usability Wizard</td>
<td></td>
</tr>
<tr>
<td><strong>API</strong></td>
<td>API Driven Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full API Support</td>
<td></td>
</tr>
<tr>
<td><strong>Dashboard</strong></td>
<td>Enhanced Home Page</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Actionable Dashboard</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enhanced Device View</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Top Traffic and User summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insights to threats</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy/Object Overview</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Profiles and Signatures Overview</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Zero-Day Attack Origin Analysis</td>
<td></td>
</tr>
<tr>
<td><strong>Debugging</strong></td>
<td>Enhanced Packet Monitoring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UI based System Logs Download</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SSH Terminal on UI</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System Diagnostic Utility Tools</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Policy Lookup</td>
<td></td>
</tr>
<tr>
<td><strong>Capture Threat Assessment (CTA 2.0)</strong></td>
<td>Executive Template</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Customizable Logo/Name/Company</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Industry and Global Average Statistics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risky File Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risky Application Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Malware Analysis</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Glimpse of Threats</td>
<td></td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>Risky Application Summary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enhanced AppFlow Monitoring</td>
<td></td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>CSC Simple Reporting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ZeroTouch Registration and Provisioning</td>
<td></td>
</tr>
</tbody>
</table>
Feature Support List

<table>
<thead>
<tr>
<th>Functional Category</th>
<th>Feature Area</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>SonicCoreX and SonicOS Containerization</td>
<td>Data Encryption using AES-256</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enhanced Online Help</td>
</tr>
</tbody>
</table>


For information about supported features, refer to the SonicOS 7 NSv Series administration documentation. This and other documents for the SonicWall NSv Series are available by selecting NSv Series as the Product at: [https://www.sonicwall.com/support/technical-documentation](https://www.sonicwall.com/support/technical-documentation).

Product Matrix and Requirements

The following table shows the hardware resource requirements for the SonicWall NSv Series virtual appliances.

<table>
<thead>
<tr>
<th>Product Models</th>
<th>NSv 270</th>
<th>NSv 470</th>
<th>NSv 870</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Cores¹</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Minimum Total Cores</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Management Cores</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Maximum Data Plane Cores</td>
<td>1</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>Minimum Data Plane Cores</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Network Interfaces</td>
<td>2</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Supported IP/Nodes</td>
<td>No limit</td>
<td>No limit</td>
<td>No limit</td>
</tr>
<tr>
<td>Minimum Memory Required</td>
<td>6G²</td>
<td>8G</td>
<td>10G</td>
</tr>
<tr>
<td>Minimum Hard Disk/Storage</td>
<td>35G</td>
<td>35G</td>
<td>35G</td>
</tr>
</tbody>
</table>

¹ If the actual number of cores allocated exceeds the number of cores defined in the above table, extra cores will be used as CPs.

² Memory requirements are higher with Jumbo Frames enabled. See the Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled table.

On NSv Azure deployments with Jumbo Frame support enabled, the Minimum Memory requirements are higher. This increases TCP performance. See the Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled table below.
Github Repository

SonicWall NSv Azure templates are available in the github repository:

- https://github.com/sonicwall
- https://github.com/sonicwall/sonicwall-nsv-azure-templates

Backup and Recovery Information

In certain situations, it might be necessary to contact SonicWall Technical Support, use SafeMode, or deregister the NSv appliance:

- If the splash screen 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 NSv appliance needs to be deregistered with MySonicWall. See Deregistering Your NSv on page 42 for information.
- If SonicOS does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS image, or take other actions. For information about SafeMode, see Using SafeMode on the NSv on page 52.
- If SonicOS fails three times during the boot process, it will boot into SafeMode. Verify that the minimum required memory is available and allocated based on the NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

Exporting and Importing NSv Configurations

Moving configuration settings from SonicWall physical appliances to the NSv Series is not supported. However, configuration settings may be moved from one NSv to another. Contact SonicWall technical support for assistance.
Exporting and Importing Firewall Configurations

Moving configuration settings from SonicWall physical appliances to the NSv Series is not supported. However, configuration settings may be moved from one SonicOSX 7 NSv to another.

Go to https://www.sonicwall.com/support/technical-documentation/ for more information about exporting and importing configuration settings. Search for SonicOSX 7 updates and upgrades.

Upgrading from SonicOS 6.5

SonicOSX 7 NSv for Azure supports only fresh deployments. Under SonicOSX 7, NSv virtual firewalls support only Unified Policy. Settings from SonicOS 6.5 NSv installations cannot be imported. Users must manually navigate policies, application rules, and content filtering rules for SonicOSX 7 NSv installations. Note that there are console, API and GUI approaches to completing these configurations.

Upgrading to a Higher Capacity NSv Model

It is possible to move up to a higher capacity NSv model, but not down to a lower capacity model. Go to https://www.sonicwall.com/support/technical-documentation/ and search for SonicOSX 7 updates and upgrades.

For details on the number of process and memory to allocate to the VM to upgrade, refer to Product Matrix and Requirements on page 7.

Creating a MySonicWall Account

A MySonicWall account is required to obtain the image file for initial installation of the NSv Series virtual firewall, for product registration to enable full functionality of SonicOS features, and for access to licensed security services. For a High Availability configuration, MySonicWall provides a way to associate a secondary NSv that can share security service licenses with your primary appliance.

| 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.

   **NOTE:** Your password must be at least 8 characters, but no more than 30 characters.

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. Once the code is scanned, you need only click on a button.

6 Click on **CONTINUE** to go to the **Company** page.

7 Complete the company information and click **CONTINUE**.

8 On 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 **DONE**.

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.

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

**Next Steps**

- **Installing NSv Series on Azure** on page 11
- **Licensing and Registering Your NSv** on page 37
Installing NSv Series on Azure

Topics:
- Supported NSv Series Models on Azure on page 11
- Task List for NSv Azure VM Setup on page 12
- Installing NSv on Azure on page 12
- To install from Azure Marketplace: on page 12
- To Install from an Azure template: on page 20
- Accessing Your NSv in the Azure Portal on page 25
- Forwarding Traffic to Your NSv in Azure on page 29
- Testing Traffic Through Your NSv in Azure on page 33
- Troubleshooting Installation Configuration on page 35

Supported NSv Series Models on Azure

<table>
<thead>
<tr>
<th>SonicWall NSv Model</th>
<th>Azure</th>
<th>Interface Count¹</th>
<th>Core Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSv 270</td>
<td>Standard D2 v2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>NSv 470</td>
<td>Standard D3 v2</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>NSv 870</td>
<td>Standard D4 v2</td>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>

¹ The maximum number of interfaces supported on an NSv instance is defined by the type of Azure VM. For example, if more than 2 interfaces are required for an NSv 270, use the NSv 270 with an Azure VM supporting a higher number of interfaces.

**NOTE:** The maximum number of NICs supported by SonicWall NSv is always eight for all models. But the total number of interfaces in an NSv instance may be constrained by the Azure VM.

For Azure sizing and pricing information, see:
- [https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general)
Task List for NSv Azure VM Setup

The process for setting up an NSv Azure virtual firewall is summarized in three main tasks:

1. Install the NSv Azure virtual firewall
   - Installing NSv on Azure on page 12
2. Register the NSv on MySonicWall
   - Registering the NSv Appliance from SonicOS on page 37
3. Configure traffic forwarding to the NSv
   - Forwarding Traffic to Your NSv in Azure on page 29
   - Testing Traffic Through Your NSv in Azure on page 33

Installing NSv on Azure

SonicWall NSv is deployed on Azure by using a solution template. The template is a JSON file which is loaded into Azure via a web page. Templates are a means to deploy VMs in Azure while also creating/modifying existing resources. Templates use the Azure Resource managers to support not just the deployment of the NSv but also of other virtualized network functions.

This section details two deployment procedures:

- To install from Azure Marketplace: on page 12
- To Install from an Azure template: on page 20

To install from Azure Marketplace:

1. In your browser, navigate to https://portal.azure.com/ and log into your Microsoft Azure account.


3. On the SonicWall NSv (Firewall/Security/VPN/Router)-BYOL page, click Create at the bottom to get started.
The Basics screen of the NSv configuration window is displayed.

4 On the Basics screen, configure the following options:

- **VM Name** – Type in a descriptive name for this NSv instance. Consider using lowercase letters, numbers and hyphens, as this name is used to create the default DNS Prefix which has some restrictions. You can, however, adjust the DNS Prefix as needed.

![Basics screen](image)

**NOTE:** The **SSH username** is set to **management** by default. This is the user name for accessing the NSv console using SSH. This is not the NSv administrator user name, but is a user name created as part of an NSv Azure deployment.

- **Authentication type** – Select either **SSH public key** or **Password** as the authentication method for the above management **SSH username**. The default for the template is **Password**.
  
  - If you selected **Password** for Authentication Type, type the desired password into the **Password** and **Confirm password** fields. The password must be between 12 and 72 characters in length and contain at least three of the following character types:
    - Uppercase character
    - Lowercase character
    - Number
    - Special character (non-alpha-numeric, e.g. !@#$%^&*()_+{}|:"<>?)
  
  - If you selected **SSH public key** for Authentication Type, type the SSH RSA public key file name as a string into the **SSH Public Key** field.

- **Subscription** – Select the Azure subscription on which to deploy the resources for this NSv instance.
• **Resource group** – *Create new* or select an existing resource group from the list.

A resource group is a user defined friendly name for a collection of resources. If you are deploying on Azure for the first time, click *Create new*. If you already have a network configured and some virtual machines, then you might wish to use an existing resource group. If you are deploying for test purposes, consider creating a new resource group so you can easily delete the resources, if needed.

- If you select *Create new*, type a name for this resource group into the associated text field, and then select a location for it from the *Location* drop-down list.
- If you select *Use existing*, select the resource group to use from the associated drop-down list.

• **Location** – Select the Azure location where the resources will be deployed.

5 Click **OK** to continue.

The *Instance Details* screen is displayed.

6 Select *Virtual machine size*, then select the row with the Azure equivalent for the NSv model you want to deploy in the *Choose a size* screen. Click **Select**.

<table>
<thead>
<tr>
<th>VM Size in Azure</th>
<th>NSv Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard_D2_v2</td>
<td>NSv 270</td>
</tr>
<tr>
<td>Standard_D3_v2</td>
<td>NSv 470</td>
</tr>
<tr>
<td>Standard_D4_v2</td>
<td>NSv 870</td>
</tr>
</tbody>
</table>
7 Select **Virtual Network** to configure the virtual network. **Create new** under **Choose virtual network** is selected by default and the **Create virtual network** settings are displayed.

Under **Create virtual network**:

- **Name** – This is the name of virtual network the NSv will be deployed on. Leave the default, **VNET**.
- **Address space** – The template default is **10.1.0.0/16**. This is a network address in CIDR format representing the virtual network address space. Accept the default or optionally configure a different address space, using the same format.

8 Click **OK**.
9 Select Subnets to configure the subnets for the WAN and LAN zones.

- **WAN subnet name** – The name of the WAN subnet. The default is **WAN**. If you have an existing network on Azure you may wish to change the value.

- **WAN subnet address prefix** – A sub-network of the Address space configured in Step 7, defined for WAN traffic. e.g. **10.1.0.0/24**.

- **LAN subnet name** – The name of the LAN subnet. The default is **LAN**. If you have an existing network on Azure you may wish to change the value.

- **LAN subnet address prefix** – A sub-network of the Address space configured in Step 7, defined for LAN traffic. e.g. **10.1.1.0/24**.

10 Click OK.

11 Select Public IP Address. Create new is selected by default and the Create public IP address settings are displayed. You also have the option to select an existing public IP address to reassign it for use with your NSv.

- Under Create public IP address, accept the pre-populated name or type a different name into the Name field.
• For SKU, select Basic or Standard. The default is Basic.
• For Assignment (if displayed), select Dynamic or Static. The default is Dynamic.

12 Click OK.

13 In the DNS Prefix for the public IP Address field, configure the DNS name for the NSv. This must be a unique DNS name for accessing the management interface of the NSv virtual firewall. When the NSv VM is created, the WAN will have a public IP and will be assigned the DNS name defined here.

14 In the Management source IP field, type in the public IP address that is allowed to access this NSv virtual firewall for HTTPS and SSH management.

You can find out your public IP address by typing what is my IP into Google or another search engine in a different browser window/tab. Additional addresses can be added later in Azure.

15 Select Storage Account. Create new is selected by default, displaying the Create storage account settings. You also have the option to select an existing storage account.
• For a new storage account, type in a unique **Name** for the storage account using only lowercase letters and numbers.

• Select the desired options for **Account kind**, **Performance**, and **Replication**.

• Click **OK**.

16 Click **OK** at the bottom of the **Instance Details** pane.

The **Summary** screen is displayed.

17 Confirm the settings and then click **OK**.
The **Buy** screen is displayed.

18 Read the Azure **Terms of use** | privacy policy and then click **Create** to agree to the terms and purchase the Azure NSv instance.

Azure begins the deployment process and displays the Azure **Dashboard** page.
You can click the **Notifications** icon at the top to display the **Deployment in progress** notification window, then click **Deployment in progress** to view the progress.

When finished, the notification window displays **Deployment succeeded**.

See **Accessing Your NSv in the Azure Portal** on page 25 for information about accessing the pages and settings for your NSv virtual machine available in the Azure portal.

The next step is to register your NSv virtual firewall on MySonicWall. See **Registering the NSv Appliance from SonicOS** on page 37 for information about registering your NSv.

Once you have registered the NSv, see **Forwarding Traffic to Your NSv in Azure** on page 29 and **Testing Traffic Through Your NSv in Azure** on page 33 for information about forwarding traffic to it.

**To Install from an Azure template:**

Templates are a means to deploy VMs in Azure while also creating/modifying exiting resources. There are a few different types of templates: Quick, Solution and Simple. The below is an example of a Simple template which creates the following resources and defines their interconnections.

- Virtual Machine
- Storage Group
- Public IP
- 2 x Network Interfaces
Installing NSv Series on Azure

**Deploying NSv via Templates**

1. Log into Azure.
2. Click to load the webpage: [https://github.com/sonicwall/sonicwall-nsv-azure-templates](https://github.com/sonicwall/sonicwall-nsv-azure-templates)
3. Click the **Deploy to Azure Button**: ![Deploy to Azure](deploy-button.png)
4. The **Custom Deployment** page should come up:

   ![Custom Deployment Page](custom-deployment.png)

Enter information to define the custom deployment:

- **Resource Group**: The user-defined friendly name for a group of resources.
  
  If you are deploying on a Azure for the first time you will need use “Create New,” however if you already have a network configured, and some virtual machines then you may wish to use an existing resource group. If you are deploying for test purposes, we suggest you create a new resource group so you can easily delete the resources if needed.

- **Location**: The region where you wish to deploy.

- **Storage Account**: A new or existing storage account (we recommend you create a new storage account).

- **Storage Account Type**: The type of storage account you wish to use or create.

  Currently only “Standard_LRS” is recommended.

- **Storage Account New or Existing**: Whether you wish to create or use an existing storage account.

- **User Storage Container Name**: The name of the container where the VHD file will be stored.

- **DNS Name for Public IP**: When the NSv VM is created the WAN will have a public IP, this WAN IP will be assigned a DNS name defined here.

- **SSH User Name**: The user name required to SSH into the NSv appliance.
This is not the NSv administrator’s user name, but rather a username created as part of an NSv Azure deployment.

- **Authentication Type:** Select either "password" or "sshPublicKey" as the authentication method.

- **SSH Password:** The password for the above SSH user.
  
  Password must contain one non alpha-numeric character (e.g. !@#$%^&*()_+{}|: >?<), one uppercase alpha-numeric character and one numeric character.

- **Management Access IP Source:** Public IP address to allowed access to SonicWall NSv HTTPS & SSH management.

- **VM Size:** Select the VM you wish to deploy:

<table>
<thead>
<tr>
<th>SonicWall NSv Model</th>
<th>Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSv 270</td>
<td>Standard D2 v2</td>
</tr>
<tr>
<td>NSv 470</td>
<td>Standard D3 v2</td>
</tr>
<tr>
<td>NSv 870</td>
<td>Standard D4 v2</td>
</tr>
</tbody>
</table>

- **Base Url:** This is the location of the template resources.
  
  This should remain at the default value unless you are creating your own template.

- **Virtual Network Name:** The name of the virtual network the NSv will be deployed on.
  
  If you have an existing network on Azure, and wish to install the NSv on this network then this field should be populated with the network name. e.g. 192.168.0.0/26

- **Virtual Network Address Prefix:** The virtual network "Address space".

- **Subnet WAN Name:** The name of the WAN subnet.
  
  If you have an existing network on Azure you may wish to change the default value else it can remain at default.

- **Subnet LAN Name:** The name of the LAN subnet.
  
  If you have an existing network on Azure you may wish to change the default value else it can remain at default.

- **Subnet WAN prefix:** A sub network of the above "Virtual Network Address Prefix" defined for WAN traffic. e.g. 192.168.1.0/24

- **Subnet LAN prefix:** A sub-network of the above "Virtual Network Address Prefix" defined for LAN traffic. e.g. 192.168.2.0/24

- **Subnet WAN Start Address:** The starting address from which the virtual network will provide via DHCP addresses to host on the WAN subnet.

- **Subnet LAN Start Address:** The starting address from which the virtual network will provide via DHCP addresses to host on the LAN subnet.
5. After filling in all the values you will need to click "I agree to the terms and conditions stated above" then click the "Purchase" button in order to deploy the template and create the SonicWall NSv instance.

It will take approximately 10 minutes to deploy NSv respective resources. You can view the progress by clicking the icons indicated below:
6 To connect to the SonicWall NSv management GUI click “Virtual Machines” from the left hand menu. Then select the NSv VM name, in the overview section a public IP address is displayed, in the example below, that is http://40.76.216.87/

![Image showing SonicWall NSv management GUI](image.png)

7 Login with the default SonicWall credentials “admin/sonicwall”.

![Image showing SonicWall login](image2.png)

8 Now continue with the following section, Accessing Your NSv in the Azure Portal, or go on to Installing NSv Series on Azure on page 11.
Accessing Your NSv in the Azure Portal

There are a number of pages and settings for your NSv virtual machine available in the Azure portal.

Topics:

- **Updating Your Dashboard and Accessing the NSv Resource Group** on page 25
- **Finding the Public IP Address of Your NSv** on page 26
- **Logging into Your NSv for SonicOS Management** on page 26
- **Viewing and Configuring Security Rules** on page 27

Updating Your Dashboard and Accessing the NSv Resource Group

The notification window for **Deployment succeeded** provides two buttons for your immediate use.

- Click the **Pin to dashboard** button to add links to your new NSv and its Azure configuration pages to your Azure **Dashboard** page. Click **Refresh** on the **Dashboard** page to view your new virtual machine, storage account, and network interface on the **Dashboard**.

---

SonicWall NSv Series Azure Getting Started Guide

Installing NSv Series on Azure
• Click Go to resource group to display the Resource group page.

Finding the Public IP Address of Your NSv

On the Dashboard page or the Resource group page, click the VM name link to display the Public IP address of your NSv virtual firewall. The VM name link has a description or type of Virtual machine.

**TIP:** Log into the NSv at the displayed public IP address for SonicOS management and to register the NSv on MySonicWall.

Logging into Your NSv for SonicOS Management

To log into your NSv for SonicOS management:

1. In the left navigation pane of Azure, click Virtual Machines.
2. Click the name of your NSv.
3 In the **Overview** screen, the IP address of the NSv is displayed under **Public IP address**.

4 Point your browser to **https://<Public IP address>**, using the public IP address of your NSv.

5 Log into SonicOS (default credentials: *admin/password*).

### Viewing and Configuring Security Rules

On the **Dashboard** page or the **Resource group** page, click the **NSG** link to view the inbound and outbound security rules. The NSG link has a description or type of **Network security group**.

The inbound rules control management access to the NSv. The Source for these rules is initially set to your public IP address, that you entered during the installation process for **Management Access IP Source**. To manage the NSv from another location, you need to add an inbound rule.
To add a new inbound rule for NSv HTTPS management access from another public IP address:

1. Click Inbound security rules in the left navigation pane of the Azure NSG page. The Inbound security rules page displays.

2. Click the Add button. The Add inbound security rule dialog appears.

3. For Source, select IP Addresses.

4. For Source IP addresses/CIDR ranges, type in your new public IP address or an address range in CIDR format.

5. Optionally fill in Source port ranges if you want to specify the port(s).

6. For Destination, select Any.

7. For Destination port ranges, type in 443 for HTTPS access.

8. For Protocol, select TCP.

9. For Action, select Allow.

10. For Priority, type in an available number that is less than (higher priority than) the number for the first Deny rule.
11 For Name, type in a descriptive name for this rule.
12 Optionally fill in the Description field.
13 Click Add.

Forwarding Traffic to Your NSv in Azure

This section describes how to configure a route on your SonicWall NSv Series virtual firewall so that you can pass traffic through the NSv.

If you have not yet registered your NSv on MySonicWall, do that now. See Registering the NSv Appliance from SonicOS on page 37 for information. Your NSv must be registered to enable full functionality.

To configure a route on your NSv Azure firewall:

1. If not already logged into the Azure portal, navigate to https://portal.azure.com/ and log into your Azure account.
2. In the Azure left navigation pane, click All services.

3. In the All services Filter field, type Route. The display changes to show only services with “Route” in their names.

4. Click Route tables.
5. On the Route tables page, click Add to create a new route table.
The **Create route table** dialog is displayed.

6. In the **Name** field, type in a name for this route table.

7. For **Subscription**, select the subscription you are using in Azure.

8. For **Resource group**, select **Create new** if you will use the route table for other networks, or select **Use existing** if you will use the route table for this network only. If you select **Use existing**, you can use the drop-down list to select the same resource group you are using for your NSv.

9. The **Location** field should already display the same location you selected for your NSv.

10. For **BGP route propagation**, accept the default of **Enabled**.
11 Click **Create** to create the route table. After a brief wait, **Notifications** displays *Deployment succeeded* and the new route table appears in the **Route tables** screen.

![Route tables](image)

12 Click on the route table name.

13 In the route table screen, under **SETTINGS**, click **Routes**.

![Route table settings](image)

14 On the **Routes** screen, click **Add** to add a route to the route table.

15 In the **Add route** screen, for **Route name**, type in a descriptive name such as *default_route*.

16 For **Address prefix**, type in *0.0.0.0/0* to elect all traffic to be forwarded to the NSv.

17 For **Next hop type**, select **Virtual appliance** from the drop-down list.
18 For **Next hop address**, type in the IP address of the NSv X0 interface.

19 Click **OK**. This creates the route.

20 Next, you need to associate the route table. In the **Route table** options, click **Subnets**.

21 In the **Subnets** screen, click **Associate**.
22 In the **Associate subnet** screen, click **Virtual network**. The resources with possible virtual networks are displayed to the right under **Resource**.

![Virtual网络资源选择](image1.png)

23 Click on the desired resource. The display on the right changes to the **Choose subnet** screen and shows the possible subnets available for that resource.

![选择子网](image2.png)

24 Under **Choose subnet**, click **LAN-X0**. Since we entered the X0 IP address above for **Next hop address**, the X0 subnet must be selected here.

25 Click **OK** at the bottom of the screen. Azure performs the association and the **LAN-X0** subnet appears on the screen.

![子网配置](image3.png)

This completes the configuration required for forwarding traffic through the NSv. Continue to **Testing Traffic Through Your NSv in Azure** on page 33.

## Testing Traffic Through Your NSv in Azure

After configuring a route for forwarding traffic on your NSv, you can verify it with some test traffic. You can send traffic from any client machine or virtual machine on the same subnet as the route you configured. In our configuration, this is the LAN-X0 subnet, or 192.168.2.0/24.

For example, you could create an Ubuntu virtual machine in Azure, using the same options as your NSv for the following settings:

- **Subscription**
- **Resource group**
To send traffic through your NSv:

1. On your client machine or VM (Ubuntu, for example), open a console window. For an Ubuntu VM on Azure, click Serial Console in the Virtual machine options.

2. Type `ping 192.168.2.4` on the command line. The pings should succeed.

3. Log into your NSv and navigate to the MONITOR | Appliance Health | Live Monitor page.

4. Scroll down to view the Connection Count chart. It should show a positive count, caused by the pings.

Other charts on the page will also show activity. This verifies that traffic can be forwarded to the NSv.
Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in *Using the Virtual Console* on page 41 to go to the NSv Management Console window or the SonicOS CLI window. Check the boot messages:

**NOTE:** The error messages shown below indicate that the virtual firewall cannot boot.

Insufficient Memory Assignment

The following messages will appear if the virtual machine has insufficient memory. This may occur when doing an NSv installation or a NSv product upgrade.

**SonicOS boot message:**

**Insufficient memory 4 GB, minimum memory required 10 GB for NSv model: “NSv 800 Beta”**

Power off the Network Security virtual appliance and assign 10 GB to this virtual appliance.

This message can also appear in the Management Console logs as shown in the two following screen shots.

**NOTE:** For details on navigating the NSv Management Console to troubleshoot the installation, see *Using the Virtual Console* on page 41.
Memory may be insufficient without an insufficient memory log entry:
Licensing and Registering Your NSv

Registering the NSv Appliance from SonicOS

Once you have installed and configured network settings for your NSv Series appliance, you can log into SonicOS management and register it in your MySonicWall account. Registration of your SonicWall NSv Series follows the same process as for SonicWall hardware-based appliances.

**NOTE:** System functionality is extremely limited if registration is not completed. See Using System Diagnostics on page 39 for more information.

To register your NSv appliance:

1. Point your browser to your NSv Series WAN or LAN IP address and log in as the administrator (default admin / password).
2. Licensing and Registering Your NSv
3 At this point you may log into MySonicWall and name the NSv installation while providing the serial number and authorization code to complete registration. Or, if you are unable to reach MySonicWall, use the Keyset, Serial Number and Authorization and Registration codes provided by your SonicWall representative.

4 Once complete log into SonicOS and check that licensing is complete.
Managing SonicOS on the NSv Series

The X1 interface is the default WAN Interface and is set to use DHCP addressing by default, with HTTPS management enabled. To ease testing, you can utilize a DHCP server on the X1 connected network. If DHCP is not available, use the console to access the CLI and configure a static IP address.

The X0 interface is the default LAN interface, and also has HTTPS management enabled. Its IP address is set to 192.168.168.168 by default. You can map this interface to your own network during initial deployment of the OVF template. After deployment, you can reconfigure the IP address to an address in your network.

1. Point your browser to either the LAN or WAN IP address. The login screen is displayed.
   - When the X1 WAN interface is using DHCP addressing, DNS is also enabled. You can generally access the WAN address from any machine in your network.
   - If you have an existing network on 192.168.168.0/24 in your environment, you can access the default IP address of the X0 LAN interface of your NSv Series from a computer on that network for SonicOS management. The NSv Series X0 IP address is 192.168.168.168 by default.

2. Enter the administrator credentials (default `admin / password`) and press Enter.
   - The SonicOS management interface is displayed. You can navigate and update the configuration just as you would with any SonicWall network security appliance.

Using System Diagnostics

Check Network Settings, at Device | Diagnostic > Check Network Setting, is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of the NSv Series, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.
Specifically, **Check Network Settings** automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity
- License Manager server connectivity
- Content Filter server connectivity

To use the **Check Network Settings** tool, first select it in the **Diagnostics** drop-down list and then click the check box in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, select the **Server** checkbox at the top of the table to select all items or select the checkbox for each desired item and then click **TEST ALL SELECTED**.

If probes fail, you can click the blue arrow to the left of the **IP Address** field of the failed item to jump to the configuration page to investigate the root cause.
Using the Virtual Console

Topics:

- Connecting to the Console with SSH on page 41
- Navigating the NSv Management Console on page 43
- Using SafeMode on the NSv on page 52

Connecting to the Console with SSH

SSH is used to connect to the virtual console of an NSv deployed on Azure.

To connect to the management console using SSH:

1. Launch PuTTY and type in the public IP address of the NSv on Azure.

   You can find the public IP by clicking Virtual Machines in the Azure portal, then clicking the name of your NSv and locating the public IP on the Overview screen.

2. For Port, type in 22 if it is not already set.

   **NOTE:** Changing the SSH port to anything other than 22 can prevent access to the SonicCore management console and the SonicOS CLI console.

3. For Connection type, SSH should already be selected by specifying port 22.
4. Click **Open** to open a console connection.

5. In the console window at the **login as** prompt, type in **management**, which is the SSH management user name defined during the NSv deployment.

6. At the **Password** prompt, type in the SSH management password you defined during deployment.

   The orange NSv management console displays.

   You can switch to the black SSH console window by pressing **Ctrl+s** and then the **spacebar**. If you are prompted to log in at the **User** prompt, enter the SonicOS administrator credentials (default: **admin / password**).
Navigating the NSv Management Console

The NSv management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, and other functions. You can connect to the NSv management console by using PuTTY or a similar application to SSH to the public IP address of an NSv on Azure. See Connecting to the Console with SSH on page 41.

To navigate and use the management console:

1. Press **Ctrl+s** and then press the **spacebar** to toggle between the SSH virtual console or Azure remote console and the NSv management console. That is, press the **Ctrl** key and ‘s’ key together, then release and press the **spacebar**. The NSv management console has an orange background.

2. The main menu is displayed in the side menu (left pane). 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 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 NSv management menu choices are described in the following sections:

- System Info on page 45
- Management Network or Network Interfaces on page 46
- Test Management Network on page 47
- Diagnostics on page 48
- NTP Server on page 49
- Lockdown Mode on page 50
- System Update on page 51
- Reboot | Shutdown on page 51
- About on page 52
- Logs on page 52
System Info

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

- **Model** – This is the model of the NSv appliance.
- **Product code** – This is the product code of the NSv appliance.
- **Serial Number** – The serial number for the appliance; this is a number unique to every NSv instance deployed. This number can be used to identify the NSv appliance on MySonicWall.
- **Model Name** – This is the model name of the NSv appliance.
- **SonicOS Version** – This is the currently running SonicOS version of the NSv appliance.
- **GUID** – Every NSv instance has a GUID which is displayed here.
- **System Time** – This is the current system time on the NSv appliance.
- **Up Time** – This is the total time that the NSv appliance has been running.
- **Average Load** – 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.
- **SonicOS** – This presents the current state of the SonicOS service on the NSv. **Operational** is displayed here when the SonicOS service is running normally, **Not Operational** when there is a problem with the service and **Operational (debug)** if the service is currently running in debug mode.
Management Network or Network Interfaces

Network Interfaces screen (Azure)

In this screen, the network settings are read-only except when the management console is in SafeMode. In SafeMode, you can configure these settings.

- **Management Interface** – This is the current interface serving as the management interface. This defaults to X1.
- **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 NSv appliance.
- **DNS** – This is a list of the DNS servers currently being used by the NSv appliance.
The **Test Management Network** screen is displayed for an NSv on Azure, but not for an NSv on Azure. In an Azure NSv, the **Ping** and **Nslookup** commands are available on the **Diagnostics** screen.

The **Test Management Network** 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 NSv appliance.

**To use Ping:**

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

![Nslookup dialog](image)

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.

![Nslookup query results](image)

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

**Diagnostics**

In the **Diagnostics** screen, you can send diagnostics to SonicWall Technical Support. This has the same functionality as clicking **SEND DIAGNOSTIC REPORTS TO SUPPORT** in the **INVESTIGATE | Tools | System Diagnostics** page of the SonicOS web management interface.

![Diagnostics screen](image)

**NOTE:** Your NSv appliance 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 NSv appliance’s NTP client to perform a sync with the configured NTP server(s).
- **Current time** – The current time on the NSv appliance.
- **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 NSv appliance is currently synchronized with the configured NTP server(s).

**Lockdown Mode**

In the **Lockdown Mode** screen, you can enable **Strict Lockdown** mode. When enabled, the management console is effectively disabled. A dialog box that cannot be closed is permanently displayed on the management console. This prevents any person from accessing the management console.

To enable Strict Lockdown mode, select **Enable** and then press **Enter**.

⚠️ **CAUTION:** Be careful about enabling Strict Lockdown mode. Strict Lockdown mode cannot be disabled.

**Temporary Lockdown Mode**

A temporary lockdown mode can be enabled and disabled in SonicOS on the **MANAGE | Appliance > Base Settings** page. You can enable lockdown mode by clearing the **Enable management console** checkbox under the **Advanced Management** section, and can disable lockdown mode by selecting the checkbox. Click **ACCEPT** after each change.

The management console will automatically be enabled/disabled a few seconds after it has been enabled/disabled in the SonicOS web interface page.
System Update

The **System Update** screen is available on NSv in Azure.

---

**Reboot | Shutdown**

The **Reboot | Shutdown** screen provides functions for rebooting the NSv appliance, enabling debug mode, 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 SonicWall** – Restarts the NSv Series virtual appliance with current configuration settings.
- **Shutdown SonicWall** – Powers off the NSv Series virtual appliance.
- **Boot with factory default settings** – Restarts the NSv Series virtual appliance using factory default settings. All configuration settings will be erased.
- **Boot SonicWall into debug** – Restarts the NSv Series virtual appliance into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** – Puts the NSv Series virtual appliance into SafeMode. For more information, see Using SafeMode on the NSv on page 52.
About

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

Logs

The **Logs** screen displays log events for the NSv appliance.

Using SafeMode on the NSv

The NSv appliance will enter SafeMode if SonicOS restarts three times unexpectedly within 200 seconds. When the NSv appliance is in SafeMode, the appliance starts with a very limited set of services and features enabled. This is useful when trying to troubleshoot issues. The NSv appliance can also be configured to boot into SafeMode by using the **Reboot | Shutdown** screen in the NSv 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

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

When the NSv is in SafeMode, the SonicOS service is one of the services that is not enabled and is shown as *Not operational* on the SafeMode **System Info** screen.
The SafeMode Management Console always starts with the **System Info** screen.

**NOTE:** To exit SafeMode, disable it on the **Reboot | Shutdown** screen or deploy a new firmware image. See [Disabling SafeMode](#) on page 54 and [Installing a New SonicOS Version in SafeMode](#) on page 58 for more information.

**Topics:**
- [Enabling SafeMode](#) on page 53
- [Disabling SafeMode](#) on page 54
- **Configuring the Management Network in SafeMode** on page 55
- [Installing a New SonicOS Version in SafeMode](#) on page 58
- [Downloading Logs in SafeMode](#) on page 59

## Enabling SafeMode

SafeMode can be enabled from the management console.

**To enable SafeMode:**

1. Access the NSv management console as described in one of:
   - For NSv on Azure, see: [Connecting to the Console with SSH](#) on page 41
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**.

![SonicWall NSv Series Azure Getting Started Guide](image)

4 Select **Yes** in the confirmation dialog.

5 Press **Enter**.

The NSv 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 NSv 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**.

![SonicWall NSv Series Azure Getting Started Guide](image)

3 Select **Yes** in the confirmation dialog.

4 Press **Enter**.

The NSv immediately reboots and boots up in normal mode.
Configuring the Management Network in SafeMode

When the Management Console is in SafeMode, the Management Network screen in the NSv management console provides features to configure the NSv appliance interfaces:

- **Management Interface** – This is the currently selected interface. This defaults to X1. Use this to select any of the NSv appliance interfaces.
- **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 NSv appliance.
- **DNS** – A list of the current DNS servers currently being used by the NSv appliance.

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

**Topics:**
- Configuring Interface Settings on page 55
- Disabling an Interface on page 57

**Configuring Interface Settings**

In SafeMode, the Management Network 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 Management Network screen, select the Management interface option and then press Enter.

   The Select Interface list appears, displaying all of the interfaces available on the NSv.

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 Management Network screen, select the Management interface option.
2. Press Enter.
   
   The Select Interface list appears, displaying all of the interfaces available on the NSv.
3. 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.
4. Select IPv4 Address and press Enter.
   
   The on-screen dialog displays the current IP address.
5. Navigate into the dialog and change the IP address to 0.0.0.0, then press Enter.

   ![Screen shot of interface settings]

   The Save changes button is displayed.
6. Press Tab to navigate to the Save changes button and then press Enter.
The interface is disabled.

<table>
<thead>
<tr>
<th>Management Network</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Interface</td>
<td></td>
<td>X1</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td></td>
<td>Not configured</td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mac Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>fe80::50e:23ff:fe5e:1947</td>
<td></td>
</tr>
<tr>
<td>Gateway</td>
<td>10.0.0.1</td>
<td></td>
</tr>
<tr>
<td>DNS 1</td>
<td>8.8.4.4</td>
<td></td>
</tr>
<tr>
<td>DNS 2</td>
<td>8.8.4.4</td>
<td></td>
</tr>
</tbody>
</table>

**Installing a New SonicOS Version in SafeMode**

SWI files are used to upgrade SonicOS. You can download the latest SWI image file from MySonicWall.

In SafeMode, you can upload a new SonicOS SWI image and apply it to the NSv appliance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the NSv management console. When viewing the NSv management console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

For additional instructions on the following procedure, see:
For additional information on uploading a new image, refer to:
https://www.sonicwall.com/support/knowledge-base/?sol_id=180404172741874

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

**To install a new SonicOS from SafeMode:**

1. Depending on the type of NSv deployment, determine the IP address to use to access the SafeMode web management interface:
   - On an NSv deployed in Azure, you can access the SafeMode web interface at the public IP address assigned to the NSv.
2 In a browser, navigate to http://<IP address>, using the applicable IP address. 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 NSv appliance reboots with the new image.

### Downloading Logs in SafeMode

When the NSv appliance 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 public IP address of an NSv on Azure.

**NOTE:** In SafeMode, the web management interface is only available via http (not https).
To download logs from SafeMode:

1. In a browser, navigate to http://<IP address>, using the applicable IP address. The SafeMode web management interface displays.

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

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

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. 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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support
- 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.

NSv Series on Azure Getting Started Guide
Updated - September 2020
Software Version - 7.0
232-005463-00 Rev A

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 NONINFRINGEMENT. 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