SonicOS 7.1

Upgrade Guide

for the NSv Series

SONICWALL®

Contents

Upgrading to SonicOS 7.1

Welcome to the *SonicOS 7.1 Upgrade Guide for NSv Series*. This guide is applicable for the following SonicWall Virtual Firewall Models.

- NSv Series: NSv 270, NSv 470, and NSv 870.

This upgrade guide provides information about upgrading your NSv Series firewall from previous versions of SonicOS 6.5 or SonicOS 7.0 to the latest version of SonicOS 7.1.

ⓘ **NOTE:** The initial deployment of SonicOS 7.0 and 7.1 must be a fresh install. Upgrading to SonicOS 7.0 and 7.1 from SonicOS 6.5.4.v via the SWI file is not supported.

ⓘ **NOTE:** If you are upgrading SonicOS from a Gen6 (versions 6.5 or older) firewall to a Gen7 (version 7.1) firewall via an online migration tool is not supported, Minimum version SonicOS 7.0.1-11 is required to upgrade to the latest version of SonicOS 7.1.

ⓘ **NOTE:** To upgrading SonicOS from a Gen6 (versions 6.5 or older) firewall to a Gen7 (version 7.0.1-11) firewall, you must use an online migration tool to "migrate" your settings to Gen7 (version 7.0.1-11) after the configuration file has been saved. See the **Knowledge Base** article titled, How to Create Gen 7 Settings File by Using the Online Migration Tool for more information.

This guide also provides related information including importing configuration settings from one NSv model to another and between NSv platforms, upgrading a High Availability pair, using System Update to upgrade SonicOS, SonicCore and SonicCoreX, using SafeMode to upgrade SonicOS, and how to perform a Model Upgrade to increase the available number of cores on your NSv. See the following topics for details.

Topics:

- Upgrading Firmware
- Performing a Model Upgrade
- Importing Configuration Settings
- SonicWall Support

Upgrading Firmware

This section provides instructions for obtaining new firmware, preparing to upgrade your firewall, and different ways to upgrade.

Topics:

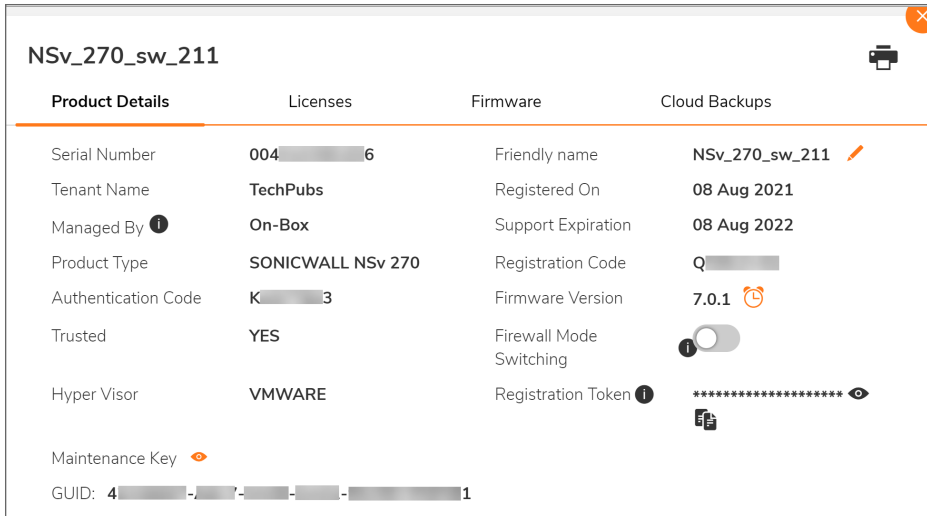- Obtaining the Latest SonicOS Firmware
- Creating a System Backup and Exporting Your Settings
- Upgrading via System Update in the NSv Management Console
- Upgrading SonicOS with Current Settings
- Upgrading SonicOS with Factory Default Settings
- Upgrading a High Availability Pair
- Using SafeMode to Upgrade the SonicOS Image
- Upgrading an Existing Deployment from SonicOS 6.5.4.v to SonicOS 7.0

Obtaining the Latest SonicOS Firmware

To obtain a new SonicOS image file for your SonicWall NSv virtual firewall:

1. In a browser on your management computer, log into your MySonicWall account at https://www.mysonicwall.com.

2. In MySonicWall, navigate to **My Workspace> Products** in the left navigation pane to display the list of your registered NSv virtual firewalls.

3. Click on the serial number for your appliance to display a window frame with Product Details, Licenses, Firmware and Cloud Backup. The **Product Details** screen displays the type of **Hyper Visor**, such as AWS, Azure or VMware.

NSv_270_sw_211			
Product Details	Licenses	Firmware	Cloud Backups
Serial Number	004 6	Friendly name	**NSv_270_sw_211**
Tenant Name	**TechPubs**	Registered On	**08 Aug 2021**
Managed By	**On-Box**	Support Expiration	**08 Aug 2022**
Product Type	**SONICWALL NSv 270**	Registration Code	Q
Authentication Code	K 3	Firmware Version	7.0.1
Trusted	**YES**	Firewall Mode Switching	
Hyper Visor	**VMWARE**	Registration Token	********************
Maintenance Key			
GUID: 4 - - - - 1			

4. Click the **Firmware** tab. The screen displays the recently available firmware versions. Scroll down to find firmware for your hyper visor.

SONICWALL NSv 270			🖨
Product Details	Licenses	**Firmware**	Cloud Backups

⚠ Updated release available

Serial Number	00401038B524	Firmware Version	**7.0.0.0**	Latest Released Firmware	**7.0.1-R1283**
		Type	**N/A**	Type	**Maintenance Release**
		Release Date	**N/A**	Release Date	**Jun 01, 2021**

⌄ Available Downloads

NSv 270 KVM

sonicwall_nsv_qemu_7.0.1.0-1283-5db19878.0.swi
Release Date - Jun 01, 2021, Release type - Maintenance Release, File Size - 200.72 MB
Version 7.0.1-R1283

SonicWall_NSv_7.0.1.0-1283_For_QEMU_VM.zip
Release Date - May 31, 2021, Release type - Maintenance Release, File Size - 1.6 GB
Version 7.0.1-R1283

SNMP MIBs
Release Date - May 28, 2021, Release type - Maintenance Release, File Size - 46 KB
Version 7.0.1-R1456

NSv 270 Hyper-V

sonicwall_nsv_hyperv_7.0.1.0-1282-5db19878.0.swi
Release Date - Jun 01, 2021, Release type - Maintenance Release, File Size - 200.66 MB
Version 7.0.1-R1282

SonicWall_NSv_7.0.1.0-1282_For_Microsoft_HyperV.zip
Release Date - May 31, 2021, Release type - Maintenance Release, File Size - 1.6 GB
Version 7.0.1-R1282

SNMP MIBs
Release Date - May 28, 2021, Release type - Maintenance Release, File Size - 46 KB
Version 7.0.1-R1456

NSv 270 VMware

sonicwall_nsv_vmware_7.0.1.0-1282-5db19878.0.swi
Release Date - Jun 01, 2021, Release type - Maintenance Release, File Size - 200.59 MB
Version 7.0.1-R1282

SonicWALL_NSv_270_R1282.ova
Release Date - May 31, 2021, Release type - Maintenance Release, File Size - 1.62 GB
Version 7.0.1-R1282

SNMP MIBs
Release Date - May 28, 2021, Release type - Maintenance Release, File Size - 46 KB
Version 7.0.1-R1456

NSv 270 BYOL AWS SWI

sonicwall_nsv_aws_7.0.1.0-1282-5db19878.0.swi
Release Date - Jun 01, 2021, Release type - Maintenance Release, File Size - 200.39 MB
Version 7.0.1-R1282

SNMP MIBs
Release Date - May 28, 2021, Release type - Maintenance Release, File Size - 46 KB
Version 7.0.1-R1456

NSv 270 PAYG AWS SWI

sonicwall_nsv_aws-payg_7.0.1.0-1282-5db19878.0.swi
Release Date - Jun 01, 2021, Release type - Maintenance Release, File Size - 200.36 MB
Version 7.0.1-R1282

SNMP MIBs
Release Date - May 28, 2021, Release type - Maintenance Release, File Size - 46 KB
Version 7.0.1-R1456

NSv 270 BYOL Azure SWI

sonicwall_nsv_azure_7.0.1.0-1282-5db19878.0.swi
Release Date - Jun 01, 2021, Release type - Maintenance Release, File Size - 200.4 MB
Version 7.0.1-R1282

SNMP MIBs
Release Date - May 28, 2021, Release type - Maintenance Release, File Size - 46 KB
Version 7.0.1-R1456

(Browse All Firmware)

5. Optionally, click the **Browse All Firmware** button to display all available firmware versions. Depending on your NSv platform, the following file types are available:

   - SWI – Upgrade image file for an existing deployment on any platform. If not displayed, a fresh installation may be required for this release. Check the *Release Notes*.
   - ZIP – Contains image file for fresh installation on NSv Hyper-V or NSv KVM.
   - OVA – Fresh installation image file for NSv VMware/ESXi.

   ⓘ **NOTE:** SonicOS 7.1 is the latest and the default version available on the Amazon Web Services or Microsoft Azure web sites. For information on how to deploy the SonicOS 6.5.4 version on AWS and Azure platforms, refer to the respective Knowledge Base article:

   - For NSv Azure, refer to the following Knowledge Base article:
     https://www.sonicwall.com/support/knowledge-base/how-do-i-deploy-an-old-version-of-nsv-on-azure/191202144945079/
   - For NSv AWS, refer to the following Knowledge Base article:
     https://www.sonicwall.com/support/knowledge-base/deploying-previous-versions-of-nsv-on-aws/201111071141760/

6. Mouse over the row for the firmware you want. Options appear at the right. The PDF icon for the SonicOS Release Notesmight only appear on the first row of that group, usually the row with the SWI.
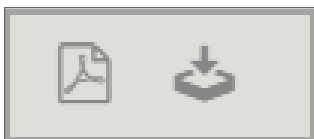
7. Click the **Download** icon to download the firmware to your computer, and click the **PDF** icon to display the SonicOS Release Notes. Be sure to download the firmware that matches your hyper visor.

Creating a System Backup and Exporting Your Settings

Before beginning the update process, make a system backup on your SonicWall NSv. When you click the **Create Backup** button, SonicOS takes a "snapshot" of your current system state, SonicOS image, and configuration preferences, and makes the snapshot the new System Backup image. You can save Backups locally or on the cloud. You can also schedule backups to occur automatically. Clicking **Create Backup** overwrites the existing Backup image as necessary.

You can also export the NSv configuration settings to a file on your local management station. This file serves as an external backup of the configuration settings, and can be imported into another NSv or into the same NSv if it is necessary to reboot SonicOS with factory default settings.

To save a system backup and export configuration settings to a file on your local management station:

1. In SonicOS 7, in the **DEVICE** view, navigate to **Settings > Firmware and Settings**. For a local backup, click on **Firmware & Local Backups**. For a cloud backup, click on **Cloud Backups**.

2. In SonicOS 6.5, in the **MANAGE** view, navigate to **Updates | Firmware & Backups**.

3. Click **Create Backup** and select one of the following:

   • **Local Backup** – SonicOS takes a "snapshot" of your current system state, firmware, and configuration preferences, and saves it as the latest local backup file.

   In the **Local Backup** dialog, optionally select **Retain Local Backup** to prevent this backup from being overwritten by a future local backup. Optionally enter a comment in the **Comment** field, and then click **OK** to proceed with the backup.

   • **Cloud Backup** – The Cloud Backup dialog is displayed. Optionally select **Retain Local Backup** to prevent this backup from being overwritten by a future cloud backup. You can retain a maximum of 3 configuration backup files per firmware version. Optionally enter a comment in the **Comment** field, and then click **OK** to proceed with the backup.

4. To export your settings to a local file on your management computer, click **Import/Export Configuration** (in SonicOS 7, this option is available on the **Firmware & Local Backups** screen) and select **Export Configuration**. In the popup dialog, which displays the name of the saved file, click **Export** to complete the process.

Upgrading via System Update in the NSv Management Console

When you upgrade using System Update, SonicCore and SonicCoreX are updated as well as SonicOS. All configuration and registration settings are retained.

When upgrading a High Availability pair using System Update, upgrade each unit individually.

Topics:

- Upgrading SonicOS 6/6.5 and 7.0 via System Update in the SonicCore Console
- Upgrading SonicOS 7.1 via System Update in the SonicCoreX Version with CLI Console

Upgrading SonicOS 6/6.5 and 7.0 via System Update in the SonicCore Console

You can access the orange NSv management console by opening the virtual console from your hypervisor or by connecting to it with SSH, and then pressing **Ctrl+s** followed by the **spacebar**, if needed.

To upgrade your NSv using System Update:

1. Select **System Update** in the left pane of the NSv management console.

2. Check for available system updates. Press the **Tab** key to move to the right pane, and use the **arrow keys** to select **Start Update** and then select **Yes** and press **Enter**.
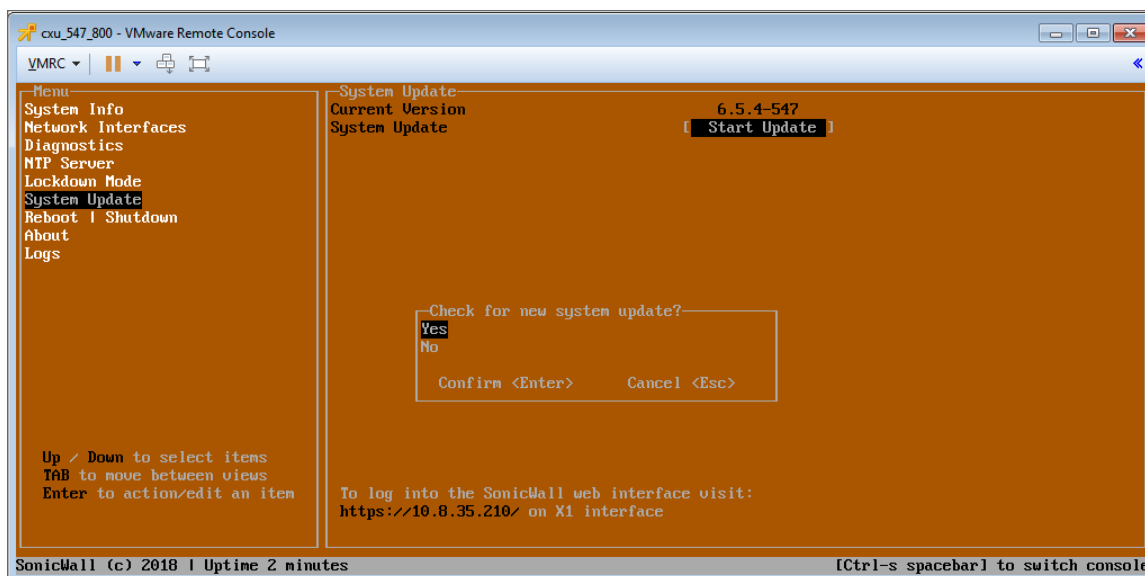
3. If a new version is available, it is displayed in the center of the screen. Select **Start update** and then press **Enter**. The update version will begin to download and can take a few minutes or, in some cases, a few hours.

    ⓘ | **NOTE:** SonicOS 6/6.5 to 6.5.x versions upgrade is possible via the orange SonicCore console and an upgrade from SonicOS 6.5 to 7.0 version is not supported. You have to do the fresh deployment if you want SonicOS 7.0 version.

    ⓘ | **NOTE:** SonicOS 7.0 to 7.0.x versions upgrade is possible via the orange SonicCore console and an upgrade from SonicOS 7.0 to 7.1 version is not supported. You have to do the fresh deployment if you want SonicOS 7.1 version.
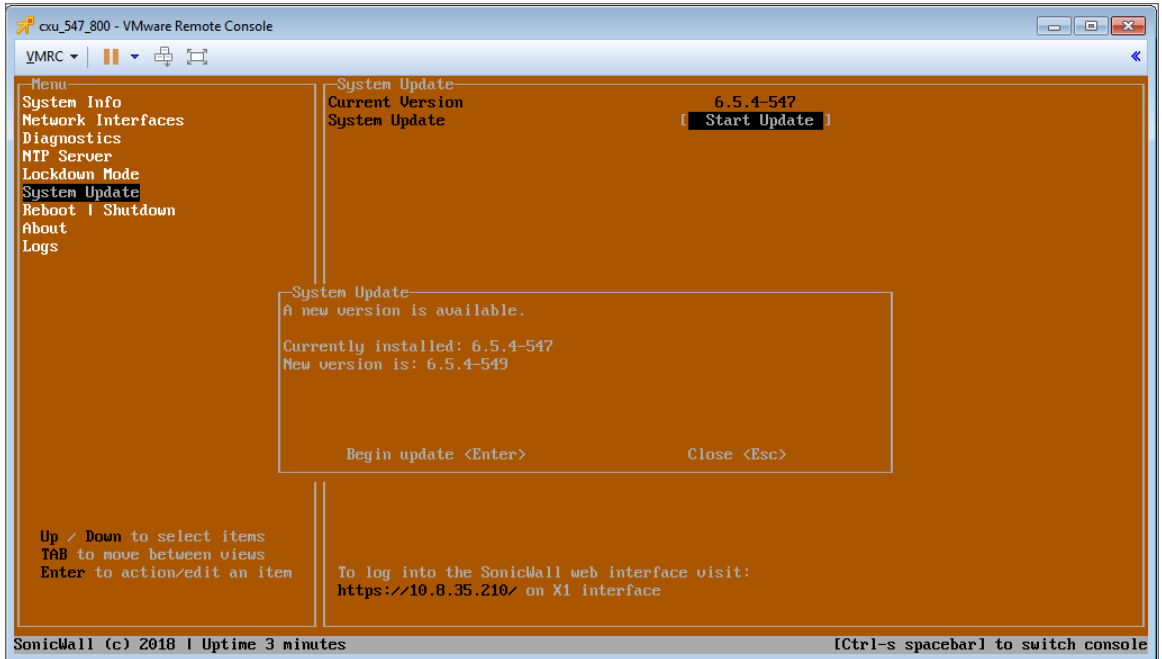
⚠ | **CAUTION:** Do not power off or reboot during the download.
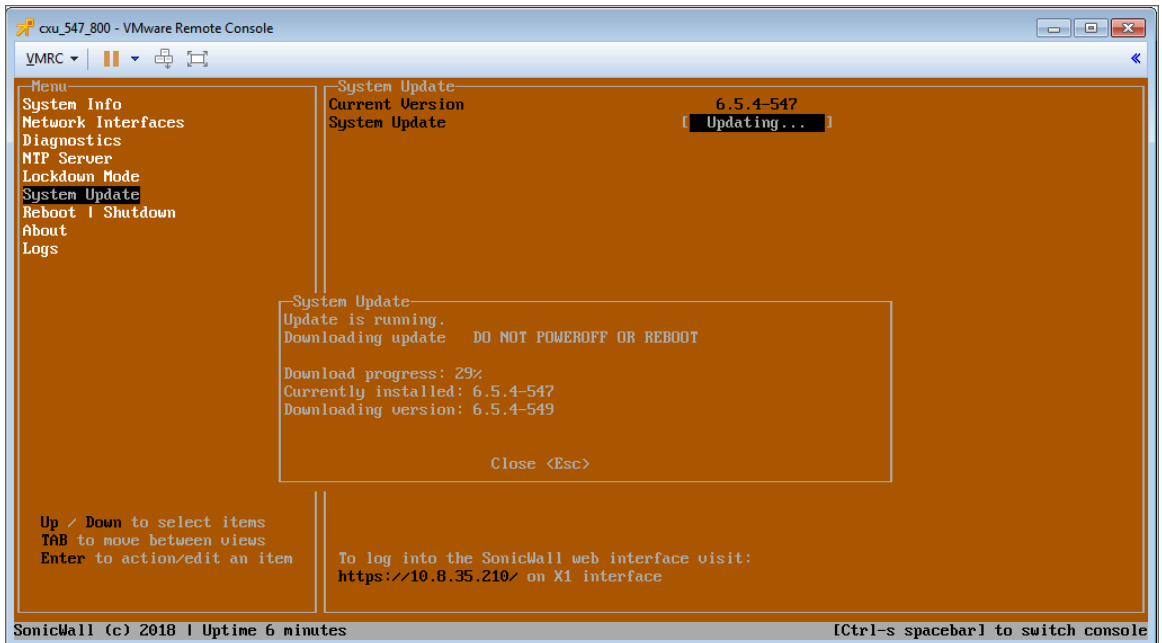
4. If you want to close the downloading progress display, press the **ESC** key. This allows you to move around the NSv management console or switch to the SonicOS CLI console with **Ctrl+spacebar**. SonicOS continues to run during the download.

5. When the download completes, the message **Reboot to complete update** is displayed in the NSv management console. Press **ESC** to close the status display.
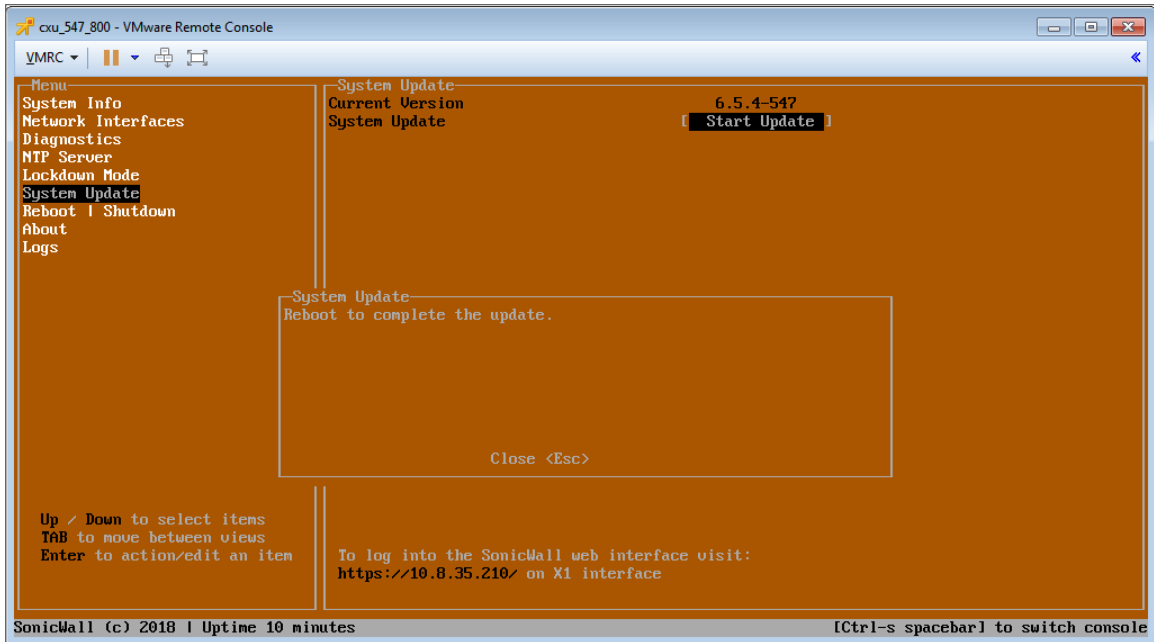
6. Select **Reboot | Shutdown** in the left pane, then select **Reboot** in the right pane and select **Yes** and press **Enter** to start the reboot process.
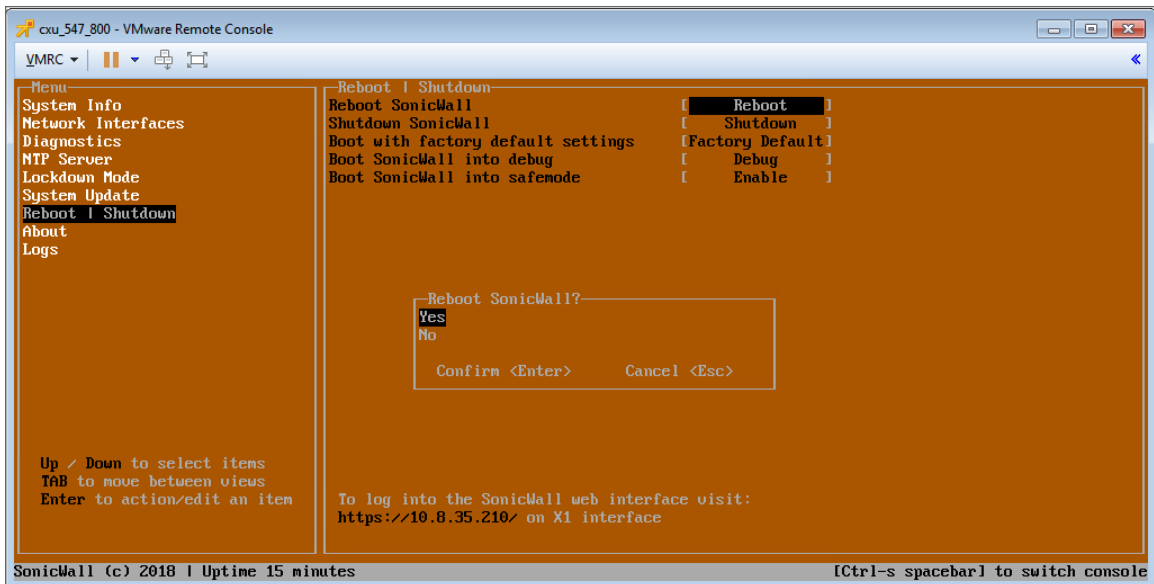
⚠ **CAUTION:** You can reboot from the NSv management console as shown here, or from the VM menu. However, DO NOT reboot from the SonicOS web management interface or the CLI – those methods will reboot to the old version.

After the reboot but before SonicOS comes up, the **Initializing services** message is displayed. *Do not power off or reboot again until this completes.*
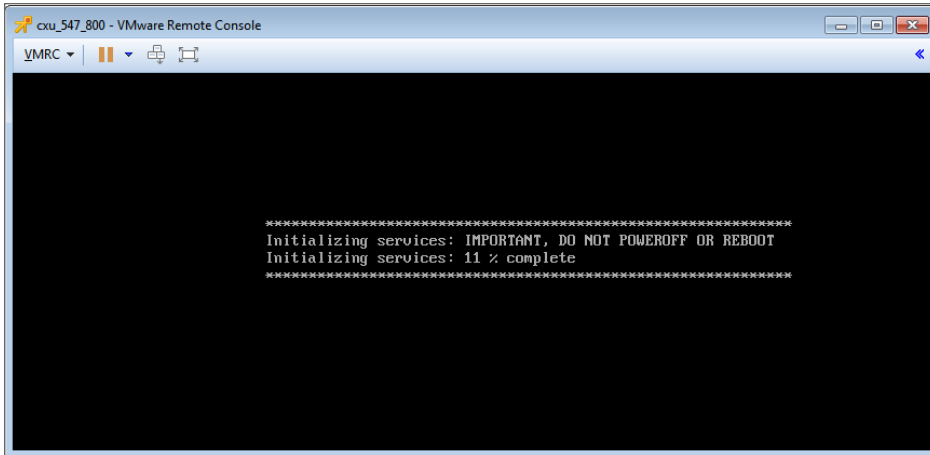
7. When SonicOS comes up, view the **About** screen in the orange NSv management console to verify that SonicCore is updated.
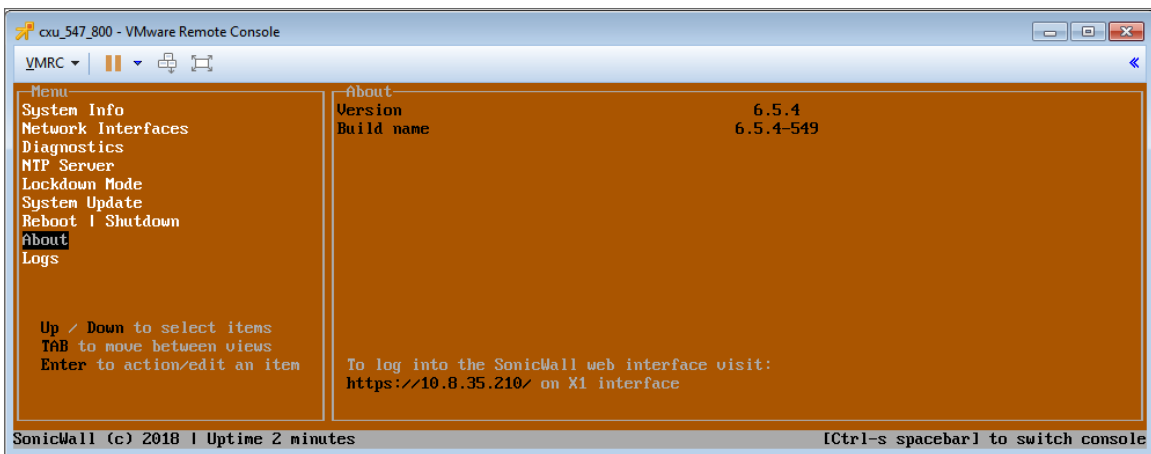
8. Switch to the SonicOS CLI console to verify that SonicOS is updated to the new version, and that the NSv is still registered and X0 still has the configured IP address.

```
Initializing IPv6 engine
Initializing LM API Layer
Initializing AWS S3 Client
Initializing Cloud Backup Client
Initializing IPv6 Interfaces
delay interval:60, clockrate:1, report interval:15
Initializing SSLVPN Server
Initializing DHCPv6 Server
Initializing Router Advertisement Daemon
Initializing DHCPv6 Client
Initializing DHCPv6 client runtime
Initializing CLI
Initializing Data-Plane Timer Tick
Starting ZeroTouch
Upgrade Legacy BWM Configuration
Update Firmware Boot History
Flushing Incomplete Arp Entries
Admin Up Ports
Initialize Mac lookup tables
Initializing hardware watchdog
Generate shadow policies
System is in Policy Mode
No need to bootstrap because NSv is registered


Product Model         : NSv 270
Product Code          : 27002
Firmware Version      : SonicOSX 7.0.1-16-1317
Serial Number         : 00401039D3CF
X0 IP Addresses       : 192.168.55.1


*** Startup time: 07/14/2021 15:46:09.896 ***
open the https management file


Copyright (c) 2021 SonicWall, Inc.


User:Signature Downloaded

SonicWall (c) 2019 | Uptime                         [Ctrl-s spacebar] to switch console
```

ⓘ | **NOTE:** The system might require two or three minutes to mark the update as successful. To avoid rolling back to the previous NSv management console SonicCore version during a subsequent reboot, wait a couple of minutes before rebooting the system again.

Upgrading SonicOS 7.1 via System Update in the SonicCoreX Version with CLI Console

You can access the NSv management SonicCoreX version with CLI console by opening the virtual console from your hypervisor.

```
Copyright (c) 2023 SonicWall, Inc.

Starting ZeroTouch
Upgrade Legacy BWM Configuration
Update Firmware Boot History
Flushing Incomplete Arp Entries
Admin Up Ports
Initialize Mac lookup tables
Initializing hardware watchdog
Generate shadow policies
System is in Policy Mode
Directory : /opt/sonicwall/sonicos/logs/pcaplogdir EXISTS
No need to bootstrap because NSv is registered
Initializing local mirroring

Product Model         : NSv 870
Product Code          : 27008
Firmware Version      : SonicOSX 7.1.1-7040-R5387
Serial Number         :
X0 IP Addresses       : 192.168.168.168


*** Startup time: 12/07/2023 18:09:09.912 ***
#### serve policy block page = 0
User:delay interval:60, clockrate:1, report interval:15
Signature Downloaded
12/07 18:18:21.400:  tick_offset_set_69: System Time updated
12/07 18:39:15.400:  dynHandleGetObjectListJson_9466: System Time was updated - reload all data and reset systemTimeUpdated
12/07 19:18:41.384:  tick_offset_set_69: System Time updated
12/07 20:19:01.560:  tick_offset_set_69: System Time updated

User:
User:12/07 21:19:21.208:  tick_offset_set_69: System Time updated
12/07 21:20:11.352:  dynHandleGetObjectListJson_9466: System Time was updated - reload all data and reset systemTimeUpdated

SonicWall (c) 2023 |                                [Ctrl-s spacebar] to switch console
```

You can access the NSv management SonicCoreX version with CLI console in Normal mode.

```
NSv >
  #              Comments on Shell
  dns-lookup     Perform a DNS Lookup.
  help           Key bindings' overview
  ping           Send messages to network hosts. Example: "ping ip ip_address/hostname" or "ping ip6 ipv6_address/hostname"
  restart        Restart the Appliance
  safemode       Restart the Appliance in Safe Mode.
  show           Show Information
  shutdown       Shutdown the appliance.
  support-data   Send SonicWall Support diagnostic data
  update         Utility commands for update related activity.
  update-channel Utility commands for update channel related operations.
```

You can access the NSv management SonicCoreX version with CLI console in Safe mode.

```
[Safe Mode] NSv >
  #              Comments on Shell
  date           Utility commands for date related operations.
  dhcp           Enable DHCP on a interface in Safe Mode
  dns            Configure DNS in Safe Mode
  dns-lookup     Perform a DNS Lookup.
  exit           Exit from the CLI
  help           Key bindings' overview
  network        Configure Network in Safe Mode, Example : network interface eth1 ip 10.202.10.20 netmask 255.255.255.0 gateway
10.202.10.1
  ping           Send messages to network hosts. Example: "ping ip ip_address/hostname"
  restart        Restart the Appliance
  show           Show Information
  shutdown       Shutdown the appliance.
  support-data   Send SonicWall Support diagnostic data
  update         Utility commands for update related activity.
  update-channel Utility commands for update channel related operations.
```

To upgrade your NSv using System Update in the SonicCoreX version with CLI console:

ⓘ **NOTE:** SonicOS 7.0 to 7.1 version upgrade is not supported. You have to do the fresh deployment if you want SonicOS 7.1 version. SonicOS 7.1 to 7.1.x versions upgrade is possible via SonicCoreX version with CLI console, See more information on the KB article.

1. Launch the virtual console and then click inside the console window.

2. The CLI console displays, enter the user name and password.

3. Enter the command **update** followed by a space and then followed by a '?' in the CLI console.

```
NSv > update
  check     Check for an update
  download  Download an update
  install   Install an update

NSv > update _
SonicWall (c) 2023 |                                                              [Ctrl-s space
```

4. To check for available system updates, enter the command **update check**.

```
update          update channel
NSv > update check
Update Available :  7.1.1-7039-R5375 . Issue 'update download' command to download the update.
NSv >
```

5. To download the available system updates, enter the command **update download**. After the command is issued download will start and you will get notified once the download is finished and to proceed with next step.
   ⓘ **NOTE:** Do not power off or reboot during the download

```
NSv > update download
Downloading .......................................................................................................

.................
Download Finished. Issue 'update install' command to install the update and reboot the device.
NSv >
```

6. To install the available system updates, enter the command **update install**.
   ⓘ **NOTE:** The device will reboot automatically after installation.

```
NSv > update install
NOTE: The device will reboot automatically after installation.
Installing uploadedFirmware.bin.sig
The device will reboot shortly with current setting.
```

7. After the reboot, the SonicOS Nsv upgrade process will be completed, to view the update information, enter the command **show sonicos** in the CLI console to verify that SonicCoreX version and SonicOS Nsv is updated.

```
NSv > show sonicos
Model           :  NSv 870
Platform        :  vmware
Product Code    :  27008
Serial Number   :  ██████████
Registration    :  true
Support License :  true
Version         :  SonicOSX 7.1.1-7039-R5375
Build Date      :  Fri Dec  1 23:20:45 UTC 2023
Install Date    :  Fri Dec  8 05:40:08 UTC 2023
Status          :  Running
```

8. To view the system information, enter the command **show system**.

```
NSv > show system
Product Name     :  nsv
Product Family   :  sonicos
Product Code     :  27008
Serial Number    :  0040103BBB03
Platform         :  vmware
OS               :  soniccorex
Hostname         :  nsv-vmware
Up Time          :  3:12
System Time      :  Fri Dec  8 05:15:01 UTC 2023
Load Average     :  1.27 (1 Mins) 1.23 (5 Mins) 1.36 (15 Mins)
Safe Mode        :  false
External Storage :  false
```

The following are the descriptions of the commands and their usage in the CLI console.

(i) **NOTE:** The command syntax, usage, and description can be fetched by typing the command on the SonicCoreX version with CLI console followed by a space and then followed by a '?'.

Command	Syntax	Description	Example
date	• date set <"mm/dd/yyyy HH:MM:SS"> • date read	Set and Displays the current date.	date set "02/12/2023 12:23:12" OR date read
dhcp	dhcp interface <interface name>	Enable dhcp on an interface in safe mode.	dhcp interface X1
dns	• dns primary <dns1> • dns primary <dns1> secondary <dns2>	Configure DNS server in safe mode	dns primary 8.8.8.8 OR dns primary 8.8.8.8 secondary 8.8.4.4
dns-lookup	dns-lookup <string>	Runs the DNS query for the Domain given as a parameter.	dns-lookup www.google.com
exit	exit	Exits the SonicCoreX with CLI console and switch to safemode menu.	exit

Command	Syntax	Description	Example
help	help	It shows the default help of the SonicCoreX with CLI console.	help
network	network interface <interface name> ip <ip address> netmask <netmask> gateway <gateway ip>	Configure network in safemode.	network interface enp11s0 ip 10.203.78.81 netmask 255.255.255.0 gateway 10.203.78.1
ping	• ping <ip/hostname> • ping ip <ip/hostname> • ping ip6 <ip/hostname>	Runs the ping command on the mentioned IP address or String	ping google.com OR ping ip google.com OR ping ip6 <ipv6 address>
restart	restart	• Restart the firewall in normal mode again without any parameters. • Restart the firewall in safemode with'enter-safemode' parameter.	restart OR restart enter-safemode
safemode	safemode	Restart the firewall in safemode.	safemode
show (normal mode)	• show system • show sonicos • show status • show network • show dns • show logs	• Shows system information • Shows sonicos information • Shows status information • Shows network information • Shows dns information • Shows logs information	show system OR show sonicos OR show network OR show dns OR show logs
shutdown	shutdown	Shut down the firewall.	shutdown
support-data	support-data	Sends logs to support.	support-data

Command	Syntax	Description	Example
update	• update check • update download • update install	Check, download, and install an available update.	update check OR update download OR update install
update-channel	• update-channel read • update-channel set <channel name> • update-channel restore	It is used to modify/read/restore the update channel to deliver updates	update-channel read OR update-channel set <channel name> OR update-channel restore

Upgrading SonicOS with Current Settings

You can update the SonicOS image on a SonicWall NSv remotely if the LAN or WAN interface is configured for management access. You can also connect to the virtual console, put the NSv into SafeMode, and perform the upgrade. See Using SafeMode to Upgrade the SonicOS Image for that procedure.

To upload a new upgrade image to your SonicWall NSv and restart using current configuration settings:

1. Download the SonicOS SWI image file from MySonicWall and save it to a location on your local computer.

2. Point your browser to the NSv IP address, and log in as an administrator.

3. In the **DEVICE** view, on the **Settings > Firmware and Settings** page, on the **Firmware & Local Backups** screen, click **Upload Firmware**.

4. In the **Backup of current settings** popup dialog, click **OK** to continue with the firmware upload.

5. In the **Upload Firmware** dialog, browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it is displayed in the table on the **Firmware & Local Backups** screen.

6. Click the **Boot** icon in the **Uploaded Firmware Version** row and select **Boot firmware with Current Configuration**.

7. In the **Warning** dialog box, click **OK**. The NSv restarts and displays the login page.

8. Enter the user name and password.

    Your new SonicOS image version information is displayed on the **Settings > Status** page.

6

Upgrading SonicOS with Factory Default Settings

Upgrading with factory defaults returns your NSv to the initial configuration. All customized network settings, policies and other configuration will be lost, but logs and local backups remain in place.

To upload a new image to your NSv and restart it using the default configuration:

1. Download the SonicOS *SWI* image file from MySonicWall and save it to a location on your local computer.

2. Point your browser to the NSv IP address, and log in as an administrator.

3. In the **DEVICE** view, on the **Settings > Firmware and Settings** page, use **Create Backup** to create a local or cloud backup.
    Wait for the backup to complete.

4. On the **Firmware & Local Backups** screen, click **Upload Firmware**.

5. In the **Backup of current settings** popup dialog, click **OK** to continue with the firmware upload.

6. In the **Upload Firmware** dialog, browse to the location where you saved the SonicOS image file, select the file, and click **Upload**. After the image finishes uploading, it is displayed in the table on the **Firmware & Local Backups** screen.

7. Click the **Boot** icon in the **Uploaded Firmware Version** row and select **Boot firmware with Factory Default Configuration**.

8. In the **Warning** dialog box, click **OK**. The NSv restarts and then displays the SonicOS login prompt.
    ⓘ | **NOTE:** The IP address for the X0 (LAN) interface reverts to the default, 192.168.168.168. You can log into SonicOS by connecting to X0 and pointing your browser to https://192.168.168.168. You can also use the virtual console to configure the LAN or WAN IP address, and then log in. See the *NSv Series Getting Started Guide* for information about using the virtual console.

9. Enter the user name and password.
    Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, MyP@ssw0rd.

10. Perform the following steps to change password:

    a. In the **Old Password** text box, enter your default password that was provided.

    b. In the **New Password** text box, enter your new password.

    c. In the **Confirm Password** text box, re-enter the new password again.

11. Click **Change Password**.

12. Your new SonicOS image version information is displayed on the **Settings > Status** page.

7

Upgrading a High Availability Pair

SonicOS on NSv Series supports High Availability (HA) on VMware ESXi, Hyper-V, KVM, and Azure platforms.

HA Stateful Synchronization is supported, which means that the secondary unit will automatically synchronize with the primary unit when SonicOS is updated on the primary. Simply upgrade the primary unit as described in Upgrading SonicOS with Current Settings.

However, when upgrading a High Availability pair using **System Update**, upgrade each unit individually. See the Upgrading via System Update in the NSv Management Console for details.

Using SafeMode to Upgrade the SonicOS Image

If you are unable to connect to the SonicOS management interface, you can restart the SonicWall NSv in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes some of the functionality available in the **DEVICE | Settings > Firmware and Settings** page.

When you access the SafeMode interface in your browser, you will be prompted to enter the *Maintenance Key* for your NSv.

- In SonicOS 7.0.0, you must obtain the Maintenance Key from MySonicWall.
- In SonicOS 7.0 and 7.1, you can use the Auth Code as the key if your NSv is unregistered. The Auth Code is available in the SonicOS web management interface. After the appliance is registered, you will need to use the Maintenance Key, which is available from MySonicWall.

Topics:

- To obtain the Maintenance Key for your Appliance
- To use SafeMode to upgrade the SonicOS 6/6.5 and 7.0 image file (SWI)
- To use SafeMode to upgrade the SonicOS 7.1 image file (Sig)

To obtain the Maintenance Key for your appliance:

1. Log into your MySonicWall account at https://www.mysonicwall.com.
2. Navigate to **My Workspace> Products** and locate your NSv in the table.
3. Click on the serial number for your NSv to display a window frame with Product Details, Licenses, Firmware and Cloud Backup.
4. In the **Product Details** screen, move your mouse pointer over the "eye" icon next to **Maintenance Key**. The key value is displayed in a popup until you move your mouse. Make a note of the key.
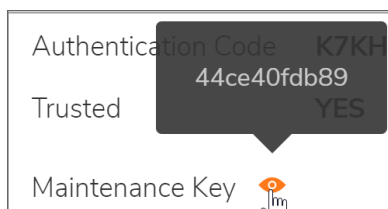
To use SafeMode to upgrade the SonicOS 6/6.5 and 7.0 image file (SWI):

1. Launch the virtual console and then click inside the console window.

2. Press **Ctrl+s** and then press the **spacebar** to switch to the NSv management console.

3. In the console, use the arrow keys to select the **Reboot | Shutdown** option and then press **Enter**. The right pane displays the **Reboot | Shutdown** options.

4. Navigate down to the **Boot SonicWall into safemode** option to highlight **Enable**, and then press **Enter**.
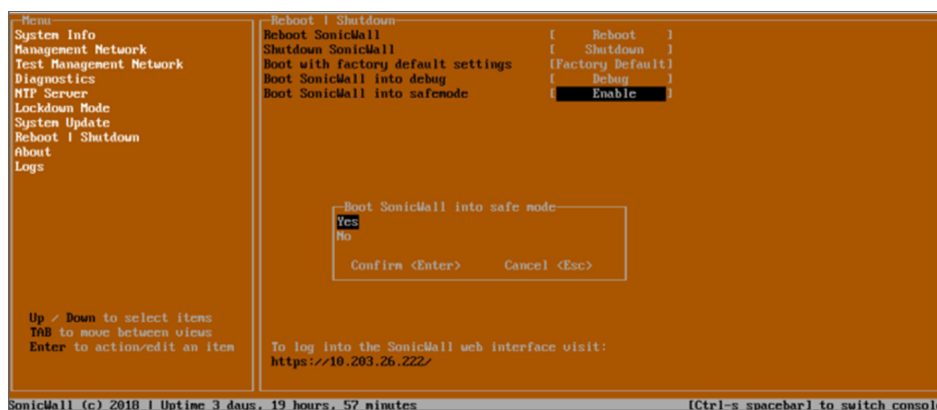
5. Select **Yes** in the confirmation dialog and press **Enter** to confirm.

6. The NSv immediately reboots and comes back up in SafeMode. When viewing the NSv management console in SafeMode, the URL for the SafeMode **web** interface is displayed at the bottom of the screen.

   In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

7. In a browser, navigate to the URL provided at the bottom of the NSv management console screen.

   The SafeMode web management interface displays.
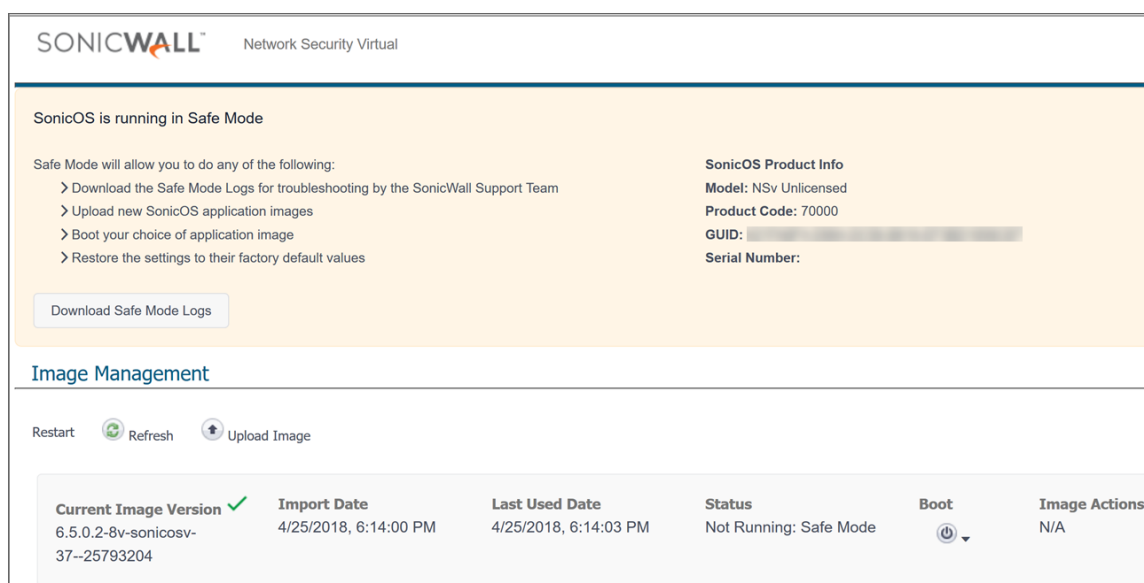
8. Click **Upload Image** button to select the *SWI* file that you downloaded from MySonicWall, and then browse to the location where you saved the SonicOS image, select the file, and click **Upload**. Once the upload completes, the image is available in the **Image Management** list in the SafeMode web interface.

9. Click the **Boot** button in the row for **Available Image Version** and select one of the following:

   - **Boot Available Image with Current Configuration**

     Use this option to restart the NSv with your current configuration settings.

   - **Boot Available Image with Factory Default Configuration**

     Use this option to restart the NSv with factory default configuration settings. The configuration settings revert to default values, but logs and local backups remain in place.

   - **Boot Available Image with Backup Configuration**

     Use this option to restart the NSv with saved backup configuration settings. You can choose which backup to use.

10. In the confirmation dialog, click **Boot** to proceed.

    The NSv reboots with the new image

11. After successfully booting the SonicOS image, if the login screen is not displayed, point your browser to the firewall IP address. If you booted with factory default settings, the default IP address of the X0 interface is 192.168.168.168.

12. Enter the user name and password.
    Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, MyP@ssw0rd.

13. Perform the following steps to change password:

    a. In the **Old Password** text box, enter your default password that was provided.

    b. In the **New Password** text box, enter your new password.

    c. In the **Confirm Password** text box, re-enter the new password again.

14. Click **Change Password**.

You can manage the NSv from the X0 interface or another LAN interface, or from the WAN interface, if configured.
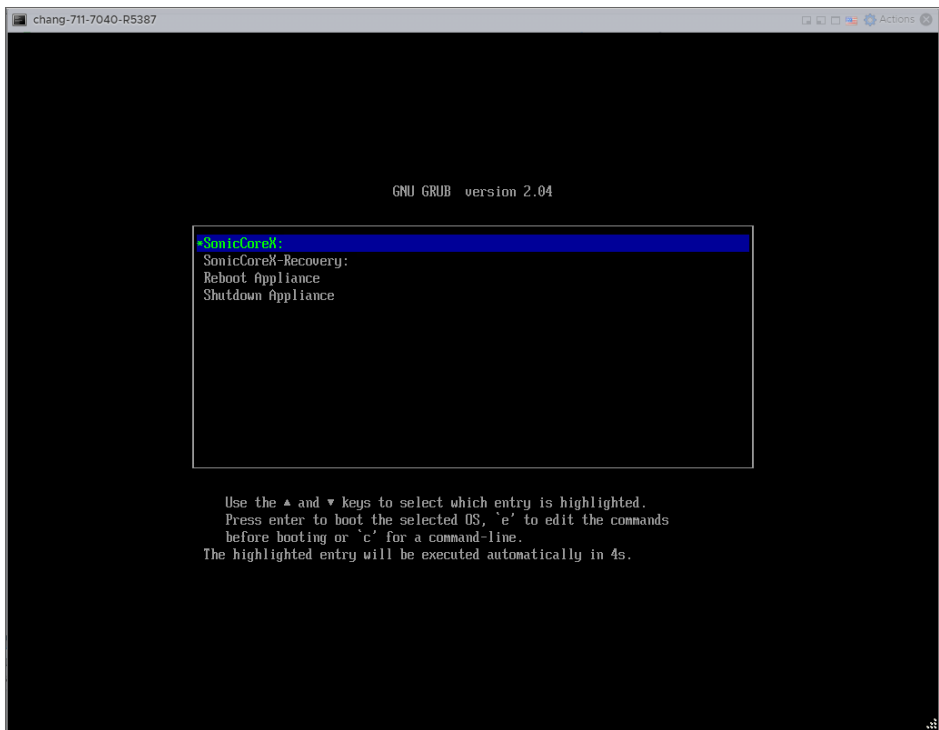
To use SafeMode to upgrade the SonicOS 7.1 image file (Sig):

1. Launch the virtual console and then click inside the console window.

2. The CLI console displays, enter the user name and password.

3. Enter the command **safe mode** and type **yes** to enter into safe mode.

```
User:admin
Password:

admin@00401038BB03> safemode
Are you sure you wish to enter into safemode? (yes/cancel)
[cancel]:
SonicWall (c) 2023 |                                    [Ctrl-s spacebar] to switch console
```

4. Select the SonicCoreX option and then press **Enter**.

   ⓘ | **NOTE:** The highlighted entry will be executed automatically in 4 seconds.

```
chang-711-7040-R5387                                        ▣ ▣ ▢ ▦ ⚙ Actions ⊗




                          GNU GRUB  version 2.04

        ┌────────────────────────────────────────────────────────────┐
        │*SonicCoreX:                                                  │
        │ SonicCoreX-Recovery:                                         │
        │ Reboot Appliance                                             │
        │ Shutdown Appliance                                           │
        │                                                              │
        │                                                              │
        │                                                              │
        │                                                              │
        │                                                              │
        └────────────────────────────────────────────────────────────┘

        Use the ▲ and ▼ keys to select which entry is highlighted.
        Press enter to boot the selected OS, `e' to edit the commands
        before booting or `c' for a command-line.
     The highlighted entry will be executed automatically in 4s.
```

5. When the appliance boots into SafeMode., after initializing SonicWall appliance page displays the list of accessible IP addresses is shown in the CLI console.

```
SonicWALL NSv Unlicensed Safe Mode -
  * Safemode : SonicCoreX 7.1.x-R5375 (nsv-vmware 2023-12-01 23:11:31)
  * Appliance rebooted to enter Safe Mode on user request.
  * Appliance booted from
Recovery Menu Available on:
  * Serial port console
Safemode is accessible via X0 port at:
  * https://192.168.168.168/
  * https://169.254.168.168/
Installed Firmware:
  * Current Version: SonicOSX 7.1.1-7039-R5375
  * Rollback Version: SonicOSX 7.1.1-7040-R5387


Recovery menu:
 0)   Enable maintenance mode
 1)   Restart SonicWall <SonicOSX 7.1.1-7039-R5375>
Enter an option: 0
```

6. Using a web browser, enter the appropriate URL in the address bar to login the safemode GUI using X0 port IP address. The following interface displays.
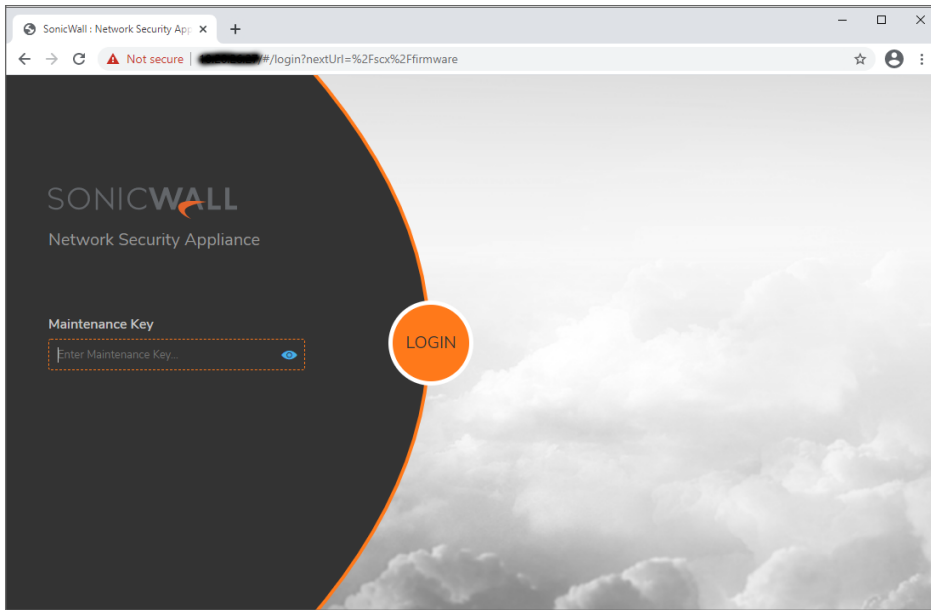
7. Enter the maintenance key and click login.
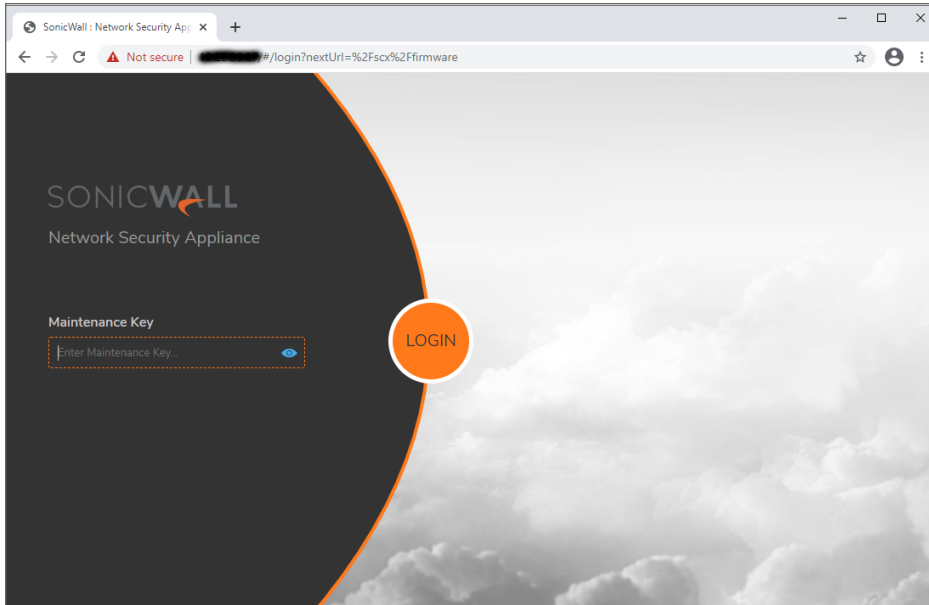
8. The firmware version page is where you can reboot the appliance, upload and install firmware upgrades, each with different configurations. In addition, the page facilitates other possible operations including performing a full Factory Reset or even Wiping the Appliance. The page lists the Current Firmware Image along with all of the Available Firmware Images - uploaded or present on a mounted USB drive.
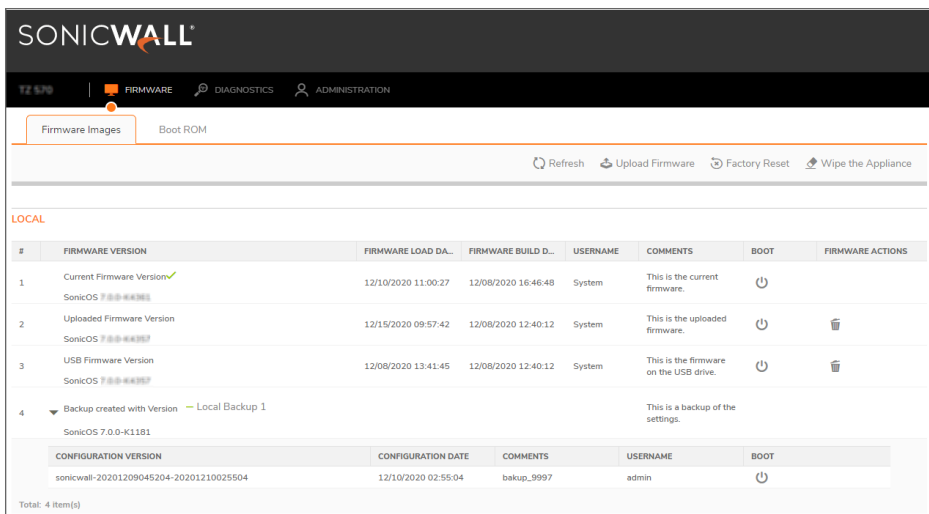
9. To boot the currently installed firmware image, click on the Boot button on the appropriate row in the table. A popup menu will appear asking whether you want to use the Current Configuration or revert to the Default Configuration. The appliance will be restarted with your choice of configuration.
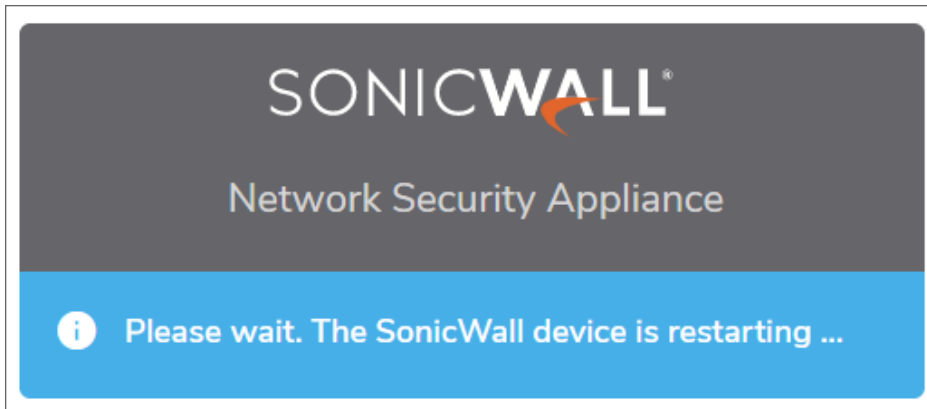
10. Click the **Boot** button in the row for **Available Image Version** and select one of the following:

    - **Boot Available Image with Current Configuration**
      Use this option to restart the NSv with your current configuration settings.

    - **Boot Available Image with Factory Default Configuration**
      Use this option to restart the NSv with factory default configuration settings. The configuration settings revert to default values, but logs and local backups remain in place.

    - **Boot Available Image with Backup Configuration**
      Use this option to restart the NSv with saved backup configuration settings. You can choose which backup to use.

11. In the confirmation dialog, click **Boot** to proceed.
    The NSv reboots with the new image

12. After successfully booting the SonicOS image, if the login screen is not displayed, point your browser to the firewall IP address. If you booted with factory default settings, the default IP address of the X0 interface is 192.168.168.168.

13. Enter the user name and password.
    Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, MyP@ssw0rd.

14. Perform the following steps to change password:

    a. In the **Old Password** text box, enter your default password that was provided.

    b. In the **New Password** text box, enter your new password.

    c. In the **Confirm Password** text box, re-enter the new password again.

15. Click **Change Password**.

16. You can manage the NSv from the X0 interface or another LAN interface, or from the WAN interface, if configured.

# Upgrading an Existing Deployment from SonicOS 6.5.4.v to SonicOS 7.0

SonicWall provides the Secure Upgrade process for upgrading an existing SonicOS 6.5.4.v NSv deployment to SonicOS 7.0 or higher.

Upgrade from 6.5.4.v to 7.0 requires a Secure Upgrade license key that is purchased separately. You can choose from any of the following:

- SONICWALL NSV 270 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 470 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 870 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 270 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 470 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 870 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)

To upgrade an existing SonicOS 6.5.4.v NSv deployment to SonicOS 7.0 or higher:
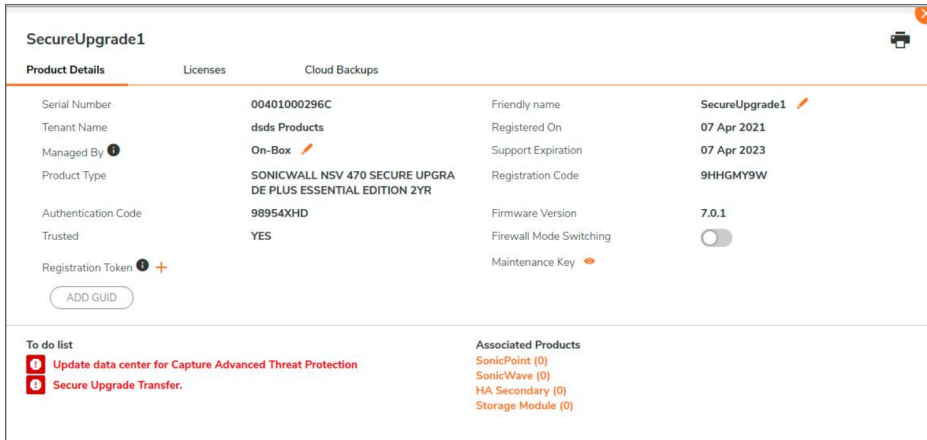
1. Purchase a Secure Upgrade license key.

2. Log into MySonicWall and register the Secure Upgrade serial number. Enter a descriptive "friendly" name in the available field, shown here as "SecureUpgrade1".
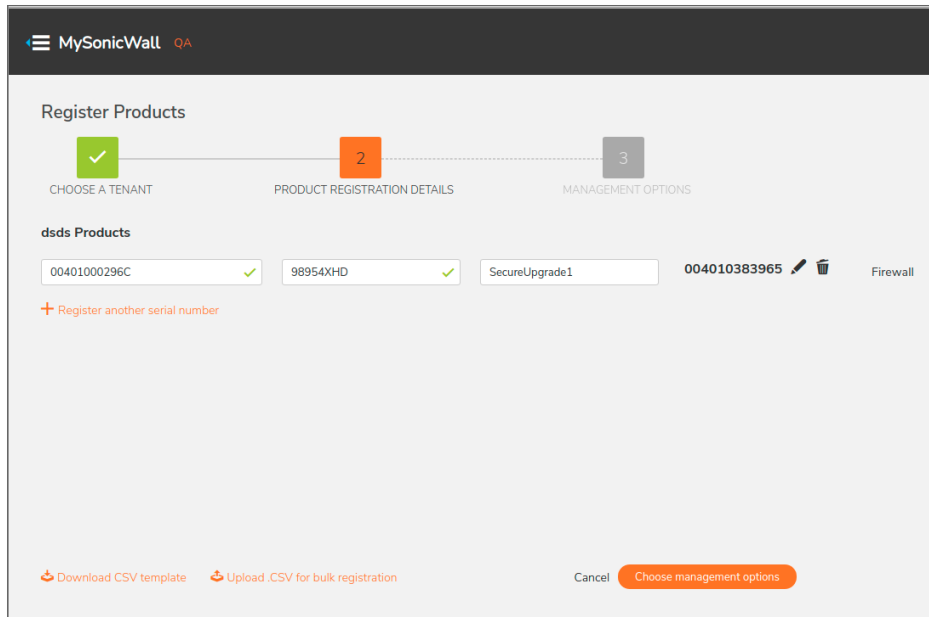
3. Click **Choose management options**.

4. In the Secure Upgrade popup window, select **Register Only** at the top.
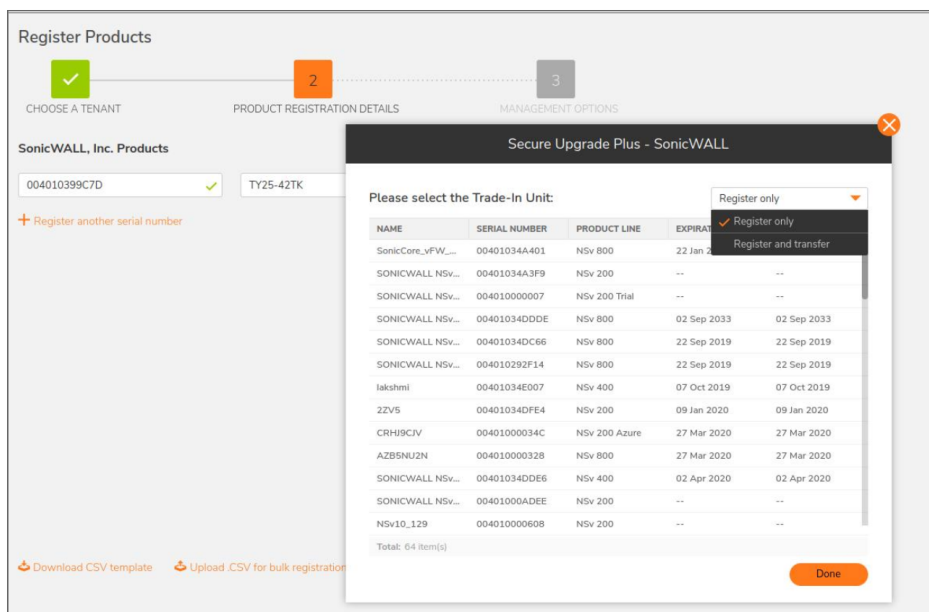
5. Select the Trade-In Unit from the list of registered NSv instances. This is the SonicOS 6.5.4.v NSv instance to be upgraded to SonicOS 7.0.

6. Click **Done** after selecting the Trade-In Unit. The Secure Upgrade serial number is then registered to your MySonicWall account.

7. The action item **Secure Upgrade Transfer** is added to the **To do list** at the bottom of the page.

You can perform the service transfer *after* you have deployed the SonicOS 7.0 NSv instance and moved the configuration settings ("prefs") from the SonicOS 6.5.4.v NSv to the new SonicOS 7.0 NSv.

The service transfer moves all active services from the SonicOS 6.5.4.v NSv to the new SonicOS 7.0 NSv and then deregisters the SonicOS 6.5.4.v NSv.

(i) | **NOTE:** If you do not perform the service transfer within 60 days, the transfer will be performed automatically.

8. Deploy a new SonicOS 7.0 NSv instance with the desired model and platform. Refer to the *NSv Getting Started Guide* for the installation procedure.

9. Register the SonicOS 7.0 NSv using the **Secure Upgrade** serial number. When prompted to select either Classic mode or Policy mode, select Classic mode. Classic mode supports configuration settings import from a SonicOS 6.5.4.v NSv.

    Registration initiates a 60-day countdown at the end of which the SonicOS 6.5.4.v NSv is deregistered, completing the Secure Upgrade Transfer.

10. Log into the SonicOS 6.5.4.v NSv and export the configuration settings to a file on your management computer.

11. Using the migration tool (https://migratetool.global.sonicwall.com/), migrate the SonicOS 6 NSv preferences to SonicOS 7.0 NSv model.

12. Log into the SonicOS 7.0 NSv and import the configuration settings.
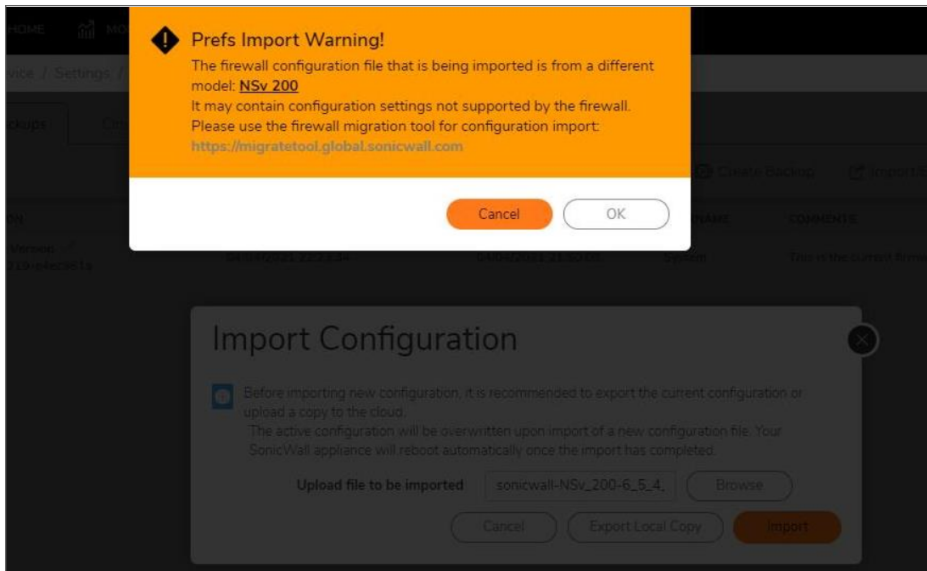
The upgrade is now complete and the SonicOS 7.0 NSv is ready for use.

9

Performing a Model Upgrade

Model Upgrade provides additional cores to increase computing power. You can upgrade your NSv to a model with a higher number of cores by selecting and purchasing the desired SKU for the higher model on MySonicWall and then applying the activation key on the Service Management page. Model Upgrade SKUs are available for single NSv appliances and for High Availability pairs.

Model Upgrade on NSv AWS or NSv Azure platforms might require moving to a new virtual machine model from the vendor (Amazon AWS or Microsoft Azure) if it does not already have the CPU and memory allocations required for the new NSv model, For information about VM models supported by these vendors, refer to the *NSv Series Getting Started Guide* for your platform.

ⓘ **NOTE:** Be sure to manually update the memory and CPU/processor settings in the VM console before this upgrade. For details about changing your hypervisor settings, see the *Upgrading to a Higher Capacity NSv Model* section in the *NSv Series Getting Started Guide* for your platform. For the new memory and CPU/processor values, refer to the *Product Matrix and Requirements* section in the *NSv Series Getting Started Guide* for your platform.

Upon activation of the Model Upgrade service, the product ID of the NSv is updated to match the ID of the new model. This update is also communicated to the SonicWall License Manager to update the product code for the NSv serial number.

SUPPORTED MODEL UPGRADES, SINGLE NSV AND HA PAIRS, ALL NSV PLATFORMS

	NSv 270	NSv 470	NSv 870
NSv 270		Supported	Supported
NSv 470			Supported

Depending on your NSv deployment, refer to one of the following sections:

- For Model Upgrade on a single NSv, see Performing a Model Upgrade on a Single NSv.
- For Model Upgrade on NSv AWS or NSv Azure platforms when the current NSv does not already have the CPU and memory allocations in the vendor VM that are required for the new NSv model, see Performing a Model Upgrade on NSv AWS or NSv Azure.
- For Model Upgrade on a High Availability pair, see Performing a Model Upgrade on an HA Pair.

Performing a Model Upgrade on a Single NSv

This procedure works for Model Upgrade on NSv ESXi, NSv Hyper-V, and NSv KVM, and **Step 2** through **Step 9** also apply to NSv AWS or NSv Azure platforms that have enough CPU and memory for the upgrade in the underlying vendor VM model.

To perform a model upgrade on a single NSv:

1. In the VM console of your hypervisor, adjust the memory and CPU/processor settings of the NSv you are upgrading to match the required settings for the new model.
2. In a browser on your management computer, log into your MySonicWall account at https://www.mysonicwall.com.
3. In MySonicWall, navigate to **Product Management > My Products** in the left navigation pane to display the list of your registered NSv virtual firewalls.
4. Click the link for the NSv that you wish to upgrade. The **Service Management** page opens.
5. Under **Applicable Services** in the **GATEWAY SERVICES** section, click the Cart icon in the Model Upgrade row to buy the SKU for the higher model. Or, obtain the license from your SonicWall sales contact. Copy the resulting activation key into your clipboard or make a note of it.
6. Click the Key icon in the Model Upgrade row to open the **Activate Service: Model Upgrade** dialog.
7. Enter the key into the **Activation Key** field and then click **Submit**.
8. Log into the NSv, navigate to the **DEVICE | Settings > Licenses** page and click **Synchronize**.
9. Restart the NSv if prompted, or navigate to **Settings > Restart** and click **Restart System** to reboot the NSv.
   Your NSv is updated to the new model, both in MySonicWall and in the License Manager. All services and maximum limits are now applied according to the updated Product ID.

Performing a Model Upgrade on NSv AWS or NSv Azure

If your NSv AWS or NSv Azure does not already have the CPU and memory allocations in the vendor VM that are required for the new NSv model, use the following procedure for the Model Upgrade. If the CPU and memory are already adequate for the new NSv model, you can use the steps provided in Performing a Model Upgrade on a Single NSv.

To perform a model upgrade on NSv AWS or NSv Azure:

1. Log into your current NSv and navigate to **DEVICE | Settings > Firmware and Settings**.
2. Click **Import/Export Configuration** and select **Export Configuration** to export your settings.

3. Navigate to **HOME | Dashboard > System > Device** and write down the values shown in the **Serial Number** and **Authentication Code** fields.

4. Navigate to **DEVICE | Settings > Licenses** and click **DEREGISTER**, then click **OK** in the confirmation dialog.

5. In either Amazon AWS or Microsoft Azure, deploy the same NSv model as you had before, but select a higher VM model from the vendor, with the CPU and memory capacity required for your desired higher NSv model. For information about VM models supported by these vendors, refer to the *NSv Series Getting Started Guide* for your platform.

6. Log into your new NSv and register it using the same serial number and authentication code that you saved in Step 3.

7. Navigate to **DEVICE | Settings > Firmware and Settings** and select **Import Configuration** to import your saved settings.

8. To complete the Model Upgrade process, perform Step 2 through Step 9 of the procedure in Performing a Model Upgrade on a Single NSv.

Performing a Model Upgrade on an HA Pair

For Model Upgrade on a High Availability pair, you need two activation keys, one for the primary unit and one for the secondary unit. The primary unit upgrade key is generated using a regular SKU, while the secondary unit upgrade key is generated using an HA SKU. First, associate the HA pair (if not already associated) in MySonicWall before the model upgrade, then perform similar steps as you would for a single node model upgrade on both the primary and secondary units to complete the model upgrade on your HA pair.

To perform a model upgrade on a High Availability pair:

1. In the VM console of your hypervisor, adjust the memory and CPU settings of the NSv you are upgrading to match the required settings for the new model.

2. Log into your MySonicWall account and associate the HA secondary unit with the primary unit (if not already associated).

3. Click the link for the primary unit to open the **Service Management** page for it. Buy the Model Upgrade license using the Cart icon, if needed.

4. Click the Key icon in the Model Upgrade row to open the **Activate Service: Model Upgrade** dialog.

5. Enter the key into the **Activation Key** field and then click **Submit**.

6. Go to the **Service Management** page for the secondary unit. Buy the Model Upgrade license (HA SKU) using the Cart icon, if needed.

7. Click the Key icon in the Model Upgrade row, enter the key (the HA SKU key) into the **Activation Key** field and then click **Submit**.

8. Log into the HA Pair as an administrator. This logs you into the active (primary) unit.

9. Navigate to the **DEVICE | Settings > Licenses** page and click **Synchronize**.

10. Restart the NSv if prompted, or navigate to **DEVICE | Settings > Restart** and click **Restart System** to reboot the primary unit.

    After bootup, the NSv will stay in the STANDBY state and the previously idle (secondary) NSv will become the active unit

11. Log into the HA Pair again, as administrator. This logs you into the secondary NSv, which is now the active unit.

12. Navigate to the **DEVICE | Settings > Licenses** page and click **Synchronize**.

13. Restart the NSv if prompted, or navigate to **DEVICE | Settings > Restart** and click **Restart System** to reboot the secondary unit.

    While this unit boots up, the first unit becomes active again and the HA Pair is upgraded and synchronized.

Importing Configuration Settings

You can import configuration settings from one NSv model to another on the same platform, which can save a lot of time when replacing or deploying a new NSv. This feature is also useful when you need multiple NSv virtual firewalls with similar configuration settings.

Before importing settings, you need a configuration file exported from an NSv whose settings you want. You can export configuration settings from an NSv to a file on your management computer at any time.

To export the configuration settings from an appliance running SonicOS 7, navigate to the **DEVICE | Settings >
Firmware and Settings** page, click **Import/Export Configuration** and select **Export Configuration**. In the
popup dialog, click **Export** to complete the process. Refer to Creating a System Backup and Exporting Your
Settings for more information.

You can then import the settings file to another appliance by selecting **Import Configuration** from the
Import/Export Configuration list.

You can also import settings from an NSv running SonicOS 6.5.4.4v to an NSv on the same platform running
SonicOS 7.

Topics:

- Settings Import Support Across NSv Platforms
- Settings Import Support Across NSv Models
- Settings Export and Import Procedures

Settings Import Support Across NSv Platforms

Configuration settings import is supported between NSv virtual firewalls on the same platform, but cross-platform settings import is not supported. The NSv Cross-Platform Settings Import Support table illustrates support for importing configuration settings between NSv virtual firewall platforms.

NSV CROSS-PLATFORM SETTINGS IMPORT SUPPORT

		DESTINATION PLATFORM				
		NSv AWS	NSv Azure	NSv Hyper-V	NSv KVM	NSv VMware
SOURCE PLATFORM	NSv AWS	Y	N	N	N	N
	NSv Azure	N	Y	N	N	N
	NSv Hyper-V	N	N	Y	N	N
	NSv KVM	N	N	N	Y	N
	NSv VMware	N	N	N	N	Y

LEGEND

Y	Supported
N	**Unsupported**. While importing the settings file may be successful across platforms with equivalent features, cross-platform settings import is not recommended.

Settings Import Support Across NSv Models

The following table illustrates support for importing configuration settings between NSv virtual firewall models. The source firewalls are in the left column, and the destination firewalls are listed across the top.

CONFIGURATION SETTINGS IMPORT SUPPORT ON NSV MODELS

DESTINATION NS*v*

	NS*v* 270	NS*v* 470	NS*v* 870
NS*v* 270	Y	Y	Y
NS*v* 470	N	Y	Y
NS*v* 870	N	N	Y
NS*v* 10	Y	Y	Y
NS*v* 25	Y	Y	Y
NS*v* 50	Y	Y	Y
NS*v* 100	Y	Y	Y
NS*v* 200	Y	Y	Y
NS*v* 300	N	Y	Y
NS*v* 400	N	Y	Y
NS*v* 800	N	N	Y
NS*v* 1600	N	N	N

SOURCE NS*v* (row labels in left column)

LEGEND

Y	Supported
N	**Unsupported**. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.

Settings Export and Import Procedures

To export the configuration settings from an NSv running SonicOS 7:

1. Navigate to the **DEVICE | Settings > Firmware and Settings** page in SonicOS.

2. On the **Firmware & Local Backups** screen, click **Import/Export Configuration** and select **Export Configuration**.

   The exported configuration settings file is saved to your **Downloads** folder. The file type extension is **.exp**.

To export the configuration settings from an NSv running SonicOS 6.5.4.4v:

1. Navigate to the **MANAGE | Updates | Settings** page in SonicOS.

2. Click the **Import/Export Configuration** drop-down list and select **Export Configuration**.

3. In the popup dialog, click **Export**.

   The exported configuration settings file is saved to your **Downloads** folder. The file type extension is **.exp**.

To import configuration settings to an NSv running SonicOS 7:

1. Navigate to the **DEVICE | Settings > Firmware and Settings** page in SonicOS.

2. On the **Firmware & Local Backups** screen, click **Import/Export Configuration** and select **Import Configuration**.

3. The popup dialog advises you to export a copy of the current configuration before importing new configuration settings. Do one of the following:

   - Click **Export Local Copy** to export the current settings to your management computer. Then repeat the step to open the **Import Configuration** dialog.

   - If you have already saved the current settings or prefer not to, click **Browse** and select the **.exp** file to import, or enter the filename into the **Upload file to be imported** field. Then click **Import**.

4. The imported configuration overwrites the existing configuration settings and then the NSv automatically reboots.

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 https://mysonicwall.com
- Learn about SonicWall Professional Services at https://sonicwall.com/pes.
- 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

SonicOS Upgrade Guide for the NSv Series
Updated - December 2023
Software Version - 7.1
232-005380-20 Rev C

End User Product Agreement

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

Open Source Code

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

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