SonicWall™ SonicOS 6.2 Upgrade Guide

March 2017

This Upgrade Guide provides instructions for upgrading your SonicWall™ network security appliance from SonicOS 6.1 firmware or a previous version of SonicOS 6.2 to the latest version of SonicOS 6.2.

This guide also provides information about importing the configuration settings from an appliance running SonicOS 5.8, 5.9, 6.1, or 6.2 to an appliance running SonicOS 6.2. See Importing Configuration Settings for details about the models and firmware versions supported.

Topics:

⚠ CAUTION: **On a SuperMassive™ 9800, you might need to update the ChassisOS and FailSafe versions prior to installing SonicOS 6.2.1.3 or higher. You can view these versions in SafeMode. See the SonicOS 6.2.1.x Release Notes for required versions. Please contact SonicWall Technical Support before upgrading your SuperMassive 9800 appliance if these versions are out of date.**

ⓘ **NOTE:** Starting in SonicOS 6.2.5.0, all SonicOS default certificates are updated to 2048-bit/SHA-256 encryption, except the Default SonicWall DPI-SSL CA certificate which is updated starting in SonicOS 6.2.5.1. After upgrading your appliance to 6.2.5 or higher, do one or both of the following to replace the older 1024-bit certificates with the new ones:

- Navigate to the System > Administration page, scroll down to **Web Management Settings**, and click the **Regenerate certificate** button. This regenerates the self-signed HTTPS management certificate.
- Navigate to the System > Settings page, click **Export Settings** to save a copy of your configuration settings, and then click the Boot icon for **Current Firmware with Factory Default Settings**. This will regenerate all default certificates. After the restart, click the **Import Settings** button to import your settings and return to your previous configuration.

Obtaining the Latest SonicOS Firmware

To obtain a new SonicOS firmware image file for your SonicWall security appliance:

1. In a browser on your management computer, log into your MySonicWall account at http://www.mysonicwall.com.
2. In MySonicWall, click **Downloads** in the left navigation pane to display the Download Center screen.
3. Select your product in the **Software Type** drop-down list to display available firmware versions.
4. To download the firmware to your computer, click the link for the firmware version you want. You can download the *Release Notes* and other associated files in the same way.

Creating a System Backup and Exporting Your Settings

Before beginning the update process, make a system backup on your SonicWall appliance.

On SonicWall NSA and SuperMassive 9000 series appliances, the backup feature saves a copy of the current system state, firmware, and configuration settings on your appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

On SonicWall TZ series and SOHO Wireless appliances, you can create a backup of your current configuration settings on the appliance, to be used with the current firmware version or with a newly uploaded firmware version.

You can also export the appliance 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 appliance or into the same appliance if it is necessary to reboot the firmware with factory default settings.

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

1. On the System > Settings page, do one of the following:
   - On a SuperMassive or NSA appliance, click **Create Backup**. SonicOS takes a “snapshot” of your current system state, firmware, and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing System Backup image, if any. The **System Backup** entry is displayed in the Firmware Management table.
   - On a TZ or SOHO W appliance, click **Create Backup Settings**. SonicOS saves a small file on the appliance with all your configuration settings. Any previous backup settings file is overwritten. The Firmware Management table displays the **Current Firmware with Backup Settings** entry.

> ⓘ **NOTE:** A **Download** button is displayed in the Firmware Management table for the System Backup and the Backup Settings file. However, the downloaded files cannot be imported into another appliance, nor can they be uploaded like firmware. Use **Export Settings** to save your configuration settings for import into another appliance.

2. To export your settings to a local file, click **Export Settings** and then click **Export** in the popup window that displays the name of the saved file.

Upgrading Firmware with Current Settings

You can update the SonicOS image on a SonicWall security appliance remotely if the LAN or WAN interface is configured for management access. On SonicWall NSA or SuperMassive platforms, you can also connect directly to the MGMT port and point your browser to that IP address (http://192.168.1.254 by default) to log in and perform the upgrade.

To upload new firmware to your SonicWall appliance and use your current configuration settings upon startup:

1. Download the SonicOS firmware image file from MySonicWall and save it to a location on your local computer.
2. Point your browser to the appliance IP address, and log in as an administrator.
3. On the System > Settings page, click **Upload New Firmware**.
4. 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 Firmware Management table.
5. On the System > Settings page, click the Boot icon in the row for **Uploaded Firmware – New!**
6. In the confirmation dialog box, click **OK**. The appliance restarts and then displays the login page.
7. Enter your user name and password. Your new SonicOS image version information is displayed on the System > Status page.

Upgrading Firmware with Factory Default Settings

To upload new firmware to your SonicWall appliance and start it up using the default configuration:

1. Download the SonicOS firmware image file from MySonicWall and save it to a location on your local computer.
2. Point your browser to the appliance IP address, and log in as an administrator.
3. On the System > Settings page, do one of the following:

   - On a SuperMassive or NSA appliance, click **Create Backup**.
   - On a TZ or SOHO W appliance, click **Create Backup Settings**.

   Wait for the backup to complete.
4. Click **Upload New Firmware**.
5. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
6. On the System > Settings page, click the Boot icon in the row for **Uploaded Firmware with Factory Default Settings – New!**

7 In the confirmation dialog box, click **OK**. The appliance restarts and then displays the options to launch the Setup Wizard or go to the login page of the SonicOS management interface.

> ⓘ **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. On SonicWall NSA or SuperMassive platforms, you can also log in by connecting to the MGMT port and pointing your browser to http://192.168.1.254.

8 Enter the default user name and password (admin / password) to access the SonicOS management interface.

Using SafeMode to Upgrade Firmware

If you are unable to connect to the SonicOS management interface, you can restart the SonicWall security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the System > Settings page.

Topics:

- Using SafeMode on Most Platforms
- Using SafeMode on SuperMassive 9800

Using SafeMode on Most Platforms

This implementation of SafeMode is supported on the following platforms:

SuperMassive	NSA	TZ	SOHO
9200	2600	TZ300/TZ300W	SOHO W
9400	3600	TZ400/TZ400W	
9600	4600	TZ500/TZ500W	
	5600	TZ600	
	6600		

The SafeMode procedure uses a recessed ***SafeMode*** button in a small pinhole near the USB ports on the front of the SonicWall appliance.

To use SafeMode to upgrade firmware on a SonicWall security appliance:

1 Do one of the following:

- On a SonicWall TZ or SOHO W appliance, connect your computer to the X0 port on the appliance and configure your computer with an IP address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
- On a SonicWall NSA or SuperMassive appliance, connect your computer to the MGMT port on the appliance and configure your computer with an IP address on the 192.168.1.0/24 subnet, such as 192.168.1.20.

2 Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the SafeMode button on the security appliance for more than 20 seconds.

The Test light starts blinking when the appliance has rebooted into SafeMode.

3 Do one of the following to access the SafeMode management interface:

- On a SonicWall TZ or SOHO W appliance, point your browser to http://192.168.168.168.
- On a SonicWall NSA or SuperMassive appliance, point your browser to http://192.168.1.254.

4 Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.

5 Click the Boot icon in the row for one of the following:

- **Uploaded Firmware – New!**

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

- **Uploaded Firmware with Factory Default Settings – New!**

  Use this option to restart the appliance with factory default configuration settings.

6 In the confirmation dialog box, click **OK** to proceed.

7 After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicOS management interface.

On a SonicWall NSA or SuperMassive appliance, you can continue to manage the appliance from the MGMT interface at 192.168.1.254.

On all SonicWall platforms, you can manage the appliance from the X0 interface or another LAN interface, or from the WAN interface, if configured. The default IP address of the X0 interface is 192.168.168.168.

8 To manage the appliance from an interface other than the one to which your computer is physically connected:

a Disconnect your computer from the appliance.

b Reconfigure the computer to automatically obtain an IP address and DNS server address, or reset it to its normal static values.

c Connect the computer to your network or to the desired interface on the appliance.

d Point your browser to the appropriate WAN or LAN IP address of the appliance.

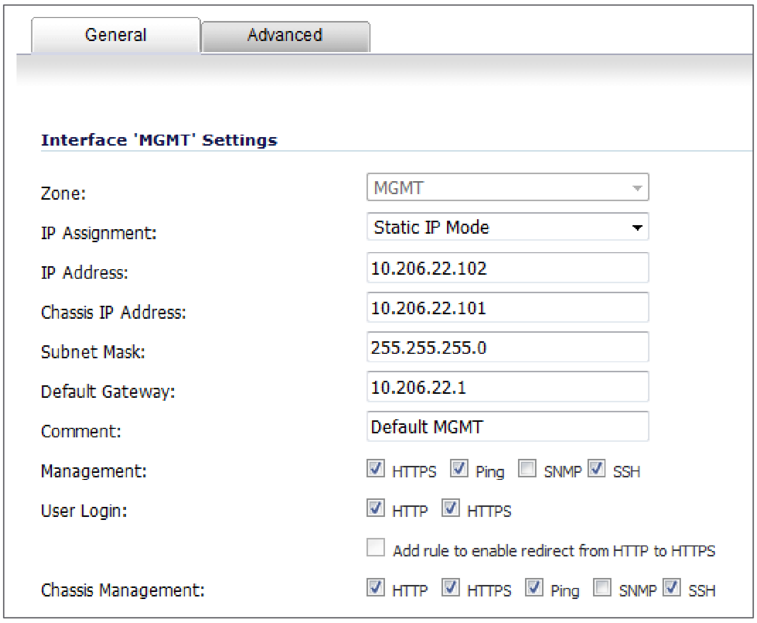
Using SafeMode on SuperMassive 9800

This implementation of SafeMode is supported on the SuperMassive 9800. You can view the **ChassisOS** and **FailSafe** versions in the SafeMode interface.

To use SafeMode to upgrade firmware on a SuperMassive 9800:

1 Log into the appliance and navigate to the Network > Interfaces page.

2 In the **Network Settings** table, click the Configure icon for the **MGMT** interface. The **Edit Interface – MGMT** dialog displays.



Interface 'MGMT' Settings

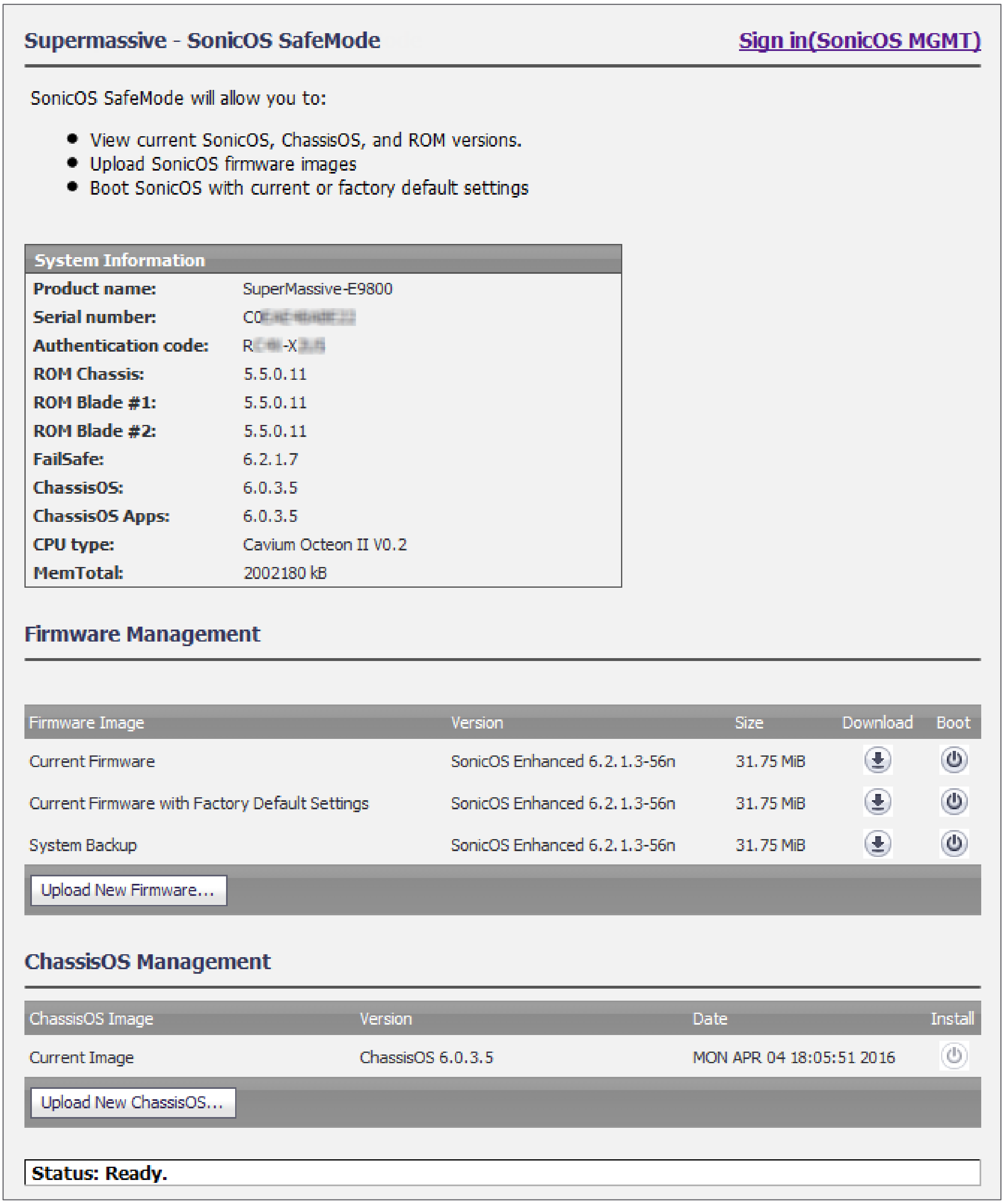
Zone:	MGMT
IP Assignment:	Static IP Mode
IP Address:	10.206.22.102
Chassis IP Address:	10.206.22.101
Subnet Mask:	255.255.255.0
Default Gateway:	10.206.22.1
Comment:	Default MGMT
Management:	☑ HTTPS ☑ Ping □ SNMP ☑ SSH
User Login:	☑ HTTP ☑ HTTPS
	□ Add rule to enable redirect from HTTP to HTTPS
Chassis Management:	☑ HTTP ☑ HTTPS ☑ Ping □ SNMP ☑ SSH

3 For **Chassis Management**, select the following checkboxes:

- **HTTP**
- **Ping**
- **SSH**

4 Click **OK**.

5 Point your browser to the chassis IP address, such as *http://10.206.22.101* (use the chassis IP address for the primary unit in an HA pair). The SonicOS SafeMode page displays.



SonicOS SafeMode will allow you to:

- View current SonicOS, ChassisOS, and ROM versions.
- Upload SonicOS firmware images
- Boot SonicOS with current or factory default settings

System Information	
Product name:	SuperMassive-E9800
Serial number:	C0[redacted]
Authentication code:	R[redacted]-X[redacted]
ROM Chassis:	5.5.0.11
ROM Blade #1:	5.5.0.11
ROM Blade #2:	5.5.0.11
FailSafe:	6.2.1.7
ChassisOS:	6.0.3.5
ChassisOS Apps:	6.0.3.5
CPU type:	Cavium Octeon II V0.2
MemTotal:	2002180 kB

Firmware Image	Version	Size	Download	Boot
Current Firmware	SonicOS Enhanced 6.2.1.3-56n	31.75 MiB	⬇	⏻
Current Firmware with Factory Default Settings	SonicOS Enhanced 6.2.1.3-56n	31.75 MiB	⬇	⏻
System Backup	SonicOS Enhanced 6.2.1.3-56n	31.75 MiB	⬇	⏻

ChassisOS Image	Version	Date	Install
Current Image	ChassisOS 6.0.3.5	MON APR 04 18:05:51 2016	⏻

Status: Ready.

6 Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.

7 Click the Boot icon in the row for one of the following:

- **Uploaded Firmware – New!**

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

- **Uploaded Firmware with Factory Default Settings – New!**

  Use this option to restart the appliance with factory default configuration settings.

8 In the confirmation dialog box, click **OK** to proceed.

9 After successfully booting the firmware, the login screen is displayed. Point your browser to the appliance IP address (not the Chassis IP address) and log in, or use the default IP address if you booted with factory default settings.

If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicOS management interface.

10 Navigate to the Network > Interfaces page.

11 In the **Network Settings** table, click the Edit icon for the **MGMT** interface.

12 For **Chassis Management**, clear the following checkboxes:

- **HTTP**
- **Ping**
- **SSH**

This disables the SafeMode feature and protects your appliance from unauthorized access.

13 Click **OK**.

About Upgrading and VPN Tunnels

Significant design changes for VPN tunnel interfaces are implemented in SonicOS 6.2.4, SonicOS 6.2.5, and again in SonicOS 6.2.6.

- SonicOS 6.2.3 and earlier versions support Unnumbered Tunnel Interfaces for static and dynamic (advanced) routing, while SonicOS 6.2.4 only supports Numbered Tunnel Interfaces including support for advanced routing. Upgrading from or importing settings from an earlier release to SonicOS 6.2.4 might require manual reconfiguration of tunnel interfaces.
- SonicOS 6.2.5 supports both Unnumbered Tunnel Interfaces and Numbered Tunnel Interfaces on all platforms. Upgrading from all earlier releases is fully supported. An Unnumbered TI is configured by creating a VPN policy of policy type Tunnel Interface and can only be used with static routing. A Numbered TI is configured by adding a VPN Tunnel Interface on the Network > Interfaces page, and can be used with static or dynamic routing.
- SonicOS 6.2.6 expands on the 6.2.5 capabilities by adding dynamic routing (RIP, OSPF) support on Unnumbered Tunnel Interfaces. Dynamic routing is enabled with the Allow Advanced Routing option on the Advanced tab when creating a VPN policy of policy type Tunnel Interface.

See the *SonicOS 6.2 Administration Guide* for more information.

Summary of tunnel interface support in SonicOS:

Firmware version	Tunnel interface support
SonicOS 5.8.1/5.8.4	Supports Unnumbered TI on all platforms.
SonicOS 5.9	Supports only Unnumbered TI on TZ 105/200/205/210 series and NSA 2400MX. The TZ 100 series do not support any dynamic routing (no Advanced Routing) over Unnumbered TI. Supports Numbered TI in addition to Unnumbered TI on all other platforms (TZ 215 series, NSA, E-Class NSA).

SonicOS 6.1	Supports Unnumbered TI on all platforms.
SonicOS 6.2 through 6.2.2.2 and 6.2.3.1	Supports Unnumbered TI on all platforms.
SonicOS 6.2.4	Supports Numbered TI on all platforms.
SonicOS 6.2.5	Supports Unnumbered TI and Numbered TI on all platforms. Only Numbered Tunnel Interfaces support dynamic routing.
SonicOS 6.2.6	Supports Unnumbered TI and Numbered TI on all platforms. Both Unnumbered TI and Numbered TI support dynamic and static routing.

For numbered tunnel interfaces, changes in SonicOS 6.2.4.2 and 6.2.5.1 can cause an OSPF MTU (maximum transmission unit) mismatch in the following situations:

- A tunnel using non-AES encryption is changed to AES after the firewall is upgraded from a previous version to 6.2.5.1 or higher.
- A tunnel using AES encryption exists between two firewalls running a previous version, and only one firewall is upgraded to 6.2.5.1 or higher.
- On a firewall running 6.2.4.2 or higher, the MTU is changed on the interface that terminates a VPN tunnel, causing the numbered tunnel interface MTU to change.

Administrators are advised to check the MTU setting on both VPN peering endpoints to ensure that the values match so that OSPF can establish neighbor adjacency.

See Knowledge Base article SW10735 for more information about OSPF and tunnel interfaces, available at: https://support.sonicwall.com/sonicwall-tz-series/kb?k=Interoperability+issue+for+OSPF+with+tunnel-interfaces+between+5.9.xx%2C+5.8.xx+and+6.xxx

Importing Configuration Settings

You can import configuration settings from one appliance to another, which can save a lot of time when replacing an older appliance with a newer model. This feature is also useful when you need multiple appliances with similar configuration settings.

Importing configuration settings, or preferences (“prefs”), to SonicWall network security appliances running SonicOS 6.2 is generally supported from the following SonicWall appliances running 5.8, 5.9, 6.1, or 6.2:

- SuperMassive 9600/9400/9200 (Gen 6)
- NSA 6600/5600/4600/3600/2600 (Gen 6)
- TZ600, TZ500/TZ500 W, TZ400/TZ400 W, TZ300/TZ300 W, SOHO/SOHO W (Gen 6)
- NSA E8510/E8500/E7500/E6500/E5500 (Gen 5)
- NSA 5000/4500/3500/2400, NSA 250M/250MW, NSA 220/220W (Gen 5)
- TZ 215/210/205/200/105/100 Series (Gen 5)

ⓘ **IMPORTANT:** See About Upgrading and VPN Tunnels for information about design changes for VPN tunnel interfaces in SonicOS 6.2.4, 6.2.5, and 6.2.6.

Importing configuration settings to a SuperMassive 9800 running SonicOS 6.2.1.x is supported from the following appliances running SonicOS 6.2.0.x:

- SuperMassive 9600/9400/9200
- NSA 6600/5600/4600/3600/2600

NOTE: Settings import to a SuperMassive 9800 from appliances running SonicOS versions other than 6.2.0.x or 6.2.1.x is not supported.

To export the configuration settings from an appliance, navigate to the System > Settings page in SonicOS and click the Export Settings button. You can then import the settings file to another appliance by clicking the Import Settings button on that page.

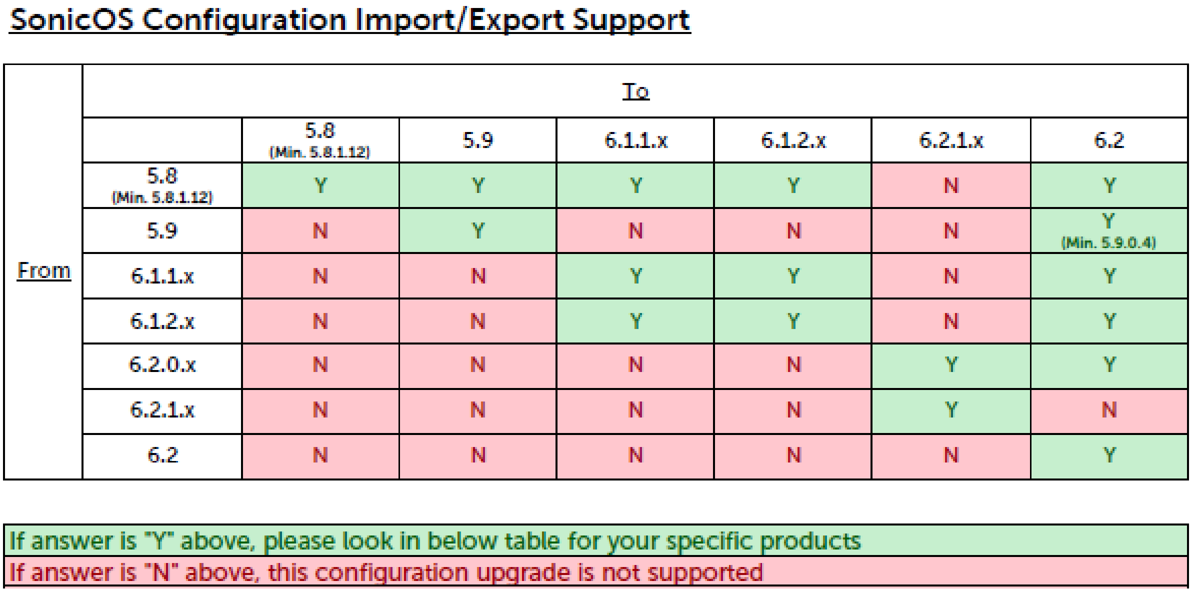
The tables in the following sections provide details about which firmware versions or which models support importing configuration settings to other models and firmware versions for 5.8, 5.9, 6.1, or 6.2.

See the following sections:

- SonicOS Versions Supporting Configuration Settings Import
- Platform Configuration Import Support Tables

SonicOS Versions Supporting Configuration Settings Import

The following table illustrates the supported source and destination versions of SonicOS when importing configuration settings from one appliance to another.



SonicOS Configuration Import/Export Support

		To					
		5.8 (Min. 5.8.1.12)	5.9	6.1.1.x	6.1.2.x	6.2.1.x	6.2
From	5.8 (Min. 5.8.1.12)	Y	Y	Y	Y	N	Y
	5.9	N	Y	N	N	N	Y (Min. 5.9.0.4)
	6.1.1.x	N	N	Y	Y	N	Y
	6.1.2.x	N	N	Y	Y	N	Y
	6.2.0.x	N	N	N	N	Y	Y
	6.2.1.x	N	N	N	N	Y	N
	6.2	N	N	N	N	N	Y

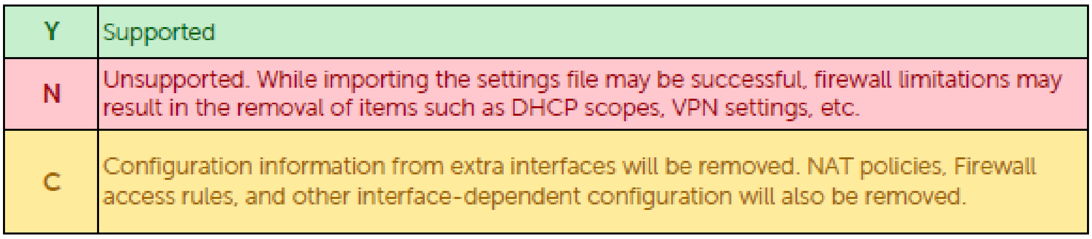
If answer is "Y" above, please look in below table for your specific products

If answer is "N" above, this configuration upgrade is not supported

Platform Configuration Import Support Tables

The tables in the following sections show the SonicWall firewalls whose configuration settings can be imported to SonicWall Gen 6 platforms running SonicOS 6.2. The source firewalls are in the left column, and the destination firewalls are listed across the top.

The legend for these tables is:



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.
C	Configuration information from extra interfaces will be removed. NAT policies, Firewall access rules, and other interface-dependent configuration will also be removed.

See the following sections:

- TZ / SOHO W Configuration Import Support
- NSA / SuperMassive Configuration Import Support

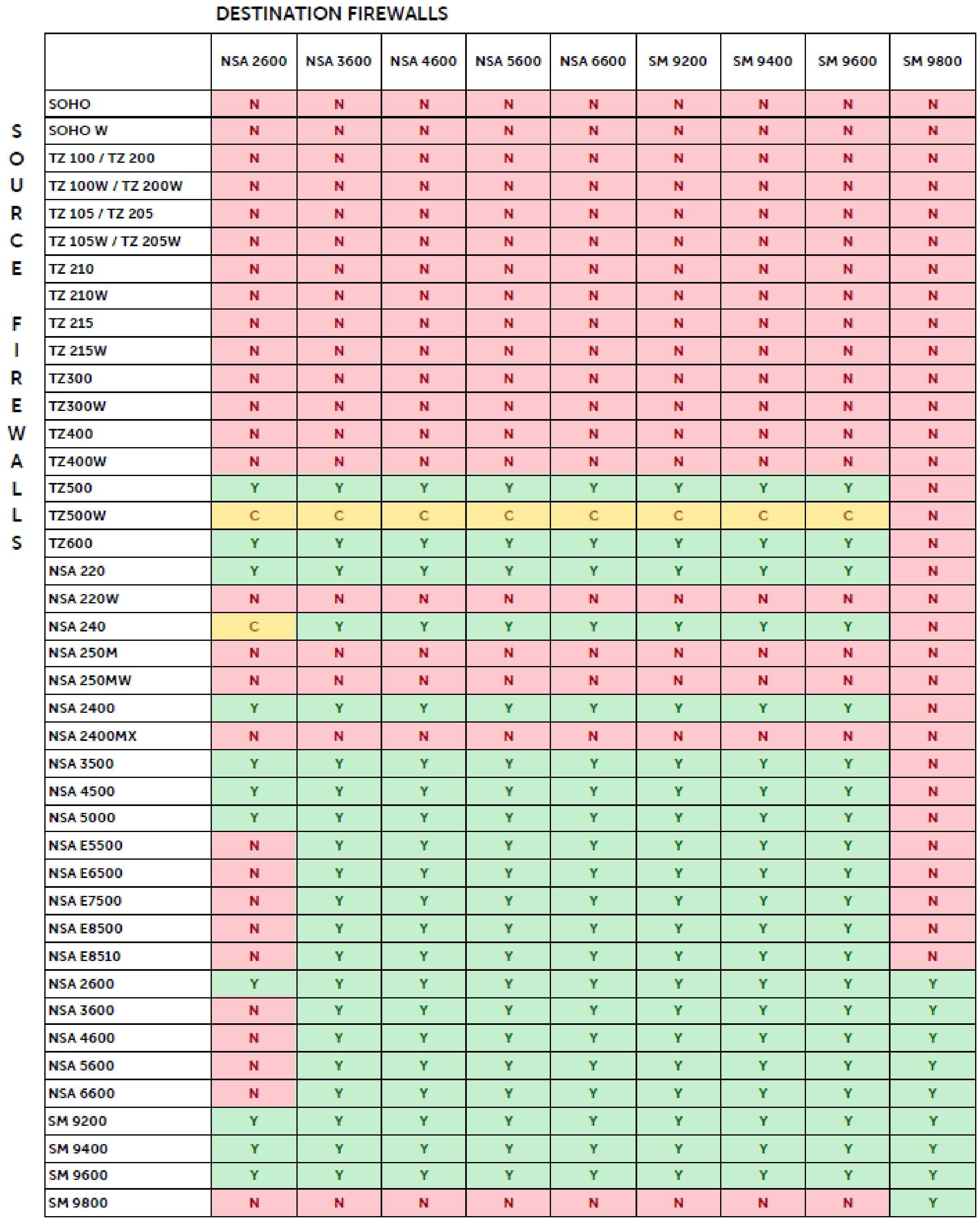
TZ / SOHO W Configuration Import Support

DESTINATION FIREWALLS

SOURCE FIREWALLS

	SOHO W	TZ300	TZ300W	TZ400	TZ400W	TZ500	TZ500W	TZ600
SOHO	C	Y	C	Y	C	Y	C	Y
SOHO W	Y	C	Y	C	Y	C	Y	C
TZ 100 / TZ 200	Y	Y	Y	Y	Y	Y	Y	Y
TZ 100W / TZ 200W	Y	C	Y	C	Y	C	Y	C
TZ 105 / TZ 205	Y	Y	Y	Y	Y	Y	Y	Y
TZ 105W / TZ 205W	Y	C	Y	C	Y	C	Y	C
TZ 210	C	C	C	Y	Y	Y	Y	Y
TZ 210W	C	C	C	C	Y	C	Y	C
TZ 215	C	C	C	Y	Y	Y	Y	Y
TZ 215W	C	C	C	C	Y	C	Y	C
TZ300	Y	Y	Y	Y	Y	Y	Y	Y
TZ300W	Y	C	Y	C	Y	C	Y	C
TZ400	C	C	C	Y	Y	Y	Y	Y
TZ400W	C	C	C	C	Y	C	Y	C
TZ500	C	C	C	C	C	Y	Y	Y
TZ500W	C	C	C	C	C	C	Y	C
TZ600	C	C	C	C	C	C	C	Y
NSA 220	C	C	C	Y	Y	Y	Y	Y
NSA 220W	C	C	C	C	Y	C	Y	C
NSA 240	C	C	C	C	C	C	C	Y
NSA 250M	N	N	N	N	N	Y	Y	Y
NSA 250MW	N	N	N	N	N	C	Y	C
NSA 2400	N	N	N	N	N	N	N	Y
NSA 2400MX	N	N	N	N	N	N	N	C
NSA 3500	N	N	N	N	N	N	N	N
NSA 4500	N	N	N	N	N	N	N	N
NSA 5000	N	N	N	N	N	N	N	N
NSA E5500	N	N	N	N	N	N	N	N
NSA E6500	N	N	N	N	N	N	N	N
NSA E7500	N	N	N	N	N	N	N	N
NSA E8500	N	N	N	N	N	N	N	N
NSA E8510	N	N	N	N	N	N	N	N
NSA 2600	N	N	N	N	N	N	N	N
NSA 3600	N	N	N	N	N	N	N	N
NSA 4600	N	N	N	N	N	N	N	N
NSA 5600	N	N	N	N	N	N	N	N
NSA 6600	N	N	N	N	N	N	N	N
SM 9200	N	N	N	N	N	N	N	N
SM 9400	N	N	N	N	N	N	N	N
SM 9600	N	N	N	N	N	N	N	N
SM 9800	N	N	N	N	N	N	N	N

NSA / SuperMassive Configuration Import Support



DESTINATION FIREWALLS

SOURCE FIREWALLS

	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600	SM 9200	SM 9400	SM 9600	SM 9800
SOHO	N	N	N	N	N	N	N	N	N
SOHO W	N	N	N	N	N	N	N	N	N
TZ 100 / TZ 200	N	N	N	N	N	N	N	N	N
TZ 100W / TZ 200W	N	N	N	N	N	N	N	N	N
TZ 105 / TZ 205	N	N	N	N	N	N	N	N	N
TZ 105W / TZ 205W	N	N	N	N	N	N	N	N	N
TZ 210	N	N	N	N	N	N	N	N	N
TZ 210W	N	N	N	N	N	N	N	N	N
TZ 215	N	N	N	N	N	N	N	N	N
TZ 215W	N	N	N	N	N	N	N	N	N
TZ300	N	N	N	N	N	N	N	N	N
TZ300W	N	N	N	N	N	N	N	N	N
TZ400	N	N	N	N	N	N	N	N	N
TZ400W	N	N	N	N	N	N	N	N	N
TZ500	Y	Y	Y	Y	Y	Y	Y	Y	N
TZ500W	C	C	C	C	C	C	C	C	N
TZ600	Y	Y	Y	Y	Y	Y	Y	Y	N
NSA 220	Y	Y	Y	Y	Y	Y	Y	Y	N
NSA 220W	N	N	N	N	N	N	N	N	N
NSA 240	C	Y	Y	Y	Y	Y	Y	Y	N
NSA 250M	N	N	N	N	N	N	N	N	N
NSA 250MW	N	N	N	N	N	N	N	N	N
NSA 2400	Y	Y	Y	Y	Y	Y	Y	Y	N
NSA 2400MX	N	N	N	N	N	N	N	N	N
NSA 3500	Y	Y	Y	Y	Y	Y	Y	Y	N
NSA 4500	Y	Y	Y	Y	Y	Y	Y	Y	N
NSA 5000	Y	Y	Y	Y	Y	Y	Y	Y	N
NSA E5500	N	Y	Y	Y	Y	Y	Y	Y	N
NSA E6500	N	Y	Y	Y	Y	Y	Y	Y	N
NSA E7500	N	Y	Y	Y	Y	Y	Y	Y	N
NSA E8500	N	Y	Y	Y	Y	Y	Y	Y	N
NSA E8510	N	Y	Y	Y	Y	Y	Y	Y	N
NSA 2600	Y	Y	Y	Y	Y	Y	Y	Y	Y
NSA 3600	N	Y	Y	Y	Y	Y	Y	Y	Y
NSA 4600	N	Y	Y	Y	Y	Y	Y	Y	Y
NSA 5600	N	Y	Y	Y	Y	Y	Y	Y	Y
NSA 6600	N	Y	Y	Y	Y	Y	Y	Y	Y
SM 9200	Y	Y	Y	Y	Y	Y	Y	Y	Y
SM 9400	Y	Y	Y	Y	Y	Y	Y	Y	Y
SM 9600	Y	Y	Y	Y	Y	Y	Y	Y	Y
SM 9800	N	N	N	N	N	N	N	N	Y

SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- Download software
- View video tutorials
- Collaborate with peers and experts in user forums
- Get licensing assistance
- Access MySonicWall
- Learn about SonicWall professional services
- Register for training and certification

To contact SonicWall Support, visit https://support.sonicwall.com/contact-support.

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.

Last updated: 3/26/2017

232-002655-01 Rev A