



SonicOS 7

Upgrade Guide

for the NSa and TZ Series

SONICWALL[®]

Contents

Upgrading to SonicOS 7	3
Upgrading Firmware	4
Obtaining the Latest SonicOS Firmware	4
Creating a System Backup and Exporting Your Settings	5
Scheduling Automatic Backups	6
Upgrading Firmware with Current Settings	6
Upgrading Firmware with Factory Default Settings	7
Using SafeMode to Upgrade Firmware	7
Importing Configuration Settings	11
Configuration Settings Import Support by Version	12
Configuration Settings Import Support by Platform	12
SonicWall Support	14
About This Document	15

Upgrading to SonicOS 7

Welcome to the *SonicOS 7 Upgrade Guide*.

This upgrade guide provides information about upgrading your SonicWall network security appliance from previous versions of SonicOS 6.5 or SonicOS 7 to the latest version of SonicOS 7. See [Upgrading Firmware](#) for information about upgrading the firmware on your firewall.

This guide also provides information about importing the configuration settings from an appliance running an earlier version of SonicOS or SonicOS 7 to an appliance running SonicOS 7. See [Importing Configuration Settings](#) for details about the platforms and firmware versions supported for configuration import.

Topics:

- [Upgrading Firmware](#)
- [Importing Configuration Settings](#)

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](#)
- [Scheduling Automatic Backups](#)
- [Upgrading Firmware with Current Settings](#)
- [Upgrading Firmware with Factory Default Settings](#)
- [Using SafeMode to Upgrade Firmware](#)

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 <https://www.mysonicwall.com>.
2. In MySonicWall, navigate to **Product Management > My Products** in the left navigation pane to display the list of your registered appliances.
3. Mouse over the row that displays your appliance model. Options appear at the right side of the row.
4. Click the **Firmware** icon.



5. Click the **Browse All Firmware** button to display all available firmware versions.
6. Mouse over the row for the firmware you want. Options appear at the right.

7. Click the **Download** icon to download the firmware to your computer, and click the **PDF** icon to display the *Release Notes*.



Creating a System Backup and Exporting Your Settings

Before beginning the upgrading process, make a system backup on your SonicWall appliance. When you create a backup, the SonicWall security appliance takes a “snapshot” of your current system state and configuration preferences, and makes the snapshot the new backup file. You can save backups locally on the appliance or on the cloud. You can also schedule backups to occur automatically.

- On SonicWall NSa 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 firewalls, you can create a backup of your current configuration settings to be used with the current firmware version or with a newly uploaded firmware version. The current firmware image itself is not included in the backup.

You can save multiple local backup files and multiple cloud backups for multiple firmware versions. If more than one backup is saved per firmware version, click the arrow next to the version to expand the list and view the saved configuration backups. From there, you can boot the current or new firmware image with any of the backed up configurations.

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 and export configuration settings to a file on your local management station:

1. In SonicOS 7.0, in the **DEVICE** view, navigate to **Settings > Firmware and Settings**.
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** – On an NSa Series firewall, SonicOS takes a “snapshot” of your current system state, firmware, and configuration preferences, and saves it as the latest local backup file.
On a TZ Series firewall, SonicOS saves a small file on the appliance with all your configuration settings.
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** and select **Export Configuration**. In the popup dialog, which displays the name of the saved file, click **Export** to complete the process.

Scheduling Automatic Backups

You can schedule automatic backups of your configuration settings. SonicWall recommends this after you have upgraded your firewall to the latest firmware.

- ① | **NOTE:** Cloud Backup must be enabled before you can schedule backups of your configuration settings. This feature is not supported for Local Backup.

To schedule a backup:

1. Navigate to **Device | Settings > Firmware and Settings**.
2. Click **Create Backup > Schedule Backup**.
3. In the Schedule Backup dialog, select the options you want to use:
 - For a one-time backup, select **Once** as the **Schedule Type**, then use the calendar to set the date and time.
 - For a recurring backup, select **Recurring** as the **Schedule Type**, then set the days and times.
 - For a mixed schedule backup, select **Mixed** as the **Schedule Type**, then set the days and times.
4. When finished, click **Save**.

For detailed instructions, refer to the *SonicOS 7 Device Settings* administration guide, available on the SonicWall technical documentation portal at <https://www.sonicwall.com/support/technical-documentation/?language=English&category=Firewalls>

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 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. In the **DEVICE** view, on the **Settings > Firmware and Settings** page, 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 under **LOCAL**.
6. On the **Firmware and Settings** page, 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 appliance restarts and displays the login page.
8. Enter your user name and password. Your new SonicOS image version information is displayed on the **Settings > Status** page.

Upgrading Firmware with Factory Default Settings

To upload new firmware to your SonicWall appliance and restart it 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 [Upgrading Firmware with Factory Default Settings](#) the appliance 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. 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 firmware image file, select the file, and click **Upload**. After the firmware finishes uploading, it is displayed in the table under **LOCAL**.
7. On the **Firmware and Settings** page, 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 appliance restarts. When you access the firewall again, it 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 platforms, you can also log in by connecting to the MGMT port and pointing your browser to <http://192.168.1.254>.
9. 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

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

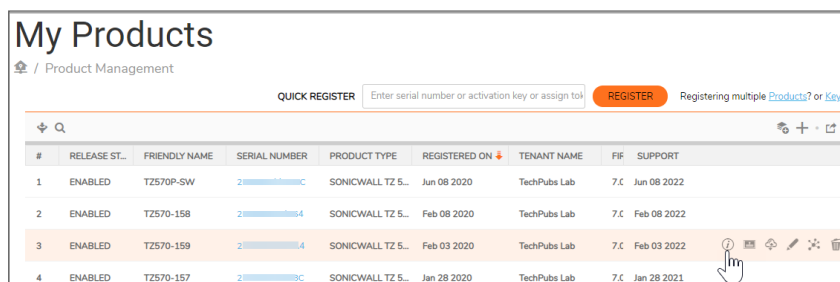
- In SonicOS 7.0.0, you must obtain the Maintenance Key from MySonicWall.
- In SonicOS 7.0.1, you can use the Auth Code as the key if your firewall is unregistered. The Auth Code is available on the label on the appliance bottom, or in the SonicOS web management interface. After the appliance is registered, you will need to use the Maintenance Key, which is available from MySonicWall.

The SafeMode procedure uses a recessed reset button in a small pinhole, called the SafeMode button:

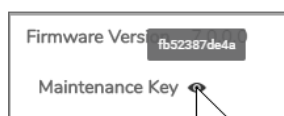
- On NSa platforms, the Safemode button is near the X0 port and above the power button on the front of the appliance.
- On TZ platforms, the button is next to the power connection on the back of the appliance.

To obtain the Maintenance Key for your appliance:

1. Log into your MySonicWall account at <https://www.mysonicwall.com>.
2. Navigate to **Product Management > My Products** and locate your firewall in the table.
3. Move your mouse pointer to the end of the row to expose the buttons and then click on the Information button.



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.



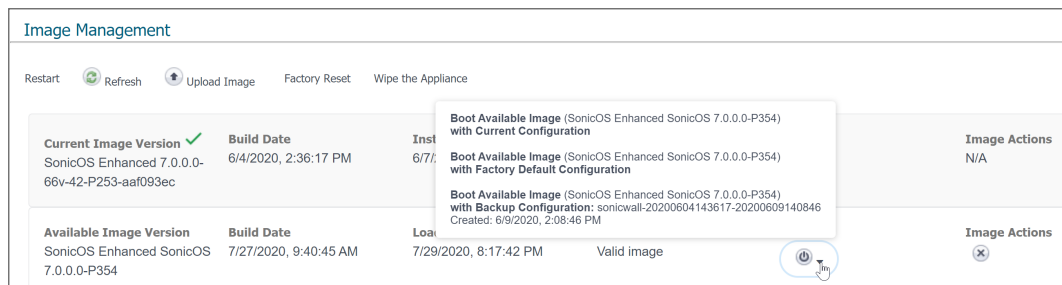
To use SafeMode to upgrade firmware on a SonicWall security appliance:

1. Do one of the following to connect your computer directly to the appliance:
 - On a SonicWall NSa, 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.
 - On a SonicWall TZ, 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.
 2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press the SafeMode button. On a TZ, press and hold the SafeMode button for approximately 60 seconds. On an NSa Series appliance, press the button, but you do not need to hold it down.
- The Test (wrench) LED starts blinking when the appliance has rebooted into SafeMode.

3. Do one of the following to access the SafeMode management interface:
 - On a SonicWall NSa, point your browser to **http://192.168.1.254**.
 - On a SonicWall TZ, point your browser to **https://192.168.168.168**.
4. In the **Maintenance Key** prompt, type in or paste the key you got from MySonicWall and then click **Authenticate**. If your appliance is running SonicOS 7.0.1 and is not yet registered, use its Auth Code as the key.

The SafeMode interface displays.

5. Click **Upload Image**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.
6. 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 appliance with your current configuration settings.
 - **Boot Available Image with Factory Default Configuration**
Use this option to restart the appliance 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 appliance with saved backup configuration settings. You can choose which backup to use.



7. In the confirmation dialog, click **Boot** to proceed.
8. Wait while the firmware is installed, then booted.
9. After successfully booting the firmware, 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. Enter the default user name and password (admin / password) to access the SonicOS management interface.
 On a SonicWall NSa, 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, another LAN interface, or from a WAN interface, if configured.
10. 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 your computer to automatically obtain an IP address and DNS server address, or reset it to its normal static values.
 - c. Connect your computer to your network or to the desired interface on the appliance.
 If the appliance is managed from any interface other than the default LAN (X0) and the computer used to manage the appliance is set to automatically obtain an IP address and DNS server, a static or dynamic DHCP lease scope must be configured in SonicOS for that interface.
 - d. Point your browser to the appropriate WAN or LAN IP address of the appliance.

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.

To export the configuration settings from an appliance running SonicOS 7.0, 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.

The following sections provide details about the firmware versions and platforms that support importing configuration settings to appliances running SonicOS 7.0:

- [Configuration Settings Import Support by Version](#)
- [Configuration Settings Import Support by Platform](#)

For information about importing configuration settings exported from firewalls running SonicOS 5.8, 5.9, 6.1, 6.2, or 6.5 into firewalls running SonicOS 6.5, refer to the *SonicOS 6.5 Upgrade Guide*.

Configuration Settings Import Support by Version

- ① **NOTE:** SonicOS 6.5.1.3 is the minimum version generally supported for settings import to a firewall running SonicOS 7.
- ① **NOTE:** Existing settings for Global Bandwidth Management, Virtual Assist and Content Filter Client Enforcement cannot be imported into SonicOS 7. Global Bandwidth Management is replaced by Advanced Bandwidth Management, and the other features are deprecated in SonicOS 7. For more information about configuring Advanced Bandwidth Management, refer to the knowledgebase article *How Can I Configure Advanced Bandwidth Management On Gen 7?* at <https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-advanced-bandwidth-management-on-gen-7/200818093436630/>.

The following matrix illustrates the supported source and destination versions of SonicOS when importing configuration settings from one appliance to another. SonicOS 6.5 and 7.0 are included.

SonicOS Configuration Import Support

From	To	
	6.5	7.0
	6.5	Y (Min 6.5.1.3)
7.0	N	Y

If answer is "Y" above, see the table in the next section for your specific products
If answer is "N" above, this configuration import is not supported

- ① **NOTE:** Configuration settings import to a firewall running SonicOS 7 from any SonicOS 6.x version prior to SonicOS 6.5.1.3 is supported as a two-step process:
1. Upgrade the firewall from SonicOS 6.x to SonicOS 6.5.1.3 or higher.
 2. Export settings from the upgraded firewall and then import them to the firewall running SonicOS 7.

Configuration Settings Import Support by Platform

The matrix in this section shows the SonicWall firewalls running SonicOS 6.5 or 7.0 whose configuration settings can be imported to SonicWall platforms running SonicOS 7.0.

- ① **NOTE:** Settings import is supported from a SOHO running SonicOS 5.9 to SonicWall platforms running SonicOS 7.0. This is a special case, as the SOHO cannot run SonicOS 6.5.

In the matrix, the source firewalls are in the left column, and the destination firewalls are listed across the top.

DESTINATION FIREWALLS												
	TZ270	TZ270W	TZ370	TZ370W	TZ470	TZ470W	TZ570	TZ570P	TZ570W	TZ670	NSa 2700	NSa 3700
S O U R C E	TZ270	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ270W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ370	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ370W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ470	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ470W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ570	C	C	C	C	Y	Y	Y	Y	Y	Y	Y
	TZ570P	C	C	C	C	Y	Y	Y	Y	Y	Y	Y
	TZ570W	C	C	C	C	C	Y	C	C	Y	C	C
	TZ670	C	C	C	C	Y	Y	Y	Y	Y	Y	Y
	NSa 2700	N	N	N	N	N	N	N	N	N	Y	Y
	NSa 3700	N	N	N	N	N	N	N	N	N	C	Y
S O U R C E	SOHO	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	SOHO W	C	Y	C	Y	C	Y	C	C	Y	C	C
	SOHO 250	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	SOHO 250W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ300	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ300P	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ300W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ350	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ350W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ400	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ400W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ500	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
	TZ500W	C	Y	C	Y	C	Y	C	C	Y	C	C
	TZ600	C	C	C	C	C	C	C	C	C	Y	Y
	TZ600P	C	C	C	C	C	C	C	Y	C	Y	Y
	NSA 2600	N	N	N	N	N	N	N	N	N	Y	Y
	NSa 2650	N	N	N	N	N	N	N	N	N	Y	Y
	NSA 3600	N	N	N	N	N	N	N	N	N	C	C
	NSa 3650	N	N	N	N	N	N	N	N	N	C	C
	NSA 4600	N	N	N	N	N	N	N	N	N	C	C
	NSa 4650	N	N	N	N	N	N	N	N	N	N	N
	NSA 5600	N	N	N	N	N	N	N	N	N	N	N
	NSa 5650	N	N	N	N	N	N	N	N	N	N	N
	NSA 6600	N	N	N	N	N	N	N	N	N	N	N
	NSa 6650	N	N	N	N	N	N	N	N	N	N	N
	SM 9200	N	N	N	N	N	N	N	N	N	N	N
	NSa 9250	N	N	N	N	N	N	N	N	N	N	N
	SM 9400	N	N	N	N	N	N	N	N	N	N	N
	NSa 9450	N	N	N	N	N	N	N	N	N	N	N
	SM 9600	N	N	N	N	N	N	N	N	N	N	N
	NSa 9650	N	N	N	N	N	N	N	N	N	N	N
	SM 9800	N	N	N	N	N	N	N	N	N	N	N

The legend for the above table is:

Y	Supported through SonicOS and/or Migration Tool
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. Built-in wireless configuration will be removed.

You can access the SonicWall Migration Tool at <https://migratetool.global.sonicwall.com/>.

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
- 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

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

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

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

SonicOS Upgrade Guide for the NSa and TZ Series

Updated - April 2021

Software Version - 7

232-005380-00 Rev D

Copyright © 2021 SonicWall Inc. All rights reserved.

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

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

End User Product Agreement

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

Open Source Code

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

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