



SonicOS 7

# Getting Started Guide

for the TZ Series

SONICWALL®

## REGULATORY MODEL NUMBERS

Regulatory Model Numbers	Product Names
APL62-0F7	TZ570 / TZ670
APL62-0F8	TZ570W
APL62-0F9	TZ570P

# Contents

<b>Package Contents</b> .....	4
<b>Front Panel</b> .....	6
<b>Back Panel</b> .....	8
<b>Mounting Options</b> .....	10
Flat Surface Option .....	10
Rack Mounting Option .....	10
Wall Mounting the TZ Appliance .....	11
<b>Determining the WAN Type</b> .....	12
<b>System Requirements</b> .....	13
<b>Connectivity and Power</b> .....	14
Connect Interfaces .....	14
Connect Power .....	15
<b>Setup Options</b> .....	16
Setup using Local Management .....	16
Setup using Cloud Management .....	17
Setup Using the SonicExpress App .....	18
Deploy Using Zero-Touch .....	19
Deploy Using SD-Branch .....	19
<b>Running the Setup Wizard</b> .....	21
<b>Testing and Troubleshooting Connectivity</b> .....	23
<b>Registering a TZ Appliance</b> .....	25
<b>Configuring TZ Wireless LAN Settings</b> .....	26
<b>Uploading the Latest Firmware</b> .....	27
<b>Enabling PoE on the Appliance</b> .....	28
<b>SonicWall Support</b> .....	30
About This Document .....	31

# Package Contents



- 1 TZ Series appliance
- 2 Antennas (2) (TZ570W only)
- 3 Ethernet cable
- 4 Serial console cable (RJ45 to DB9)
- 5 **TZ670/TZ570/TZ570W:** 12VDC/60W Power adapter (1) **TZ570P:** 54VDC/180W Power adapter (1)



---

6 Power cord

---

7 SonicWall TZ670/TZ570/TZ570W/TZ570P Quick Start Guide

---

8 Safety, Environmental, and Regulatory Information documents

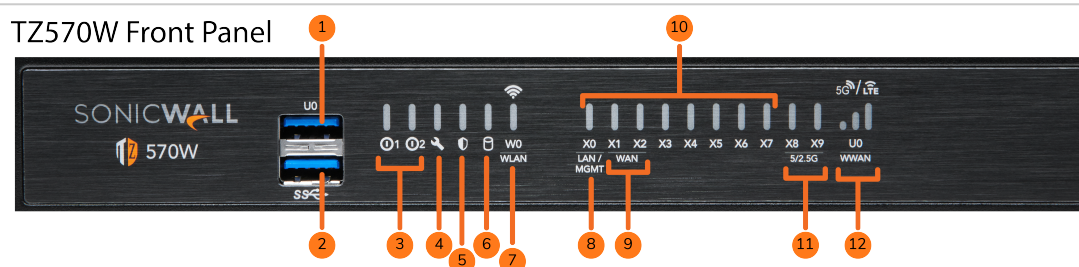
① **NOTE:** The included power cord is approved for use only in specific countries or regions. Before using a power cord, verify that it is rated and approved for use in your location. The power cord is for AC mains installation only. Refer to the *TZ670 / TZ570 / TZ570W Safety, Regulatory, and Legal Information* or *TZ570P Safety, Regulatory, and Legal Information* document for minimum power cord rating and additional safety information.







メモ: 添付の電源コードに関して電気安全を確保するために、弊社製品にご使用いただく電源コードは必ず製品同梱の電源コードをご使用ください。この電源コードは他の製品では使用できません。


**Items missing?** Contact SonicWall Technical Support at:

<https://www.sonicwall.com/support/contact-support>

## Front Panel

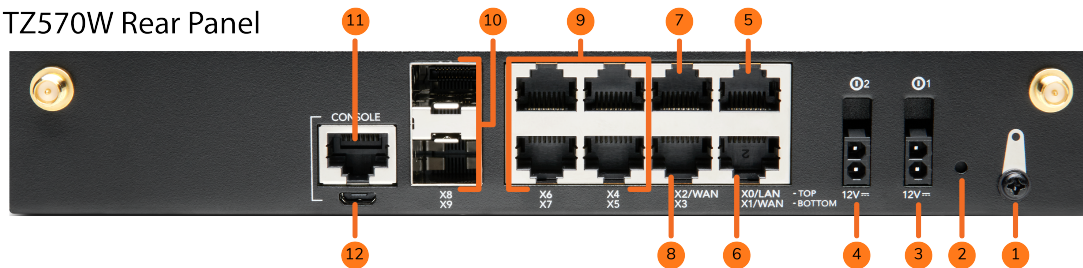


1	U0	U0 Port: USB 3.0 SuperSpeed (SS) Port for WWAN
2		USB SS 3.0 Port: For Configuration, Recovery, Re-imaging the TZ
3		Power LEDs: 1 = Primary, 2 = Redundant Blue = Powered on, Yellow = Defective adapter
4		Test LED: Yellow = Initializing, Blinking Yellow = SafeMode
5		Security LED: Green = All Security Services Licensed, Blinking Yellow = Security Services License Expired Security Services monitored by this LED: Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware
6		Storage LED: Solid Green = Extended Storage module present, Blinking Green = Activity, Yellow = Storage warning
7		Wireless W0 WLAN LED (TZ570W only): Solid Green = Wireless radio is active, Blinking Green = Activity

8	X0	LAN/MGMT X0 Port LED: Solid Green = 1G link, Blinking Green = 1G activity
9	X1/X2	WAN X1 and X2 Port LEDs: Solid Green = 1G link, Blinking Green = 1G activity
10	X0-X7	
11	X8-X9	
12		U0 WWAN LEDs for USB 5G/LTE: Green = 5G/LTE signal strength

## Back Panel

TZ570W Rear Panel



1

**Grounding Screw**

2

**SafeMode Button:** Press and hold until Test LED starts blinking to set the TZ into SafeMode

3

**Primary Power Input for:**

- **TZ670/TZ570/TZ570W:** 60W 100~240VAC - 12VDC power adapter
- **TZ570P:** 180W 100~240VAC - 54VDC power adapter

4

**Redundant Power Input for:**

- **TZ670/TZ570/TZ570W:** 60W 100~240VAC - 12VDC power adapter
- **TZ570P:** 180W 100~240VAC - 54VDC power adapter

A redundant power adapter can be ordered separately – (TZ670/TZ570/TZ570W: SKU 02-SSC-3078) (TZ570P: SKU 02-SSC-0614).

5

**X0 LAN RJ45 Port:** 1 Gbps

6

**X1 WAN RJ45 Port:** 1 Gbps

7

**X2 WAN RJ45 Port:** 1 Gbps

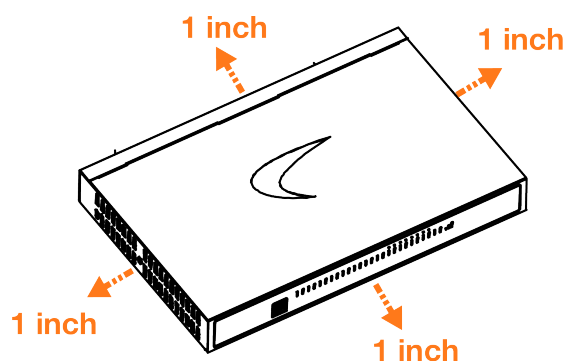
8	<b>X3 RJ45 Port:</b> 1 Gbps <b>TZ570P:</b> X3 is a PoE port
9	<b>X4/X5/X6/X7 RJ45 Ports:</b> 1 Gbps <b>TZ570P:</b> <b>X4/X5/X6/X7</b> are PoE ports
10	<b>SFP/SFP+ Ports X8/X9:</b> TZ670: 10 / 5 / 2.5 / 1 Gbps TZ570/TZ570W/TZ570P: 5 / 2.5 / 1 Gbps
11	<b>RJ45 Console Port</b>
12	<b>Micro-USB Console Port</b> A Micro-USB cable is not provided with the product, but can be ordered separately (SKU 02-SSC-5173).

**SSD Storage Module** – The TZ comes with a field-upgradable SSD Storage Module, accessible via a removable panel on the bottom of the appliance. To order, refer to the price list for available SKUs.

## Mounting Options

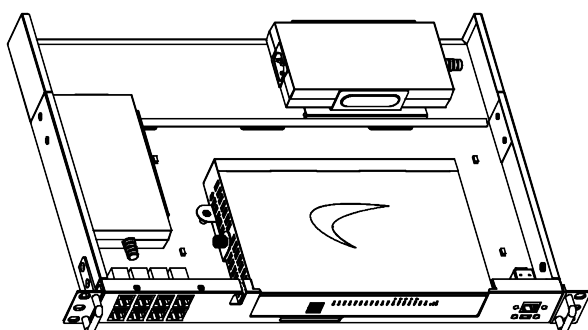
### Flat Surface Option

Place the TZ on a flat surface. Allow unrestricted airflow around the unit, leaving a minimum of 1 inch (25.44mm) clearance on all sides.



### Rack Mounting Option

SonicWall offers a rack mount tray kit for mounting your TZ and power adapter(s) in a standard 19-inch rack.



① | **NOTE:** For additional information, see the [TZ Rack Mount Tray Installation Guide](#).

Ordering information:

SKU 02-SSC-3112 SONICWALL TZ670 / TZ570 RACKMOUNT KIT

# Wall Mounting the TZ Appliance

**⚠ WARNING:** Do not mount the appliance on the ceiling, it is not designed for secure ceiling mounting.

For optional wall mounting, you need:

- Screwdriver
- Drill with appropriate size bit
- For mounting on drywall:
  - Two #6 pan-head screws, 1 inch long (7mm diameter head, 25mm long)
  - Two wall anchors
- For mounting on solid wood or metal:
  - Two #6 pan-head wood or machine screws, 1 inch long (7mm diameter head, 25mm long)

## ***To mount the appliance on the wall:***

1. Drill two holes 4.5 inches (11.5 cm) apart in the wall where you want to mount the appliance.
2. If using wall anchors, insert a wall anchor into each hole.
3. Insert a screw into each wall anchor (into each hole if not using wall anchors), leaving 3/16 inches (0.45 cm) of the screws exposed (including screw head).
4. Position the appliance mounting slots over the screws and press in and down until the appliance is securely mounted.

## Determining the WAN Type

Before configuring your SonicWall appliance, you need to determine the type of WAN connection that your setup uses. SonicWall supports the following types:

- **Static**—Configures the appliance for a network that uses static IP addresses.
- **DHCP**—Configures the appliance to request IP settings from a DHCP server on the Internet.
- **PPPoE**—Point-to-Point Protocol over Ethernet (PPPoE) is typically used with a DSL modem. If your ISP requires desktop software with a username and password, select NAT with PPPoE mode.
- **PPTP**—Point-to-Point Tunneling Protocol (PPTP) is used to connect to a remote server. PPTP typically supports older Microsoft Windows implementations that require tunneling connectivity.
- **L2TP**—Layer 2 Tunneling Protocol (L2TP) is used to transmit Layer 2 data over IP or other Layer 3 routed networks. Internet Service Providers (ISPs) often use it to enable virtual private networks (VPNs) for customers over the Internet. It does not encrypt network traffic itself. ***If L2TP is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.***
- **Wire Mode (2-Port Wire)**—Inserts the appliance into the network using two paired interfaces. Available Wire Mode types include Bypass, Inspect, and Secure. Bypass mode allows for quick and non-disruptive insertion into the data path. Inspect mode extends Bypass mode with traffic inspection for classification and flow reporting. Secure mode provides full SonicWall ReAssembly-Free Deep Packet Inspection™ (RF-DPI) and control of network traffic.  
  
Secure Mode also affords the same level of visibility and enforcement as conventional NAT or L2 Bridged Mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. If Wire Mode is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.

① **NOTE:** When operating in Wire Mode, the firewall's MGMT interface is used for local management. To enable remote management and dynamic security services and application intelligence updates, a WAN interface (separate from the Wire Mode interfaces) must be configured for Internet connectivity.

- **Tap Mode (1-Port Tap)**—Using a single interface, the firewall connects to and receives mirrored packets from an adjacent switch SPAN port. Similar to Inspect mode in Wire Mode, but with a single port and not in the physical path of traffic. ***If Tap Mode is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.***

For more information about WAN types including Wire Mode, Tap Mode, L2TP, and others, refer to the *SonicOS Administration* documentation or online Help.



# System Requirements

Before beginning the setup process, verify that you have:

- An Internet connection
- A web browser supporting Java Script and HTTP uploads

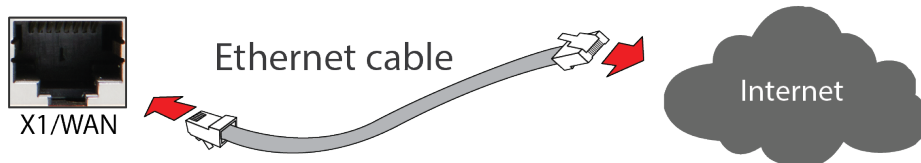
The following browsers are supported for SonicOS management:

- Chrome, version 45 and higher
- Firefox, version 38 and higher
- Internet Explorer, version 10 and higher
- Edge, all versions
- Opera, version 32 and higher
- Safari (running on non-Windows machines), version 10 and higher

# Connectivity and Power

## Connect Interfaces

- Connect the TZ WAN interface (X1 or X2) to the Internet connection using a standard Ethernet cable.
- Connect the LAN interface (X0) to your computer using a standard Ethernet cable.



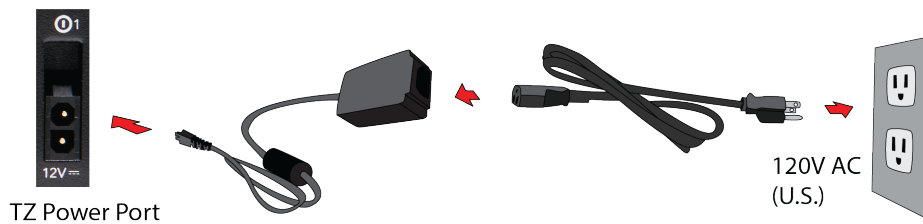
- Connect the antennas to the appliance.





① | **NOTE:** The center antenna is labeled and is only compatible with the center antenna connector.

## Connect Power



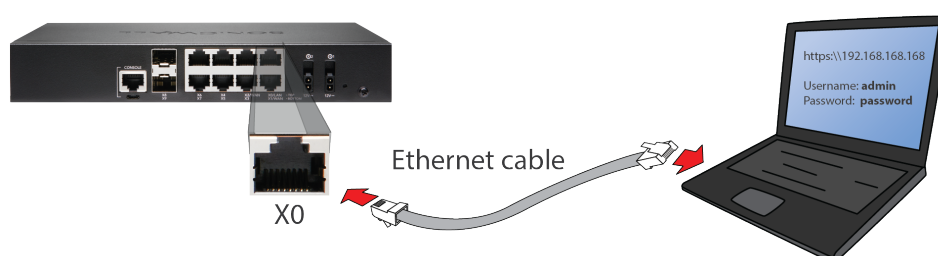
- Connect the power adapter to the appliance and to the power cable. Plug the power cable into an appropriate outlet (100-240 volts AC).
- The TZ appliance powers on, and the Test LED lights up during the boot sequence and then turns off when the boot sequence is complete.

⚠ | **CAUTION:** Use only the power adapter included with this appliance. Do not use a power adapter that is damaged or from another appliance.

# Setup Options

## Setup using Local Management

Setup and manage your TZ by connecting it to a management computer with an Ethernet cable.

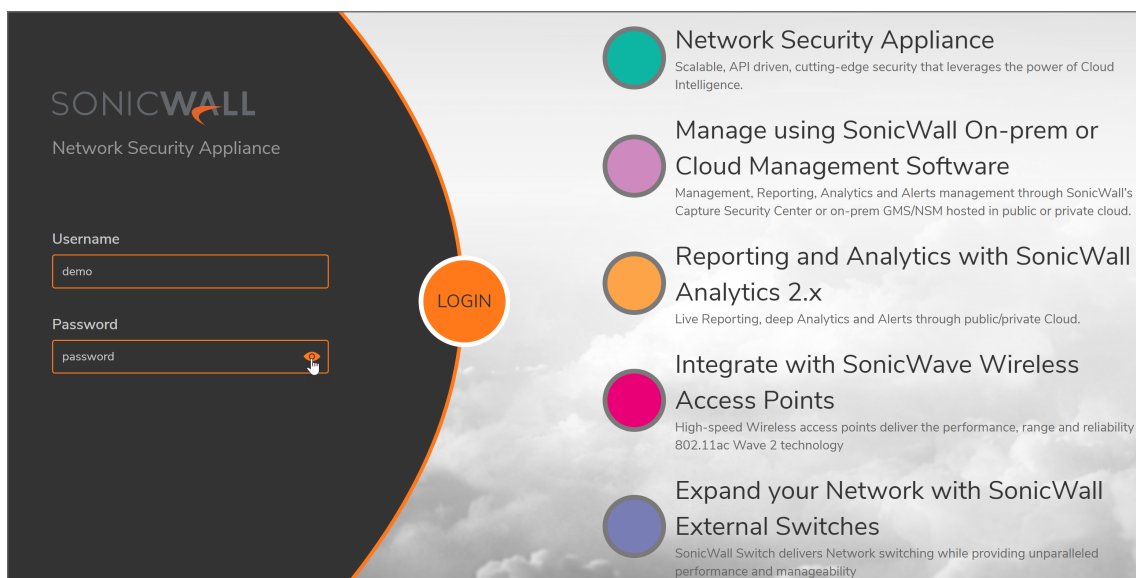


To minimize scrolling, set your screen resolution to at least 1920 x 1080 pixels.

### **To setup Local Management:**

1. Connect the TZ LAN interface (X0) to your computer.
2. Navigate to <https://192.168.168.168> in your web browser and log in with the default credentials:
3. Username: **admin**  
Password: **password**
4. Statically assign an IP address to the computer.
5. Launch the **Setup Guide** wizard or manually configure to complete initial configuration.
6. In SonicOS, click **Register** and log in with your MySonicWall credentials to register your TZ.

Your TZ is now initialized and ready for use!



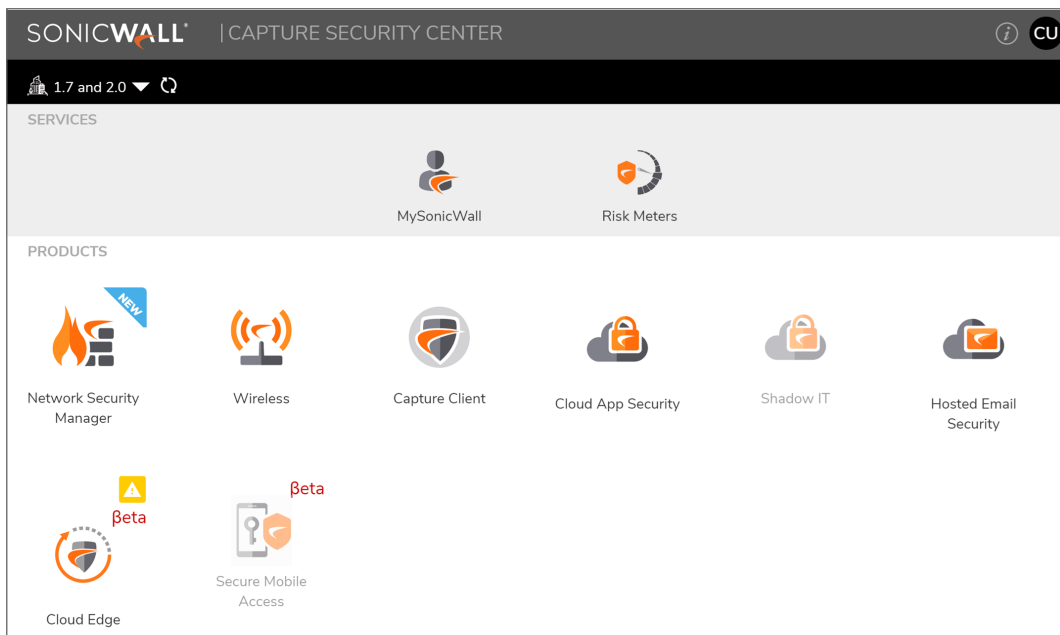
## Setup using Cloud Management

For Cloud Management, use SonicWall Capture Security Center (CSC) with Zero Touch to manage and configure your TZ.

① | **NOTE:** This option requires a Cloud Management license.

### *To manage and configure your TZ:*

1. Log into CSC at [cloud.sonicwall.com](https://cloud.sonicwall.com) using your MySonicWall credentials.
2. Select the MySonicWall tile to register your TZ.
3. Enable **Zero Touch** and **NSM Essential/NSM Advanced** license on your TZ in MySonicWall.
4. Select a Data Center accordingly (for first time users only).
5. Modify the **Managed By** option from **On Box** to **Cloud**, and then enable **Zero Touch**.
6. Select the **Network Security Manager** tile in the CSC to manage your TZ from the cloud.



#	FRIENDLY NAME	SERIAL NUMBER	TENANT NAME	GROUPS	MODEL	IP ADDRESS	TAGS	VERSION	ZERO TOUCH	LINK	STATE
1	000000000000	000000000000	NSM 2.0		Unknown			Unknown	⊖	⬇️	🔴
2	NSV800-NDAM-01	000000000000	NSM 2.0		Unknown			Unknown	⊖	⬇️	🔴
3	000000000000	000000000000	NSM 2.0		Unknown			Unknown	⊖	⬇️	🔴
4	Ag 1	180000000000	NSM 2.0		Unknown			Unknown	⊖	⬇️	🔴
5	Ag 1	180000000000	NSM 2.0		TZ 400	10.97.130.121:2102*		SonicOS Enhanced 6.5.1.3-12h	⊕	⬆️	🟢
6	TZ350W-NDAM-03	200000000000	NSM 2.0		TZ 350 wireless-AC	103.19.168.166:902		SonicOS Enhanced 6.5.4.5-53h	⊕	⬆️	🟢
7	Ag 2	200000000000	NSM 2.0		Unknown			Unknown	⊖	⬆️	🟢
8	Soho250W-Tarun-Home-01	200000000000	NSM 2.0		SCH0250 wireless-N	10.97.130.121:2102*		SonicOS Enhanced 6.5.4.6-67h	⊕	⬆️	🟢
9	Ag 2	200000000000	NSM 2.0		TZ 570	10.97.130.121:2102*		SonicOS Enhanced 7.0.0.0-60v-42-#144-cs7c8f955	⊕	⬆️	🟢

## Setup Using the SonicExpress App

Use SonicWall SonicExpress on your smart phone to register and configure your TZ.

① **NOTE:** After the initial setup, be sure to download the latest firmware from MySonicWall and upgrade your TZ.

### To setup using the SonicExpress App:

1. Download and launch the SonicExpress App on your iOS or Android device.
2. Tap **Login** and log in with your MySonicWall credentials.
3. Select the Tenant for the TZ. Tenants can contain multiple SonicWall appliances.
4. Connect your iOS/Android device to the TZ with the smart phone USB cable. This cable is not supplied with the TZ.



① | **NOTE:** Use the USB cable from your mobile device.

5. Use the **Setup Guide** to register the TZ, synchronize service licenses, change the password, and configure essential interface settings.

## Deploy Using Zero-Touch

Your SonicWall appliance is Zero-Touch enabled.

Zero-Touch makes it easy to register your unit and add it to Capture Security Center for management and reporting in three simple steps.

For information about using Zero-Touch, see the *Zero-Touch Deployment Guide* on the Support portal.

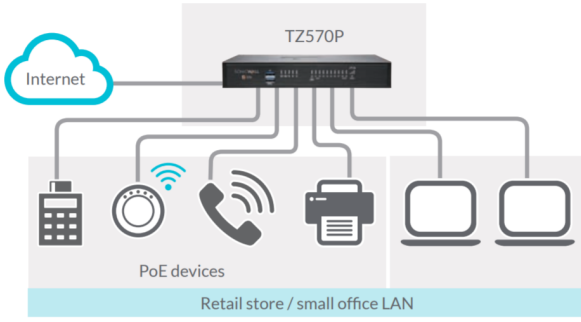
After completing the Zero-Touch deployment process, you can skip to [Mounting the TZ Appliance](#) or [Enabling PoE on the Appliance](#) in this guide.

## Deploy Using SD-Branch

SD-Branch combines SD-WAN, SD-LAN, unified security and centralized management for distributed enterprises. SonicWall Secure SD-Branch integrates next-generation firewalls, network access switches, secure WiFi access points, endpoint security, cloud application security and single-pane-of-glass management.

The latest SonicWall TZ series, are the first desktop form factor next-generation firewalls (NGFW) with 10 or 5 Gigabit Ethernet interfaces. The series consist of a wide range of products to suit a variety of use cases.

Designed for small, mid-sized organizations and distributed enterprise with SD-Branch locations, the 7th generation (Gen 7) TZ series delivers industry-validated security effectiveness with best-in-class price-performance. These NGFWs address the growing trends in web encryption, connected devices and high-speed mobility by delivering a solution that meets the need for automated, real-time breach detection and prevention.



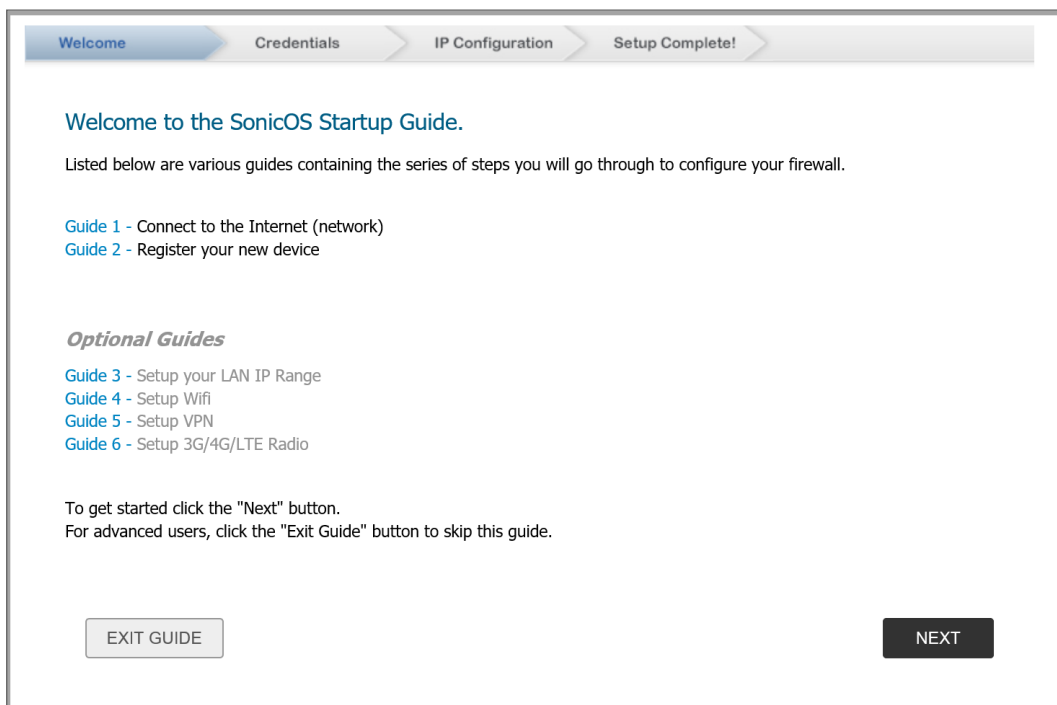


## Running the Setup Wizard

- Navigate to <https://192.168.168.168> in your web browser.
  - ① | **TIP:** Your computer should be using DHCP IP addressing.
- Click the link in “To launch the SonicWall **Setup Guide**, click **here**.”

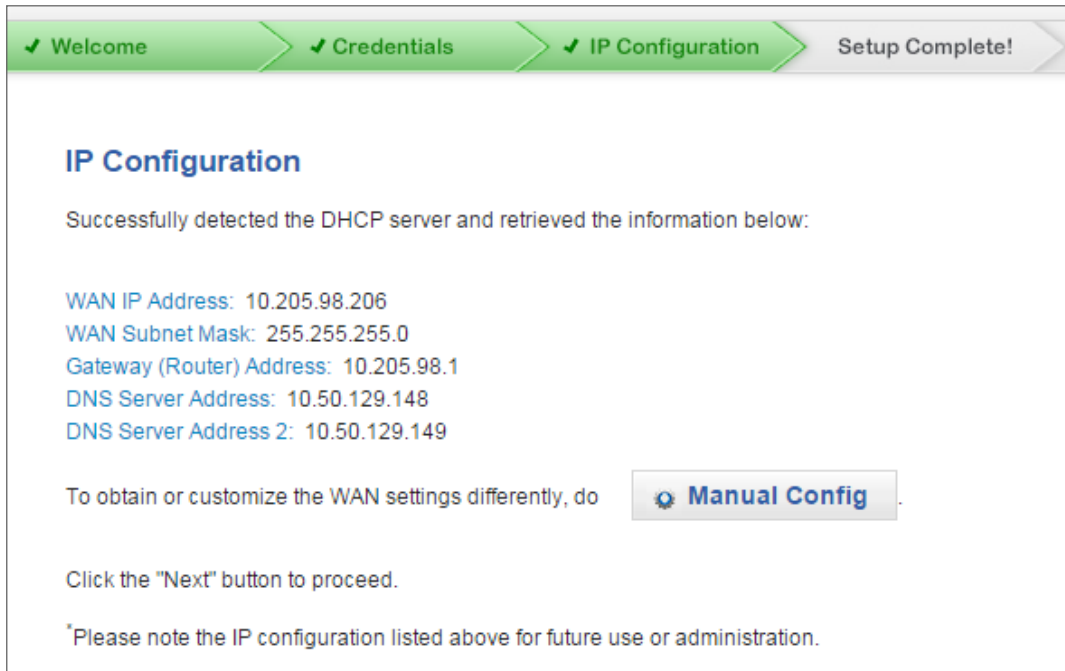


- The **SonicOS Setup Guide** opens.



- Click **NEXT** and follow the prompts in the **Setup Guide**.

- On the **Credentials** screen, enter a new administrator password. Click **NEXT**.  
① | **NOTE:** The default administrator credentials are **Username:** *admin* **Password:** *password*
- The automatically assigned DHCP IP server settings are displayed on the **IP Configuration** screen. Click **NEXT**.



- On the **Setup Complete** screen, review the settings and then click **DONE**. The SonicOS login screen displays.

# Testing and Troubleshooting Connectivity

## **To test your Internet connection:**

1. Reset your computer to use DHCP IP addressing and connect it to your LAN subnet or to the appliance X0 interface.
2. Point your browser to the X0 IP address configured during initial setup (default: 192.168.168.168).
3. Log into SonicOS using the configured credentials (default: admin/password).
4. In a command prompt window, type: `ping sonicwall.com`. You should receive a reply.
5. Open another browser tab or window and point it to <https://www.sonicwall.com> or another valid web site. If the site displays, you have correctly configured your appliance.

## **To troubleshoot your Internet connection:**

- Verify that the Local Area Connection settings on your management computer are set to use either DHCP or a static IP on the LAN subnet. Restart it or renew the DHCP address.
- Verify that the WAN interface being used for Internet connectivity is not configured in Wire Mode or Tap Mode.
- Restart your Internet router or modem to communicate with the DHCP client in SonicOS on the appliance.
- Check all cable connections and IP addresses.

## **To troubleshoot your MGMT connection, consider the following:**

- Did you correctly enter the SonicWall NSA management IP address beginning with “http://” or “https://” in your web browser?
- Did you try restarting your management station while it is connected to the appliance?
- Are the Local Area Connection settings on your computer set to a static IP address on the 192.168.1.0/24 subnet?
- Is the Ethernet cable connected to your computer and to the MGMT port on your appliance, and are the connector clips properly seated in the ports?

## **To troubleshoot your LAN connection, consider the following:**

- Did you correctly enter the IP address for the SonicWall X0 interface into your web browser, beginning with “http://” or “https://”?
- Did you try restarting your management station while it is connected to the appliance?

- Are the Local Area Connection settings on your computer set to one of the following:
  - Obtain an IP address automatically using DHCP
  - A static IP address on the default LAN subnet (192.168.168.0/24)
  - A static IP address on the configured LAN subnet, if you changed it during initial setup
- Is the Ethernet cable connected to your computer and to the X0 (LAN) port on your appliance, and are the connector clips properly seated in the ports?

# Registering a TZ Appliance

Registration is an important part of the setup process and is necessary in order to receive the benefits of SonicWall security services, firmware updates, and technical support.

## *To register the appliance from SonicOS:*

1. Continue from the Setup Guide or point your browser to the appliance LAN IP address (default <https://192.168.168.168>) and log in using the administrator credentials.
2. Click **Register** in the top banner or on the **MONITOR | Current Status | System Status** page under **Security Services**.

Your SonicWall is not registered.  
Click here to [Register](#) your SonicWall.

- ① **TIP:** Registering the appliance from SonicOS requires that DNS Server settings are configured on the WAN (X1) interface.
3. Log in using your MySonicWall account name and password. If you do not have a MySonicWall account, go to <http://www.mysonicwall.com> to create an account.
  4. MySonicWall directly obtains the necessary information from the appliance. When finished, a message that the registration has been completed appears. Click **CONTINUE**.

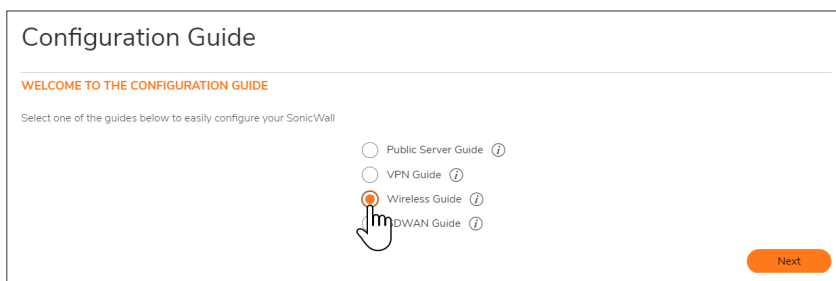
Thank you for registering this product. Registration completed successfully.

CONTINUE

# Configuring TZ Wireless LAN Settings

## To configure the TZ Wireless settings for a LAN:

1. Log in to your TZ Wireless appliance and click the **Wizards** icon at the top of the screen.
2. Select the radio button for the **Wireless Guide** wizard.



3. Click **Next** and follow the prompts in the **Wireless Guide** wizard. For more information and complete procedures, refer to the latest *SonicOS Quick Configuration Guide*.

For international (non USA or Japan) TZ370 Wireless appliances, you are asked to select a country code when using the **Wireless Guide** or when you initially navigate to the **DEVICE | Internal Wireless > Settings** page. Be sure to select the country code for the country in which the appliance is deployed, even if you are not currently in that country.

① **IMPORTANT:** If you select the country code for Canada, it cannot be changed except by contacting SonicWall Support.


# Uploading the Latest Firmware

## To get and upload the latest firmware:

1. In a web browser, navigate to <http://www.mysonicwall.com>.
2. Navigate to **Resources & Support > My Downloads** and select TZ Series from the **Select a Product** drop-down menu.
3. Click the download button for the firmware you want and save the file to a location on your computer.
4. On the TZ appliance, navigate to the **DEVICE | Settings | Firmware and Settings** page and click **Upload Firmware**.
5. Click **OK** to backup current settings.
6. Click **Browse** to select the firmware you just downloaded, then click **Upload**.

### Upload Firmware

Upload Firmware file

 Uploading new firmware will overwrite any existing uploaded firmware image.

You can get the latest firmware at [www.mysonicwall.com](http://www.mysonicwall.com)

Download it to your local disk, and then upload it to your SonicWall using this dialog. Use the "Browse" button to find the firmware file you want to upload. Firmware files have a file extension of .bin.sig for hardware devices, for e.g., tz-\*.bin.sig. After the firmware is uploaded, you will see the newly uploaded firmware image. You may select the firmware image from which to boot.

7. Click the **Boot** icon for your new firmware.

## Enabling PoE on the Appliance

If your TZ is designed for PoE support, the PoE ports must be enabled individually for powered device (PD) detection and classification. By default, the highest port number has the highest priority in powering on a PD. You can control the supplied power level and port priority from SonicOS.

### To enable PoE and configure basic PoE settings:

1. Point your browser to the LAN or WAN IP address and log into the appliance as an administrator (default: *admin / password*).
2. Navigate to the **NETWORK | System | > PoE Settings** page.
3. Select **Enable PoE**. The display changes:

The screenshot shows the SonicOS PoE Settings interface. At the top, there is a toggle for 'Enable PoE' which is turned on, and a 'Max Power Threshold(%)' field set to 100. An 'Accept' button is highlighted with a hand cursor. Below this is the 'POE STATUS' section, which includes a diagram of the appliance's ports (X0-X9) and a bar chart showing 'Total Power Available 90000mW'. The bar chart shows a single bar at 90000mW, representing the total power available. To the right of the bar chart is a legend for power levels: 0 mW (red), 0% Allocated Power (orange), 90000 mW (yellow), 100% Max Power Threshold (green), 0 mW (green), and 0% Power Consumed (green). Below the 'POE STATUS' section is the 'POE MONITOR' section, which contains a table with columns for PORT, POWER MODE, PRIORITY, POWER ALLOCATION, POWER CONSUMPTL., DETECTED DEVICE C., PORT STATUS, and SUPPORT POE. The table lists ports X0 through X9, with X3 through X7 showing '802.3 AT' power mode, 'Low' priority, and '0' power allocation and consumption. The 'DETECTED DEVICE C.' column shows 'Detection Disabled' for all ports, and the 'PORT STATUS' column shows 'Disabled' for all ports. The 'SUPPORT POE' column shows 'Yes' for all ports.

PORT	POWER MODE	PRIORITY	POWER ALLOCATION	POWER CONSUMPTL.	DETECTED DEVICE C.	PORT STATUS	SUPPORT POE
X0							
X1	--		--	--	--		
X2							
X3	802.3 AT	Low	0	0	Detection Disabled	Disabled	Yes
X4	802.3 AT	Low	0	0	Detection Disabled	Disabled	Yes
X5	802.3 AT	Low	0	0	Detection Disabled	Disabled	Yes
X6	802.3 AT	Low	0	0	Detection Disabled	Disabled	Yes
X7	802.3 AT	Low	0	0	Detection Disabled	Disabled	Yes
X8							
X9	--		--	--	--		

4. Accept the default of 100 in the **Max Power Threshold** field or type in a number between **1** and **100**. This is the percentage of the maximum available power that the PoE controller allocates to the PoE ports on the appliance.
5. Click **Accept**.



- The **NETWORK | System | > PoE Settings** page displays an interactive graphical representation of the PoE port status under **PoE Status**, with the **PoE Monitor** table showing the per port **Power Mode (802.3 AT or 802.3 AF)**, **Power Allocation**, and **Power Consumption**.
- To enable PoE power on a specific port, click the port image or checkbox of the port then click either **Configure** above the **PoE Monitor** table, or the **Edit** icon in the **PoE Monitor** table row for that port. The **Poe Port Settings** dialog displays the **Power Enable** option along with other options.

PoE Port Settings

Port(s) X5

Power Enable

Power Mode  802.3 AT  802.3 AF

Power Priority Level  High  Low

Power Consumption 0

Cancel Save

- Select **Power Enable**, then set the desired options and click **Save**.
- Power Mode** – Changes to this option do not take effect unless a PoE device is connected to that port. The TZ detects the mode from the device, but you can change the mode here. For example, if the **Power Mode** is detected as **802.3 AT**, you can change it to **802.3 AF** if you know that the device requires a lower power level.
- Power Priority Level** – By default, this option is set to **Low** for all PoE ports and the highest numbered PoE port has the highest priority for power as distributed by the PoE controller. Set this option to **High** on a lower numbered port to give it a higher priority.
- If the **Power Mode** is detected as **802.3 AT** and then changed to **802.3 AF**, the PoE device shuts down if its power consumption spikes above the **802.3 AF** power budget for that port. Similarly, reducing the **Max Power Threshold** so that not all PoE ports have some power prevents devices connected to the lower priority ports from powering on.
- Repeat Step 7 and Step 8 to enable PoE power on other ports, as needed.
- The **PoE Status** display shows blue for the PoE port when an **802.3 AT** device is connected. A green port is displayed when an **802.3 AF** device is connected.

See the *SonicOS Network administration guide* for more information.

# SonicWall Support

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

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

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <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 Getting Started Guide for the TZ Series

Updated - December 2020

Software Version - 7

232-005546-00 Rev A

Copyright © 2020 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