



SonicOS 7.1

WWAN

Administration Guide

SONICWALL®

Contents

- About SonicOS** 3
- Working with SonicOS 3
- SonicOS Workflow 5
- How to Use the SonicOS Administration Guides 6
- Guide Conventions 8

- About WWAN** 9
- Monitoring WWAN Status 9
 - USB Modem Access11

- SonicWall Support** 13
- About This Document 14

About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on configuring and managing WWAN connections for SonicOS. See the following topics.

Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

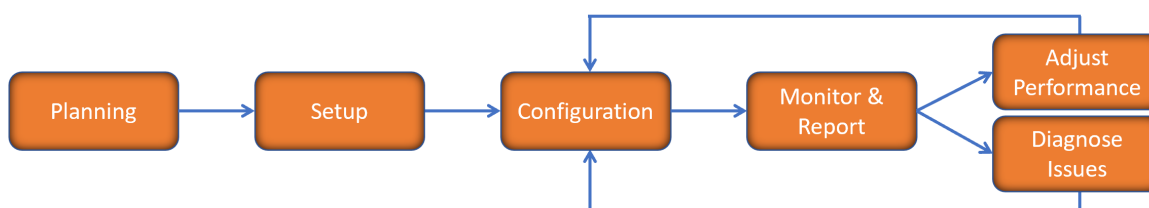
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

In addition to the management interface, SonicOS also has a full-featured API and a command-line interface (CLI) to manage the firewalls. For more information, refer to:

- [SonicOS 7.1 API Reference Guide](#)
- [SonicOS Command Line Interface Reference Guide](#)

SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

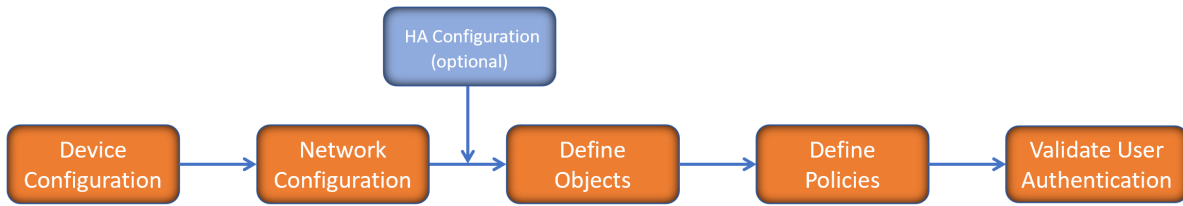


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

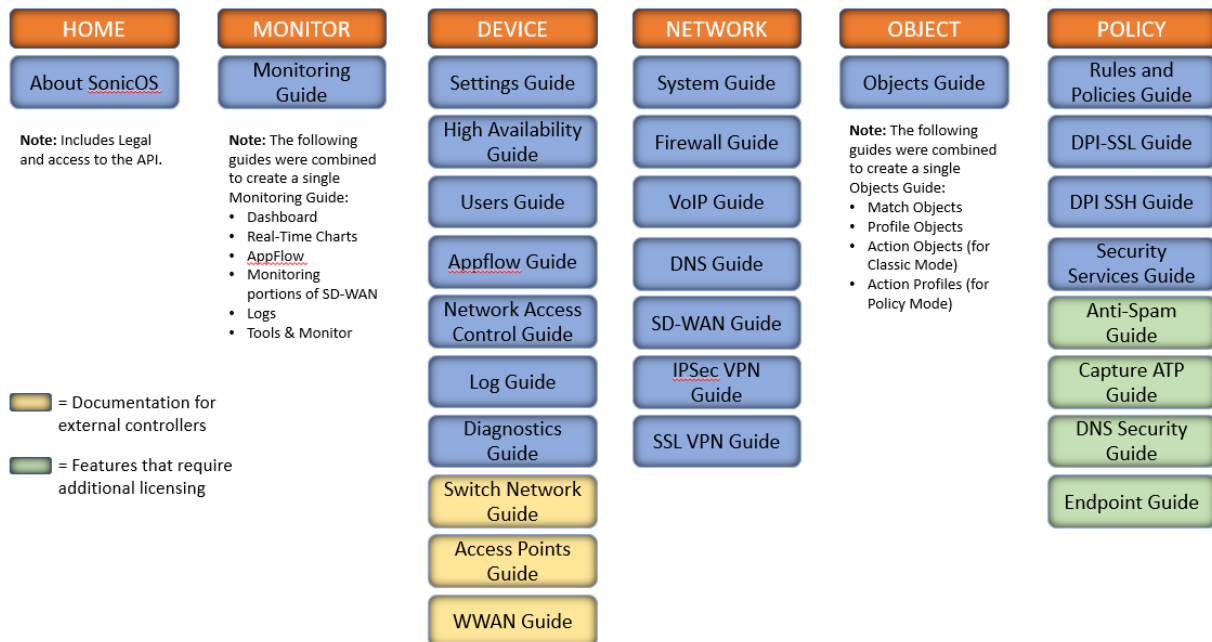


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the [SonicOS 7.1 Monitor Guide](#) and the [SonicOS 7.1 Objects Guide](#) which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

Guide Conventions

These text conventions are used in this guide:

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.

Convention	Description
Bold text	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
Function Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, NETWORK System > Interfaces means to select the NETWORK functions at the top of the window, then click on System in the left navigation menu to open the menu group (if needed) and select Interfaces to display the page.
Code	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment serialnumber=<your serial number> , replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004 .
Italics	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.

About WWAN

All SonicWall appliances support either LTE-only or LTE+5G external devices (LTE/5G) with the exception of the NSsp 15700, in conjunction with the fail-over feature of SonicOS. You can connect an LTE/5G device to a USB port on the firewall to provide Wireless WAN (WWAN) connectivity to the internet over cellular networks. WWAN devices can also be used for Load Balancing (LB) with existing wired WAN connections.

An LTE/5G connection can be used for:

- WAN failover to a connection that is not dependent on wire or cable.
- Temporary networks where a preconfigured connection might not be available, such as at trade-shows and kiosks.
- Mobile networks, where the SonicWall appliance is based in a vehicle.
- Primary WAN connections where wire-based connections are not available and LTE/5G cellular is.

To use the LTE/5G interface, you must have an LTE/5G PC card or USB device and a contract with a wireless service provider. An LTE/5G service provider should be selected based primarily on the availability of supported hardware. SonicOS supports the devices listed online at:

<https://www.sonicwall.com/support/knowledge-base/what-wireless-cards-and-usb-broadband-modems-are-supported-on-firewalls-and-access-points>

By default, the firewall tries to detect the type of device that is connected. If it can successfully identify what kind it is, the left side navigation provides the WAN device and network details in the **DEVICE | WWAN** menu group. Without a connected LTE/5G device, the WWAN page displays the current status.

Topics:

- [Monitoring WWAN Status](#)

Monitoring WWAN Status

If you have an LTE/5G device detected/connected to one of your firewalls, the **DEVICE > WWAN** page offers monitoring information for that device.


WWAN STATUS

WWAN MODEM STATUS

The 4G/LTE is currently the active WAN interface

Vendor	Huawei
Manufacturer	HUAWEL_MOBILE
Product Name	HUAWEL_MOBILE
Vendor ID	12d1
Product ID	14db
RAT Mode	LTE

SIGNAL STRENGTH



Good

■ Excellent
 ■ Good
 ■ Poor
 ■ No Device / Not Detected

WWAN NETWORK STATUS

Gateway (Router) Address	192.168.8.1
IP (NAT Public) Address	192.168.8.101
Subnet Mask	255.255.255.0
DNS Server 1	192.168.8.1
DNS Server 2	0.0.0.0

USB MODEM ACCESS

Use the following link to access the modem's internal web server, where you can monitor the runtime status and make changes to the settings.

[Click to Access Modem](#)

The first panel provides connectivity data and modem status, and the second panel shows a graphical representation of the device's signal strength. The third panel, **WWAN Network Status**, shows you the IPs of the router, subnet mask, and DNS server.

When using an ATT WWAN modem, your panels might appear like this.


WWAN STATUS

WWAN MODEM STATUS

The 4G/LTE is currently the active WAN interface

Vendor	Inseego/Novatel
Manufacturer	Novatel Wireless
Product Name	USB800
Vendor ID	1410
Product ID	b020
RAT Mode	LTE

SIGNAL STRENGTH



Good

■ Excellent
 ■ Good
 ■ Poor
 ■ No Device / Not Detected

WWAN NETWORK STATUS

Gateway (Router) Address	10.55.153.1
IP (NAT Public) Address	10.55.153.49
Subnet Mask	255.255.255.0
DNS Server 1	192.168.1.1
DNS Server 2	0.0.0.0

USB MODEM ACCESS

Use the following link to access the modem's internal web server, where you can monitor the runtime status and make changes to the settings.
(Note: This feature is useful for many WWAN devices, but it's not fully supported on all WWAN devices.)

[Click to Access Modem](#)

If no LTE/5G device is detected/connected on one of your firewalls, you get the following message on the **DEVICE > WWAN** page in the **Signal Strength** section:

No Device / Not Detected.

Without a connected LTE/5G device, the WWAN page displays the current status as follows.

The screenshot displays the WWAN STATUS page with the following content:

- WWAN MODEM STATUS:** The 4G/LTE is currently inactive. Fields include Vendor, Manufacturer, Product Name, Vendor ID, Product ID, and RAT Mode.
- SIGNAL STRENGTH:** A bar chart showing signal strength levels. The status is "No Device / Not Detected". Legend: Excellent (4 bars), Good (3 bars), Poor (2 bars), No Device / Not Detected (1 bar).
- WWAN NETWORK STATUS:** Gateway (Router) Address: 0.0.0.0, IP (NAT Public) Address: 0.0.0.0, Subnet Mask: 0.0.0.0, DNS Server 1: 0.0.0.0, DNS Server 2: 0.0.0.0.
- USB MODEM ACCESS:** Use the following link to access the modem's internal web server, where you can monitor the runtime status and make changes to the settings. (Note: This feature is useful for many WWAN devices, but it's not fully supported on all WWAN devices.) A button labeled "Click to Access Modem" is present.

NOTE: RAT Mode and Signal Strength displays are not supported on all modems. For modems that are not supported, the display defaults to RAT Mode = LTE and Signal Strength = Good. You should use the “Click to Access Modem” feature to access the management interface of your modem and to see additional information about signal-strength, mode, and so on..

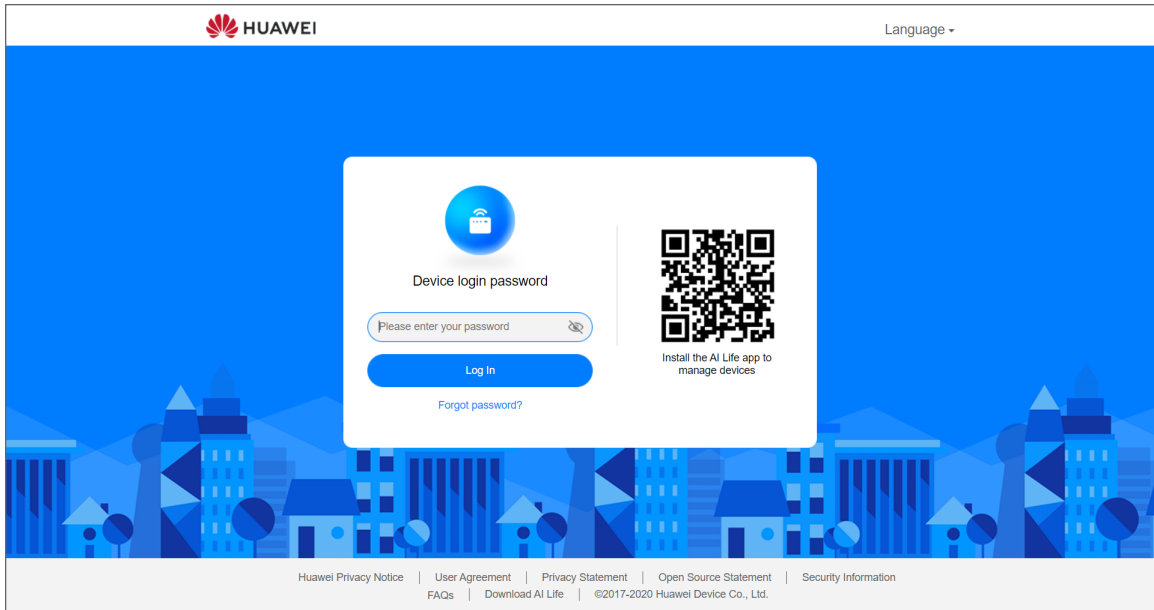
USB Modem Access

You can use **Click to Access Modem** in the **USB Modem Access** section to access the modem's internal web server to monitor runtime status and make changes to the modem settings.

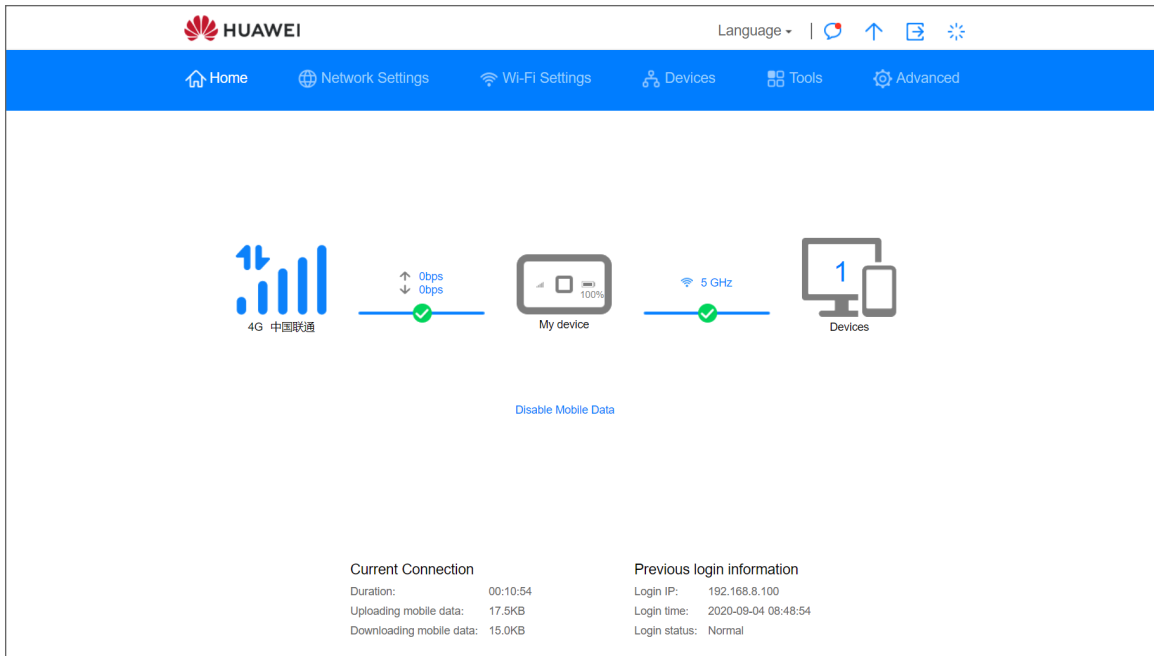
To make changes to the modem settings:

1. Navigate to **DEVICE | WWAN** and scroll to the **USB Mode Access** section.
2. Click **Click to Access Modem**.

- Depending on your modem provider, these pages might appear differently, but in this instance, you would log in to a Huawei account page that has been set up for your modem.



- Enter your password and click **Login**.



- From there, you can adjust settings as directed by your provider.

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 WWAN Administration Guide

Updated - December 2023

Software Version - 7.1

232-005869-00 Rev A

Copyright © 2023 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