




# SONICWALL SMA 210 Secure Mobile Access 210 User Guide

[Home](#) » [SONICWALL](#) » SONICWALL SMA 210 Secure Mobile Access 210 User Guide 



## SMA 210 Secure Mobile Access 210 User Guide

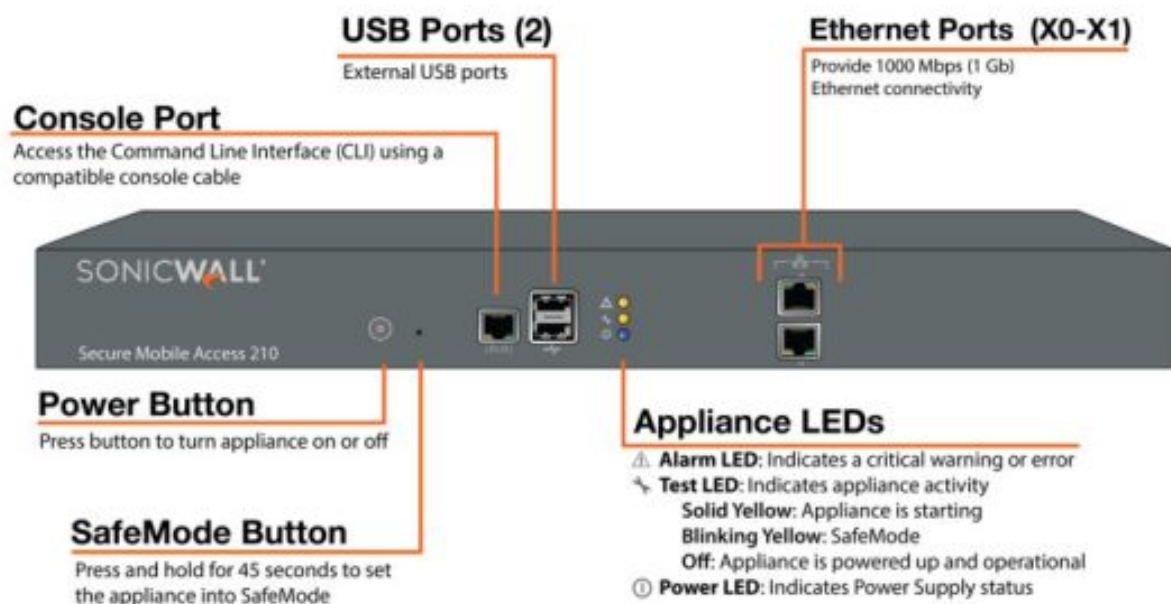
### Contents

- 1 Hardware Overview
  - 1.1 SMA 210 Front Panel
  - 1.2 SMA 410 Front Panel
- 2 SMA 210/410 Rear Panel
- 3 Checking Package Contents
  - 3.1 Package Contents
- 4 Power Input Rating
- 5 What You Need to Begin
- 6 Powering On the SMA Appliance
- 7 Accessing the Management Interface
- 8 Setting the Time Zone
- 9 Configuring DNS/WINS/Route
  - 9.1 Configuring your Network Interface
  - 9.2 Configuring a Default Route
- 10 Deploying Your Appliance
- 11 Connecting the SMA to the Gateway
- 12 Registering Your SMA Appliance
- 13 Configuring NetExtender Settings
- 14 Setting Your NetExtender Address Range
- 15 Verifying Connection from the Internet
- 16 Safety and Regulatory Information
  - 16.1 Appliance Mounting Information
  - 16.2 Lithium Battery Warning
  - 16.3 Cable Connections
- 17 Declaration of Conformity
- 18 Warranty Information
- 19 Documents / Resources
  - 19.1 References
- 20 Related Posts

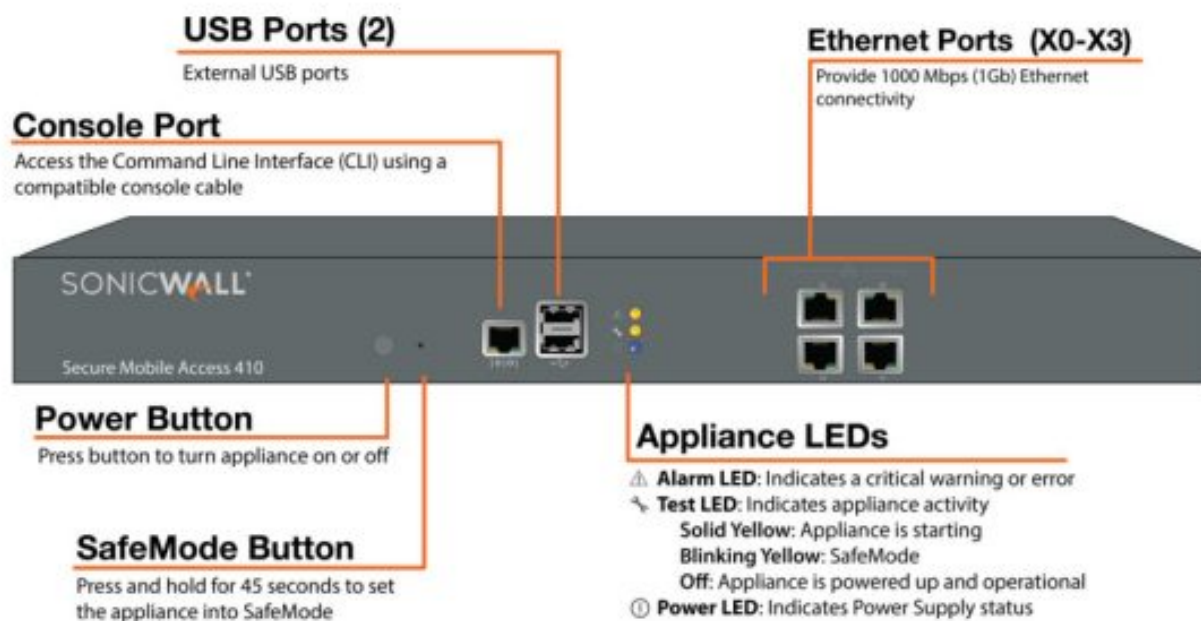
## Hardware Overview

SonicWall Secure Mobile Access 210/410 appliances provide a unified secure gateway to access all network and cloud resources.

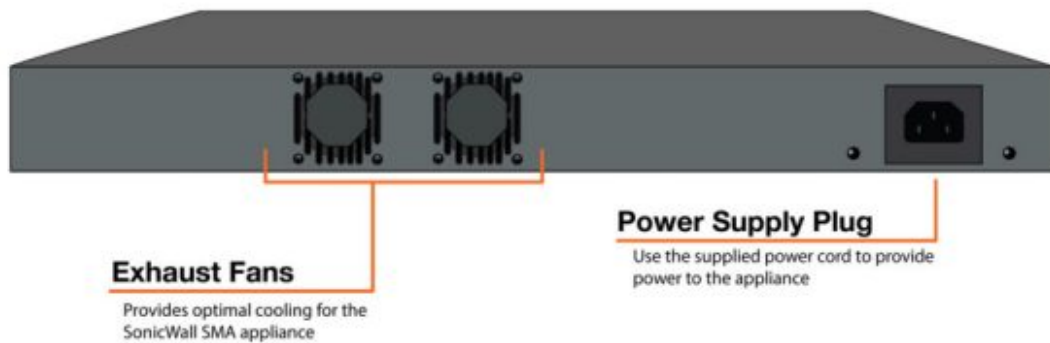
### SMA 210 Front Panel



### SMA 410 Front Panel



### SMA 210/410 Rear Panel



## Checking Package Contents

Before you begin setup, verify that your package contains the following items:

- One SonicWall SMA 210 or SMA 410 Appliance
- One SonicWall Secure Mobile Access Quick Start Guide
- One SonicWall Safety, Environmental, and Regulatory Information (SERI) Guide
- One Ethernet cable
- One serial console cable (RJ45 to DB9)
- One rack-mount kit
- Two power cords (1 North America and 1 Japan)



**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.

## Package Contents



**NOTE:** If any items are missing from your package, contact SonicWall Support at <https://www.sonicwall.com/support>

## Power Input Rating

This table lists the power input rating for the SMA 210/410 appliances:

V 1	V 100-240v~
A 1	A 1.5A Max.
Hz	50-60Hz

## What You Need to Begin

Before you install your SMA appliance, ensure that you have a Windows, Linux, or macOS computer with an RJ45 Ethernet port to use as a management station and administrative access to the network gateway device.

### Recording Configuration Information

Before you begin, record the following configuration information for your reference:

Information Needed	Your Configuration
Primary DNS Server	
IP Address	
Subnet	
Gateway Address	
Appliance IP Address	

## Powering On the SMA Appliance

To power on the SMA 210/410 appliance:

1. Plug one end of the power cord into the SMA 210/410 and the other into an appropriate power outlet.
  - The appliance automatically turns on when plugged in.
  - The power LED on the front panel illuminates blue when the appliance is turned on.
  - The test LED illuminates yellow until the firmware is booted. When the test LED is no longer lit, the SMA 210/410 is ready for configuration.
2. Connect one end of an Ethernet cable to the X0 port of your SMA 210/410.
3. Connect the other end of the cable to the management computer.

## Accessing the Management Interface

To access the web-based management interface:

1. Configure the LAN adapter on the management computer to use a static IP address.
  - Set it to a static IP address in 192.168.200.x/24 subnet, such as 192.168.200.20.
  - IMPORTANT:** Do not use 192.168.200.1, as this address will conflict with the appliance.
  - Use a Subnet Mask of 255.255.255.0. A Default Gateway is not required.
2. Open a browser and enter <https://192.168.200.1> (the default X0 management IP address).

NOTE: Accept the security certificate to continue.

3. In the Login screen, enter the default credentials and then click the Login button:

- Username – admin
- Password – password
- Domain – LocalDomain

4. A Software Transaction Agreement displays. Read the agreement, select the I Accept the terms of this Software Transaction Agreement check box, and then click Continue.

You are now successfully connected to the SMA management interface.



**CAUTION:** Changing your password from the factory default is strongly recommended. If you change your password, be sure to keep it in a safe place. If you lose your password, you will have to reset the SMA appliance to factory default settings, losing your configuration.



**NOTE:** SonicWall recommends that you create a second administrator account to prevent a logout.

## Setting the Time Zone

Setting the correct time is essential to the operations of the SMA 210/410. Be sure to set the time zone correctly. Leaving Automatically synchronize with an NTP server enabled (default setting) is recommended for accuracy.

**To set the time zone for your appliance:**

1. Navigate to the System > Time page.
2. Select the appropriate Time Zone from the drop-down menu.
3. Click ACCEPT to save changes to the time settings.

## Configuring DNS/WINS/Route

**To configure the DNS / WINS Servers:**

1. Navigate to the Network > DNS page in the management interface.
2. Enter a unique name for your appliance in the SMA Appliance Hostname field.



**NOTE:** Use an alphanumeric name with no spaces or special characters. Underbars are accepted.

3. Enter your Primary DNS Server information.
4. (Optional) Enter a Secondary DNS Server in the Secondary DNS Server field.
5. (Optional) Enter domain suffixes in the DNS Search List:
  - Type each domain suffix and click Add.
  - Use the directional up and down arrow keys to arrange the DNS suffixes in order of priority.
  - The first suffix in the list is appended to the hostname to create an FQDN, which is used to resolve names. If the name is not resolved, the next suffix in the list is used.
6. (Optional) Enter your WINS servers in the Primary WINS Server and Secondary WINS Server fields.
7. Click ACCEPT.



**NOTE:** It is not necessary to restart the system until you configure the default route.

## Configuring your Network Interface

When deploying the SMA on the LAN, you need to reset the IP address of the X0 interface on the SMA to an address within the range of the existing LAN subnet.

To configure the X0 IP address:

1. Navigate to the Network > Interfaces page.
2. In the Interfaces table, place your mouse pointer on the row for the X0 interface to display the Configure button and then click the button.
3. In the Edit Interface X0 screen, set the IP Address to an address on the same network as your default gateway. Select an unused address within your LAN subnet.
4. For the Subnet Mask, enter the value that matches your LAN subnet mask, such as 255.255.255.0.
5. Click OK. If a warning displays that you are changing the X0 IP Address, click OK.

The appliance restarts automatically. You can also press and hold the power button for 10 seconds to power down the SMA, then press it again to restart.

6. Reset the management computer to have a static IP address in the range you just set for the X0 interface. For example, if you set X0 to 10.1.1.10, you could set your computer to 10.1.1.20.
7. Log in to the SMA management interface again, using the IP address you just configured for the X0 interface. For example, point your browser to <https://10.1.1.10>.

## Configuring a Default Route

### To configure a default route:

1. Navigate to the Network > Routes page.
2. Enter the LAN interface IPv4 address in the Default IPv4 Gateway field or the IPv6 address in the Default IPv6 Gateway field.
3. Select X0 as the interface and click ACCEPT.

## Deploying Your Appliance

This guide provides configuration instructions for deploying your SMA appliance on the LAN. For information about deploying on a new or existing DMZ, see the SMA 210/410 Deployment Guide.

The primary interface (X0) on the SMA connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SMA appliance. The SMA appliance decrypts the session and determines the requested resource.

The session traffic then traverses the gateway appliance to reach the internal network resources. The gateway appliance applies security services as data traverses the gateway. The internal network resource then returns the requested content to the SMA appliance through the gateway, where it is encrypted and sent to the client.

Before deploying your SMA appliance, you must first add a custom zone on your gateway appliance. You can create a new custom zone on the gateway appliance when editing an interface on the Network | System > Interfaces page in SonicOS/ SonicOSX 7 or from the Network > Interfaces page in SonicOS 6.5. For more information about creating custom zones for an SMA appliance, see the SonicOS/X 7 System Administration Guide or the SonicOS 6.5 System Setup Administration Guide.

## Connecting the SMA to the Gateway

## To connect the SMA using the LAN:

1. Connect one end of an Ethernet cable to an unused port on your LAN hub or switch.
2. Connect the other end of the Ethernet cable to the X0 port on the front of your SMA 210/410. The X0 Port LED lights up indicating an active connection.

## Registering Your SMA Appliance

A MySonicWall account is required for product registration. Create a MySonicWall account at [www.MySonicWall.com](http://www.MySonicWall.com). Click Sign Up and follow the prompts.

To register your SMA appliance:

1. On the System > Status page click Register in the Register your SonicWall appliance link at the top of the screen. The System > Licenses page displays.
2. On the System > Licenses page, click the register link at the top of the page.
3. On the System > Licenses > License Management page, enter your MySonicWall credentials, then click Submit.
4. On the System > Licenses > License Management > Registration Completed page, click Continue.



**NOTE:** Your SMA 210/410 is loaded with SMA 10.2 firmware at the factory, but newer firmware is available. You can download the latest firmware, user licenses, and services at [www.MySonicWall.com](http://www.MySonicWall.com). For more information, see the SMA Upgrade Guide.

## Configuring NetExtender Settings

### Adding a NetExtender Client Route

NetExtender allows remote clients to have seamless access to resources on your local network.

To configure a NetExtender client route:

1. Navigate to the Clients > Routes page.
2. To force all SMA client traffic to pass through the NetExtender tunnel, select Enabled from the Tunnel All Mode drop-down list.
3. Click ADD CLIENT ROUTE.
4. Enter the network address of the trusted network to which you would like to provide access with NetExtender in the Destination Network field. For example, if you are connecting to an existing DMZ on the 10.1.1.0/24 subnet and you want to provide access to your LAN network on the 192.168.168.0/24 subnet, you would enter 192.168.168.0.
5. Enter the subnet mask of the destination network in the Subnet Mask field. Continuing the example, enter 255.255.255.0.
6. Click ACCEPT to finish adding this client route.

### Setting Your NetExtender Address Range

The NetExtender address range defines the IP address pool from which addresses will be assigned to remote users during NetExtender sessions. The range needs to be large enough to accommodate the maximum number

of concurrent NetExtender users you wish to support.

The range should fall within the same subnet as the interface to which the SMA appliance is connected, and it must not overlap or collide with any assigned addresses if other hosts are on the same segment as the SMA appliance.

You can select a range that falls within your existing LAN subnet. For example, if your LAN uses the 192.168.168.0/24 subnet, and you want to support up to 10 concurrent NetExtender sessions, you could use 192.168.168.240 to 192.168.168.249.

#### **To set your NetExtender address range:**

1. Navigate to Clients > Settings.
2. Enter an unused address range within your LAN in the Client Address Range Begin and Client Address Range End fields.
3. Click ACCEPT to add the Client Address Range.

If you do not have enough available addresses to support your desired number of concurrent NetExtender users, you may use a new subnet for NetExtender. This condition may occur if your existing LAN is configured in NAT mode with a small subnet space, such as 255.255.255.224, or more commonly if your LAN is configured in Transparent mode and you have a limited number of public addresses from your ISP. In either case, you may assign a new, unallocated IP range to NetExtender (such as 192.168.10.100 to 192.168.10.200) and configure a route to this range on your gateway appliance.

For example, if your current Transparent range is 67.115.118.75 through 67.115.118.80, and you wish to support 50 concurrent NetExtender clients, configure your SMA X0 interface with an available IP address in the Transparent range, such as 67.115.118.80, and configure your NetExtender range as 192.168.10.100 to 192.168.10.200. Then, on your gateway device, configure a static route to 192.168.10.0, using 67.115.118.80.

## **Verifying Connection from the Internet**

You can verify your connection using a remote client on the WAN.

To verify a connection from the Internet:

1. From a WAN connection outside of your corporate network, launch a browser and enter the following:  
`https://<WAN_IP_address_of_SMA>`
2. When prompted, enter the administrator or user credentials, such as admin /password.
3. Select LocalDomain or the configured domain from the drop-down menu and click Login. The SonicWall Virtual Office screen displays in your browser.
4. Click NetExtender to start the NetExtender client installation.
5. If prompted to install the SMA Connect Agent, click DOWNLOAD and then complete the client installation. Click [Details] for more information.
6. Ping a host on your corporate LAN to verify your remote connection. You have now successfully set up your SMA appliance.



**TIP:** It is easier for remote users to access the SMA appliance using a fully qualified domain name (FQDN) rather than an IP address. It is recommended that you create a DNS record to allow for FQDN access to your SMA appliance. If you do not manage your own public DNS servers, contact your ISP for assistance.

## **Next Steps**

Based on your network requirements, your next steps include:

- Configuring Custom Zones



- Configuring NetExtender
- Configuring Application Offloading

For advanced configuration topics, see the SMA Administration Guide.

## Safety and Regulatory Information

This section provides safety, regulatory, trademark, copyright, and warranty information.

Regulatory Model / Type	Product Name
1RK33-0BC	SMA 210
1RK33-0D9	SMA 410

### Appliance Mounting Information

The following conditions are required for proper installation of the SMA appliance:

1. The SonicWall appliance is designed to be mounted in a standard 19-inch rack mount cabinet.
2. Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the appliance.
3. Ensure that no water or excessive moisture can enter the unit.
4. Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
5. Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers.
6. Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C) is recommended.
7. If installed in a closed or multi-rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient.  
Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum recommended ambient temperature.
8. Mount the SonicWall appliance evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.
9. Four mounting screws, compatible with the rack design, must be used and hand-tightened to ensure secure installation. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch rack-mount cabinet.
10. A suitably rated and approved branch circuit breaker shall be provided as part of the building installation. Follow local code when purchasing materials or components.
11. Consideration must be given to the connection of the equipment to the supply circuit. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern. Do not overload the circuit.
12. Reliable grounding of rack-mounted equipment must be maintained.  
Particular attention must be given to power supply connections other than direct connections to the branch circuits, such as power strips.

13. The included power cords are 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.
14. Minimum power cord rating for European Union (CE): Certified power supply cord not lighter than light PVC sheathed flexible cord according to IEC 60227, designation, or H05 VV-F or H05 VVH2-F2, and rated for at least 3G 0.75 mm<sup>2</sup>.
15. The following statement applies only to rack-installed products that are GSMarked:  
This equipment is not intended for use at workplaces with visual display units, in accordance with §2 of the German ordinance for workplaces with visual display units.

### **Lithium Battery Warning**

The Lithium Battery used in the SonicWall SMA 210/410 appliance may not be replaced by the user. The appliance must be returned to a SonicWall authorized service center for replacement with the same or equivalent type recommended by the manufacturer. If, for any reason, the battery or SonicWall SMA 210/410 appliance must be disposed of, do so following the battery manufacturer's instructions.

### **Cable Connections**

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or another wiring that exits the building where the SonicWall appliance is located.

### **Declaration of Conformity**

A "Declaration of Conformity" in accordance with the directives and standards has been made and is on file at SonicWall International Limited, City Gate Park, Mahon, Cork, Ireland.

CE declarations can be found online at: <https://www.sonicwall.com/support>.



**NOTE:** Additional regulatory notifications and information for this product can be found online at: <https://www.sonicwall.com/support>.

### **Warranty Information**

SonicWall Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWall), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end-user of the product. SonicWall and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be a shipment of a replacement product. At SonicWall's discretion, the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWall's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWall's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse, or misapplication, or has been modified without the written permission of SonicWall.

**DISCLAIMER OF WARRANTY.** EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICES, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS

WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

**DISCLAIMER OF LIABILITY.** SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWall or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

**Copyright © 2021 SonicWall Inc. All rights reserved.**

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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/>.

## 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.

To access the Support Portal, go to <https://www.sonicwall.com/support>.

SMA Quick Start Guide

Updated – March 2021

232-004719-51 Rev A





**[SONICWALL SMA 210 Secure Mobile Access 210](#)** [pdf] User Guide  
SMA 210, SMA 410, Secure Mobile Access 210

## References

- [MySonicWall](#)
- [Support Portal & Downloads - SonicWall](#)
- [Support Portal & Downloads - SonicWall](#)
- [MySonicWall](#)
- [sonicwall.com/legal/](#)
- [Support Portal & Downloads - SonicWall](#)