

SonicWall™

Secure Mobile Access 200/400

Getting Started Guide

SMA 200 Regulatory Model Number: 1RK33-0BB

SMA 400 Regulatory Model Number: 1RK33-0BC



Copyright © 2017 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.

SMA 200/400 Getting Started Guide
Updated - March 2017
232-003789-50 RevA

In this Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWall™ Secure Mobile Access 200/400 appliances.

Chapters and sections

Chapter 1

[In this Guide](#) on page 3

Sections include:

[Chapters and sections](#) on page 3

Chapter 2

[Appliance Overview](#) on page 7

Sections include:

[SMA 200 Front and Rear Panels](#) on page 8

[SMA 200 Package Contents](#) on page 10

[SMA 400 Front and Rear Panels](#) on page 11

[SMA 400 Package Contents](#) on page 13

[Power Input Rating](#) on page 14

Chapter 3

[Setting Up the Appliance](#) on page 15

Sections include:

[What You Need to Begin](#) on page 16

[Powering On the SMA Appliance](#) on page 17

[Accessing the Management Interface](#) on page 17

[Troubleshooting](#) on page 18

[Changing Your Administrator Password](#) on page 18

[Adding a Local User](#) on page 19

[Setting the Time Zone](#) on page 20

[Configuring DNS and WINS](#) on page 21

Chapter 4

Registering Your Appliance on page 23

Sections include:

Creating a MySonicWall Account on page 24

Registering Your SMA Appliance on page 24

Services and Licensing on page 25

Upgrading Information on page 28

Chapter 5

Deploying Your Appliance on page 31

Sections include:

Selecting a Deployment Scenario on page 32

Configuring the X0 IP Address on page 34

Configuring a Default Route on page 35

Adding a NetExtender Client Route on page 35

Setting Your NetExtender Address Range on page 36

Adding a New SMA Custom Zone on page 38

Scenario A: Connecting the SMA on a New DMZ on page 40

Scenario B: Connecting the SMA on an Existing DMZ on page 45

Scenario C: Connecting the SMA on the LAN on page 49

Testing and Troubleshooting Your Remote Connection on page 52

Chapter 6

Sections include:

[Safety and Regulatory Information on page 55](#)

[Safety and Regulatory Information on page 56](#)

[Warranty Information on page 62](#)

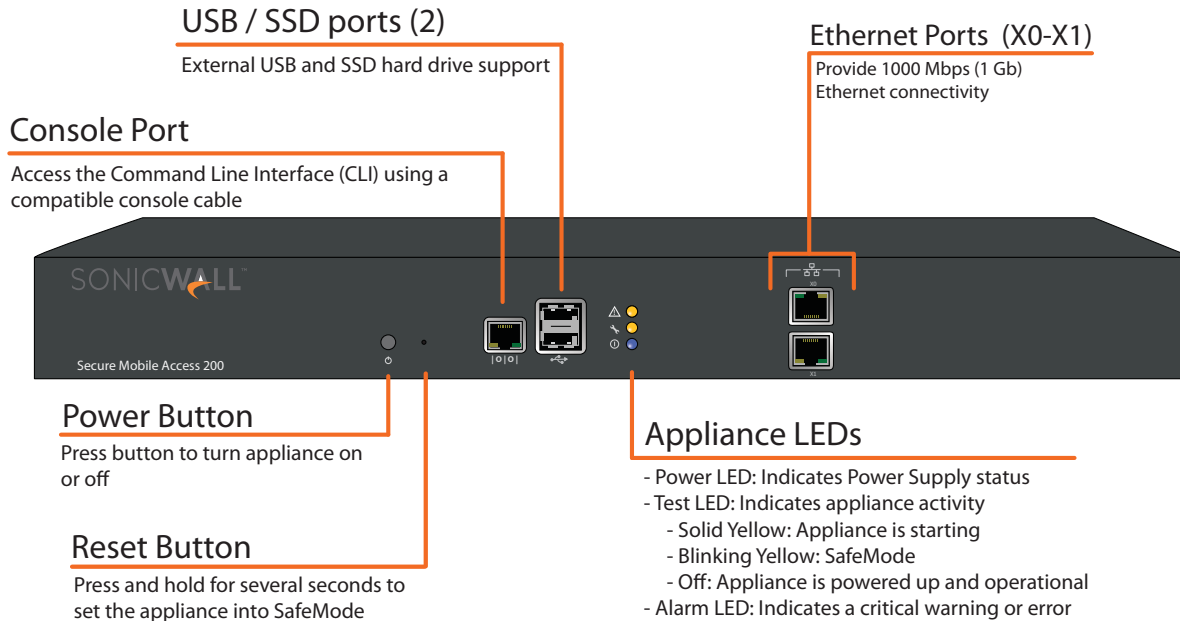
Appliance Overview

This section provides information about the SonicWall Secure Mobile Access 200/400 appliances.

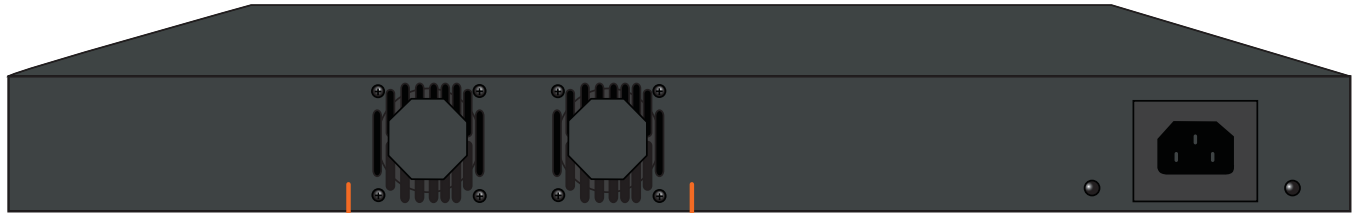
- [SMA 200 Front and Rear Panels](#) on page 8
- [SMA 200 Package Contents](#) on page 10
- [SMA 400 Front and Rear Panels](#) on page 11
- [SMA 400 Package Contents](#) on page 13
- [Power Input Rating](#) on page 14

SMA 200 Front and Rear Panels

Front Panel



Rear Panel



Exhaust Fans

Provides optimal cooling for the Sonicwall SMA appliance

Power Supply Plug

Use the supplied power cord to provide power to the appliance

SMA 200 Package Contents

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

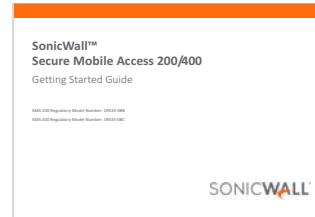
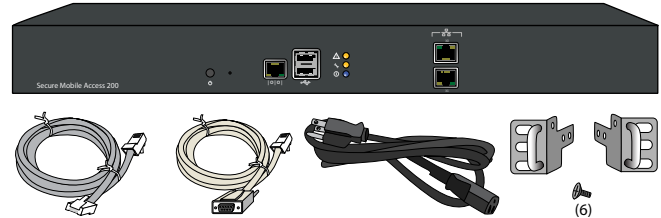
- One SonicWall SMA 200 appliance
- One SonicWall Secure Mobile Access 200/400 Getting Started Guide
- One SonicWall Safety, Environmental, and Regulatory Information Guide
- One Ethernet cable
- One serial console cable (RJ45 to DB9)
- One rack-mount kit
- One power cord

i **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.

Missing Items?

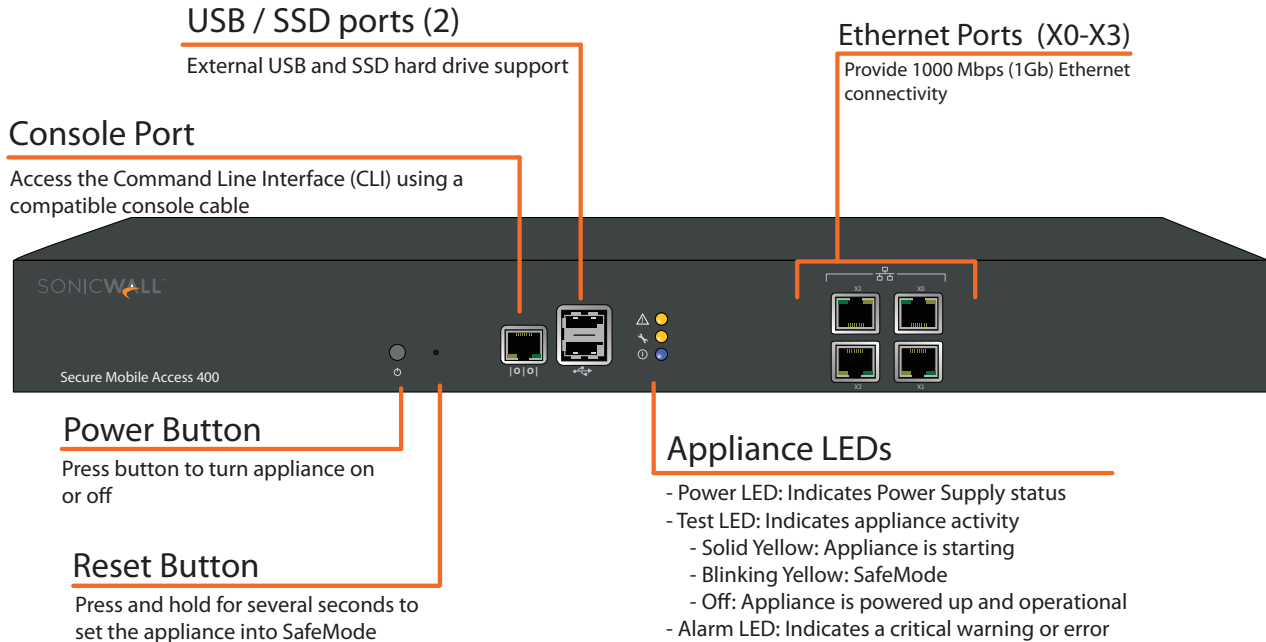
If any items are missing from your package, contact SonicWall Support:

Web: <https://support.sonicwall.com/>

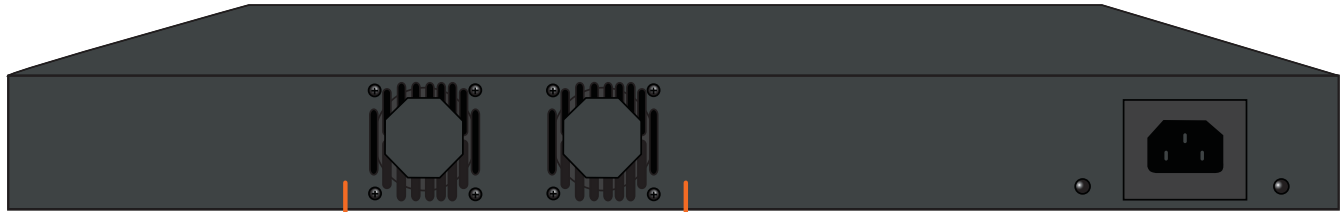


SMA 400 Front and Rear Panels

Front Panel



Rear Panel



Exhaust Fans

Provides optimal cooling for the SonicWall SMA appliance

Power Supply Plug

Use the supplied power cord to provide power to the appliance

SMA 400 Package Contents

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

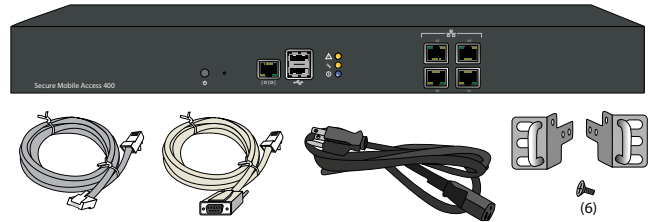
- One SonicWall SMA 400 appliance
- One SonicWall Secure Mobile Access 200/400 Getting Started Guide
- One SonicWall Safety, Environmental, and Regulatory Information Guide
- One Ethernet cable
- One serial console cable (RJ45 to DB9)
- One rack-mount kit
- One power cord

i **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.

Missing Items?

If any items are missing from your package, contact SonicWall Support:

Web: <https://support.sonicwall.com/>



Power Input Rating

The following table describes the power input rating for the SonicWall Secure Mobile Access 200/400 appliances:

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

Setting Up the Appliance

This section provides pre-configuration information and procedures for setting up your SonicWall Secure Mobile Access 200/400 appliance.

- [What You Need to Begin](#) on page 16
- [Powering On the SMA Appliance](#) on page 17
- [Accessing the Management Interface](#) on page 17
- [Troubleshooting](#) on page 18
- [Changing Your Administrator Password](#) on page 18
- [Adding a Local User](#) on page 19
- [Setting the Time Zone](#) on page 20
- [Configuring DNS and WINS](#) on page 21

What You Need to Begin

Before you install your SMA appliance, ensure the following are available:

- A Windows, Linux, or MacOS computer to use as a management station for initial configuration of the SonicWall Secure Mobile Access 200/400
- An Internet connection
- A Web browser supporting JavaScript and HTTP uploads. Supported browsers include the following:

Supported Browser	Browser Version
Internet Explorer	9.0 or higher
Mozilla Firefox	Latest version
Apple Safari	Latest version
Google Chrome	Latest version

- Administrative access to the network gateway device, depending on the deployment scenario selected

Use the following configuration information during the setup process and for future reference:

Serial Number: Record the serial number found on the top panel of your SonicWall appliance.

Authentication Code: Record the authentication code found on the top panel of your SonicWall appliance.

Admin Password: Select an administrator password. (default is *password*)

Network Configuration Information

Collect the following about your network configuration:

Primary DNS: _____

Secondary DNS (optional): _____

DNS Search List (in order): _____

WINS server(s) (optional): _____

Gateway IP address: _____

Gateway DMZ subnet (optional): _____

Powering On the SMA Appliance

To power on the SonicWall Secure Mobile Access 200/400 appliance:

- 1 Plug one end of the power cord into the SonicWall Secure Mobile Access 200/400 and the other into an appropriate power outlet.
- 2 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 SonicWall Secure Mobile Access 200/400 is ready for configuration.
- 3 Connect one end of an Ethernet cable into the X0 port of your SonicWall Secure Mobile Access 200/400. Connect the other end of the cable into the computer you are using to manage the SonicWall Secure Mobile Access 200/400.

Accessing the Management Interface

To access the Web-based management interface:

- 1 On the computer you use to manage the SonicWall Secure Mobile Access 200/400, set it to have a static IP address in the 192.168.200.x/24 subnet, such as 192.168.200.20. Use a Subnet Mask of 255.255.255.0. A Default Gateway is not required. Do not use 192.168.200.1, as this address will conflict with the appliance.
- 2 Open a Web browser, and enter <https://192.168.200.1> (the default X0 management IP address) in the Location or Address field.

i | **NOTE:** A security warning may appear. Click the option to accept the certificate and 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.

Troubleshooting

If you cannot connect to the SonicWall Secure Mobile Access 200/400, verify the following:

- Did you plug your management workstation into the X0 interface on the SMA appliance?

Management can only be performed through X0.

- Is the link light illuminated on both the management station and port X0 of the SMA appliance?
- Did you correctly enter the SMA appliance management IP address in your Web browser (default 192.168.200.1)?
- Is your computer set to a static IP address in the 192.168.200.x/24 subnet, such as 192.168.200.20?
- Is your Domain set to LocalDomain on the login screen?

If you are still unable to connect to the SMA appliance, contact SonicWall Support:

Web: <https://support.sonicwall.com/>

Changing Your Administrator Password

To change your administrator password:

- 1 In the SMA management interface, navigate to the **Users > Local Users** page.
- 2 Click the **Configure** button corresponding to the admin account.



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.

- 3 Enter a password for the **admin** account in the **Password** field. Re-enter the password in the **Confirm Password** field.

General User Settings

User Name:	admin
Primary Group:	LocalDomain (see all)
In Domain:	LocalDomain
User Type:	Administrator
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Password expires in:	<input type="text" value="0"/> days
Show warning:	<input type="text" value="0"/> days before password expiration
Require password change on next logon:	Use Domain Setting ▼
Account expires end of:	<input type="text"/>
Inactivity Timeout (minutes):	<input type="text" value="0"/>
Enforce login uniqueness:	Use Portal Setting ▼
Technician Allowed:	Use Domain Setting ▼

Single Sign-On Settings

Automatically log into bookmarks:	Use group setting ▼
-----------------------------------	---------------------

- 4 Click **Accept** to apply changes.

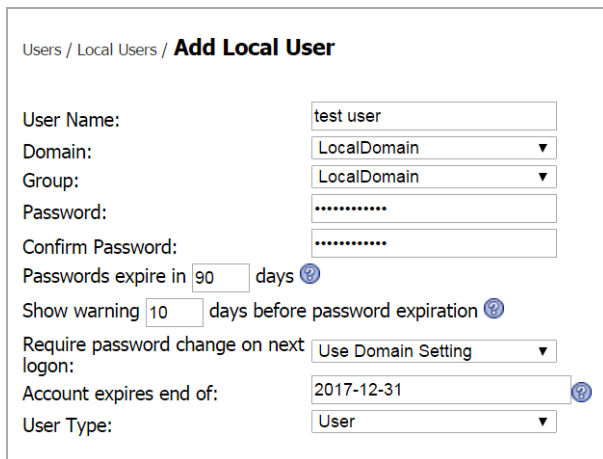
Adding a Local User

For testing and verification, you can create a local user account and in the local appliance authentication repository.

To add a local user:

- 1 Navigate to the **Users > Local Users** page.
- 2 Click the **Add User** button.
- 3 Enter a **User Name**.
- 4 Select **LocalDomain** from the **Domain** and **Group** drop-down menus.
- 5 Enter a password for the user in both the **Password** and **Confirm Password** fields.

- 6 Select **User** from the **User Type** drop-down menu.



Users / Local Users / **Add Local User**

User Name:

Domain:

Group:

Password:

Confirm Password:

Passwords expire in days

Show warning days before password expiration

Require password change on next logon:

Account expires end of:

User Type:

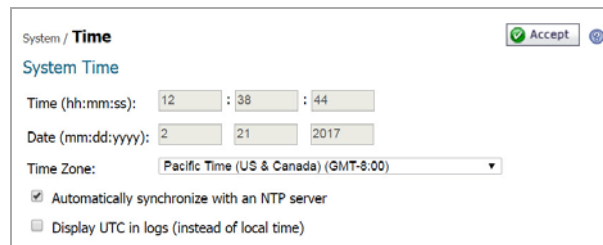
- 7 Click **Accept** to finish adding a local user.

Setting the Time Zone

Setting the correct time is essential to operations of the SonicWall SMA 200/400. Be sure to set the time zone correctly. Leaving **Automatic synchronization 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.



System / **Time** Accept

System Time

Time (hh:mm:ss): : :

Date (mm:dd:yyyy): / /

Time Zone:

Automatically synchronize with an NTP server

Display UTC in logs (instead of local time)

- 3 Click **Accept** to save changes to the time settings.

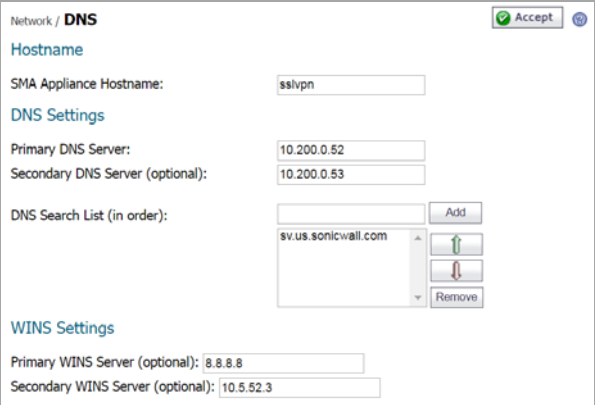
Configuring DNS and WINS

Refer to the notes you took in the [What You Need to Begin](#) on page 16 to complete this procedure.

To configure the DNS / WINS Servers:

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

- 4 (Optional) Enter a Secondary DNS Server in the **Secondary DNS Server** field.



The screenshot shows the 'Network / DNS' configuration page. At the top right, there is a green 'Accept' button. The page is divided into three sections: 'Hostname', 'DNS Settings', and 'WINS Settings'.
- **Hostname**: 'SMA Appliance Hostname' is set to 'sslvpn'.
- **DNS Settings**: 'Primary DNS Server' is '10.200.0.52' and 'Secondary DNS Server (optional)' is '10.200.0.53'. Below these is a 'DNS Search List (in order):' section with a list box containing 'sv.us.sonicwall.com'. To the right of the list box are 'Add', 'Up', 'Down', and 'Remove' buttons.
- **WINS Settings**: 'Primary WINS Server (optional)' is '8.8.8.8' and 'Secondary WINS Server (optional)' is '10.5.52.3'.

- 5 (Optional) Enter domain suffixes in the **DNS Search List**:
 - a Type each domain suffix and click **Add**.
 - b 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 host name to create a 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**.

Registering Your Appliance

This section provides instructions for registering your SonicWall Secure Mobile Access 200/400 appliances.

- [Creating a MySonicWall Account](#) on page 24
- [Registering Your SMA Appliance](#) on page 24
- [Services and Licensing](#) on page 25
- [Upgrading Information](#) on page 28

i | **NOTE:** Registration is an important part of the setup process and is necessary to receive the benefits of SonicWall services, user licensing, firmware updates, and technical support.

Creating a MySonicWall Account

A MySonicWall account is required for product registration. If you already have an account, continue to [Registering Your SMA Appliance](#) on page 24.

To create a MySonicWall account:

- 1 In your browser, navigate to www.MySonicWall.com.
- 2 In the login screen, click the [Register Now](#) link.



- 3 Complete the Registration form and click **Register**.
- 4 Verify that the information is correct and click **Submit**.
- 5 In the confirmation screen, click **Continue** to finish creating your MySonicWall account.

Registering Your SMA Appliance

Before you register your appliance, verify that the time, DNS, and default route settings on your SonicWall Secure Mobile Access 200/400 are correct.

To verify or configure these settings, navigate to the **System > Time, Network > DNS**, or **Network > Routes** pages, respectively.

Refer to [Setting Up the Appliance](#) on page 15 for more information.

To register your SMA appliance:

- 1 Log into your MySonicWall account. If you do not have an account, see [Creating a MySonicWall Account](#) on page 24.
- 2 On the main page, enter the appliance serial number in the **Register A Product** field. Click **Next**.

i **NOTE:** To determine the serial number and authentication code, refer to [What You Need to Begin](#) on page 16.

- 3 On the My Products page, select the **Product** button.
- 4 Enter a **Friendly Name** for the appliance.
- 5 If applicable, select the **Product Group** from the drop-down list.
- 6 Enter the **Authentication Code**.
- 7 Click **Register**.
- 8 Click **Continue**.

Services and Licensing

This section contains the following subsections:



- [Service Management](#) on page 26
- [Flexible Per-User Licensing](#) on page 27
- [Activating Services and Software](#) on page 27
- [Trying or Purchasing Services](#) on page 28

Service Management

The Service Management page in MySonicWall lists services, support options, and software, such as Web Application Firewall and Analyzer, that you can purchase or try with a free trial.

If you purchased an appliance that is pre-licensed, you may be required to enter your activation key here unless current licenses are already indicated in the Status column with either a license key or an expiration date.

Service Management

Serial Number:	XXXXXXXXXX	Node Support:	Unlimited
Registration Code:	LJM7TMZA	Platform:	SONICWALL
Authentication Code:	XXXXXXXXXX	Firmware:	
Product:		Product:	
Trusted:	Yes 	Release Status:	America Engineering Part Number
Registered On:	22 Apr 2016	Release Status:	ACTIVE 

The following products and services are available for the SonicWall SMA appliance:

- Gateway Services:
 - Node Upgrade
 - Spike License
- Desktop and Server Software:
 - Secure Virtual Assist/Secure Virtual Meeting
 - Web Application Firewall
 - Analyzer
 - End Point Control
 - Geo-IP & Botnet Filter
- Support Services:
 - Dynamic Support 8x5
 - Dynamic Support 24x7
 - Software and Firmware Updates
 - Hardware Warranty

Flexible Per-User Licensing

Your SMA appliance comes standard with a set number of user licenses. However, as the needs of your organization change, SonicWall offers flexible options when it comes to adding additional licenses. The ability to purchase a convenient number of additional licenses allows you to plan sensibly for the future, or provides immediate scalability when you need it most.

	SMA 200	SMA 400
Initial User Licenses	5	25
Additional Per-User License Packages	1 - 5 - 10	10 - 25 - 100
Maximum Concurrent User Sessions Allowed	50	250

Activating Services and Software

If you purchase a service subscription or upgrade from a sales representative, you will receive an activation key. This key is emailed to you after online purchases, or is on the front of the certificate that was included with your purchase.

To activate existing licenses:

- 1 Navigate to the **My Products** page and select the registered appliance you want to manage.
- 2 Locate the product on the Service Management page and click the Activate icon in that row.
- 3 In the Activate Service page, type or paste your key into the **Activation Key(s)** field and then click **Submit**. After the service is activated, you will see an expiration date or a license key string in the Status column on the Service Management page.

Trying or Purchasing Services

To try a free trial of a service, click the **Try** icon in the Service Management page.

To purchase a product or service, click Buy icon in the Service Management page.

When activation is complete, MySonicWall displays an activation screen with service status and expiration information. The service management screen also displays the product you licensed.

The licensed services also display on the **System > Licenses** page of your SonicWall SMA management interface.

Upgrading Information

This section includes the following topics for upgrading to the latest firmware image on your SMA appliance:

- [Obtaining the Latest SMA Firmware](#) on page 28
- [Uploading New SMA Firmware](#) on page 29
- [Accessing the Appliance using SafeMode](#) on page 29

Obtaining the Latest SMA Firmware

i **NOTE:** If you have already registered your SonicWall SMA appliance, and selected **Notify me when new firmware is available** on the **System > Settings** page, you are automatically notified of any updates available for your model.

To obtain a new SMA firmware image file:


- 1 Log into your MySonicWall account at www.MySonicWall.com.
- 2 Click **Downloads**.
- 3 On the Download Center page, select one of the following from the **Software Type** drop-down menu:
 - SMA 200 Firmware
 - SMA 400 Firmware
- 4 Scroll down to locate the firmware version you want, and then click the link for it and save it to a directory on your management station. For example, for the SonicWall SMA 400 appliance, this is a file such as:
sw_sma400_eng_8.6.0.0_8.1.0_p_5sv_966392.sig

Uploading New SMA Firmware

After the appliance starts up, the updated firmware version is displayed on the **System > Status** page.

To upload a new SMA firmware image:

- 1 Log into your SMA appliance as the administrator and navigate to the **System > Settings** page.
- 2 Select **Upload New Firmware** and browse to the location where you saved the SMA image file, select the file, and click the **Upload** button. The upload process can take up to one minute.
- 3 When the upload is complete, you are ready to reboot your SonicWall SMA appliance with the new SMA firmware. Do one of the following:
 - To boot the appliance with current configuration settings, click the boot icon for New Firmware
 - To boot the appliance with factory default settings, click the boot icon for New Firmware and select the check box to **Boot with factory default settings**
- 4 A warning message dialog is displayed: *Are you sure you wish to boot this firmware?* Click **Boot** to proceed.

 **CAUTION:** After clicking **Boot**, do not power off the device while the image is being uploaded to the flash memory.

Accessing the Appliance using SafeMode

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

You can upload new firmware and restart the appliance using the old or new firmware while in SafeMode.

You can set the appliance into SafeMode by using a narrow, straight object, like a straightened paper clip, to press and hold the reset button on the SMA appliance for five to ten seconds. When the appliance is in SafeMode, the test LED blinks yellow.

After the appliance is in SafeMode, connect your computer to X0 and point your browser to the default X0 IP address, then log in using the administrator credentials. You must set your computer to an available IP address on the X0 subnet.

For more information regarding SafeMode, refer to the latest version of the *SonicWall SMA Release Notes*.

Deploying Your Appliance

This section provides overviews of deployment scenarios, as well as configuration instructions for connecting your SonicWall SMA appliance to various network devices, including gateway appliances.

- [Selecting a Deployment Scenario](#) on page 32
- [Configuring the X0 IP Address](#) on page 34
- [Configuring a Default Route](#) on page 35
- [Adding a NetExtender Client Route](#) on page 35
- [Setting Your NetExtender Address Range](#) on page 36
- [Adding a New SMA Custom Zone](#) on page 38
- [Scenario A: Connecting the SMA on a New DMZ](#) on page 40
- [Scenario B: Connecting the SMA on an Existing DMZ](#) on page 45
- [Scenario C: Connecting the SMA on the LAN](#) on page 49
- [Testing and Troubleshooting Your Remote Connection](#) on page 52

 **TIP:** Before performing the procedures in this section, fill out the information in [What You Need to Begin](#) on page 16.

Selecting a Deployment Scenario

The deployment scenarios described in this section are based on actual customer deployments and are SonicWall-recommended deployment best practices for SMA appliances.

An SMA appliance is commonly deployed in one-arm mode over the DMZ interface on an accompanying gateway appliance, such as a SonicWall NSA 3600. This method of deployment offers additional layers of security control, plus the ability to use SonicWall's security services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering, Intrusion Prevention Service, and Comprehensive Anti-Spam Service, to scan all incoming and outgoing traffic.

The primary interface (X0) on the SonicWall SMA connects to an available segment on the gateway device. The encrypted user session is passed through the gateway to the SMA appliance. The SonicWall 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 SonicWall SMA appliance through the gateway, where it is encrypted and sent to the client.

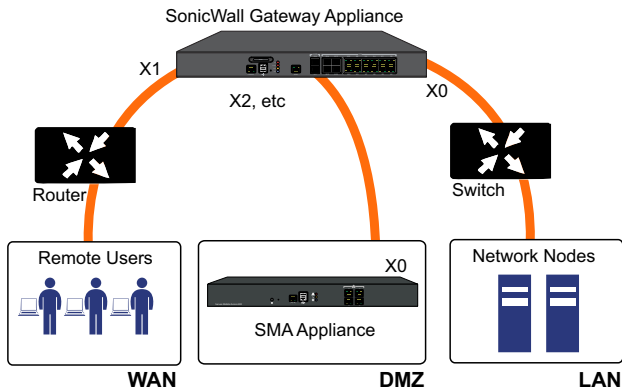
SMA 200/400 Deployment Scenarios

Gateway Appliance	Deployment Scenario	Requirements on Gateway Appliance
SonicOS 5.8.1 or higher: <ul style="list-style-type: none">• TZ Series• NSA E-Class• NSA Series• SM 9000 Series (SonicOS 6.1+)	SMA on New DMZ	<ul style="list-style-type: none">• An unused interface• New DMZ configured for NAT or Transparent Mode
	SMA on Existing DMZ	<ul style="list-style-type: none">• One dedicated interface in use as an existing DMZ
	SMA on LAN	<ul style="list-style-type: none">• None

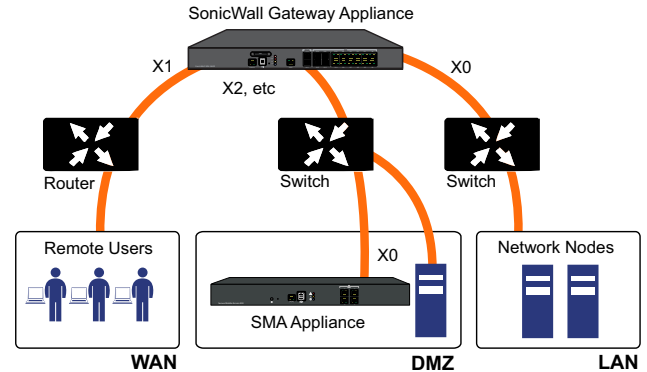
The following illustrations provide an overview of each deployment scenario:

- [Overview of Scenario A: SMA on a New DMZ](#) on page 33
- [Overview of Scenario B: SMA on an Existing DMZ](#) on page 33
- [Overview of Scenario C: SMA on the LAN](#) on page 34

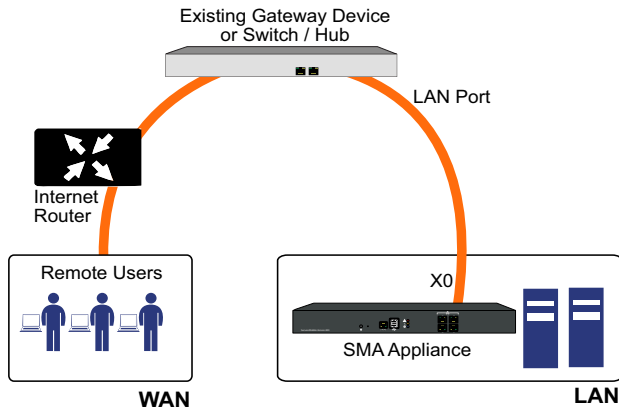
Overview of Scenario A: SMA on a New DMZ



Overview of Scenario B: SMA on an Existing DMZ



Overview of Scenario C: SMA on the LAN



Configuring the X0 IP Address

When deploying the SMA in any of the scenarios shown in [Selecting a Deployment Scenario](#) on page 32, you need to reset the IP address of the X0 interface on the SMA to an address

within the range of the new or existing DMZ or the existing LAN subnet.

To configure the X0 IP address:

- 1 Connect your computer to X0 and log into the SMA appliance by navigating to <https://192.168.200.1> on your Web browser.

TIP: For additional information, see [Accessing the Management Interface](#) on page 17.

- 2 Navigate to the **Network > Interfaces** page.
- 3 In the Interfaces table, click the Configure icon for the X0 interface.
- 4 In the Interface Settings dialog box, set the **IP Address** to an unused address within your DMZ or LAN subnet.
- 5 For the **Subnet Mask**, enter the value that matches your DMZ or LAN subnet mask, such as 255.255.255.0.
- 6 Click **Accept**. A warning displays that you are changing the X0 IP Address. Click **OK** to acknowledge.
- 7 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.

- 8 Log into 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

Refer to the following table to correctly configure your default route for the scenario you selected.

If you are using scenario:	Your upstream gateway IP address will be:
A - SMA on a New DMZ	The IP address of the DMZ interface you create
B - SMA on an Existing DMZ	The existing DMZ interface IP address
C - SMA on the LAN	The LAN interface IP address

To configure a default route:

- 1 Navigate to the **Network > Routes** page.
- 2 Enter the upstream gateway device's 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**.

Network / **Routes** Accept ?

Default Route

Default IPv4 Gateway:

Interface:

Default IPv6 Gateway:

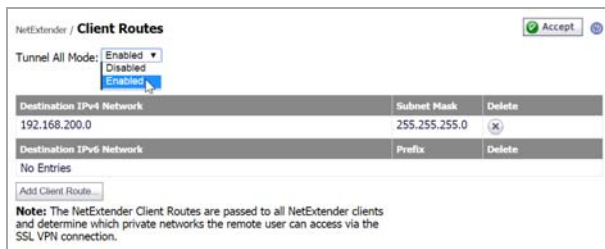
Interface:

Adding a NetExtender Client Route

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

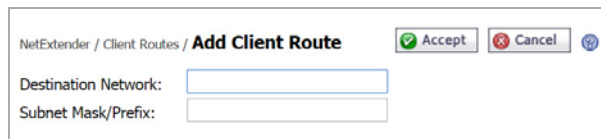
To configure a NetExtender client route:

- 1 Navigate to the **NetExtender > Client 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/Prefix** 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.

Determine the correct subnet based on your network scenario selection:

Scenario A	192.168.200.100 to 192.168.200.200 (default range)
Scenario B	Select a range that falls within your existing DMZ subnet. For example, if your DMZ uses the 10.1.1.0/24 subnet, and you want to support up to 30 concurrent NetExtender sessions, you could use 10.1.1.220 to 10.1.1.249 .
Scenario C	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 .

i **NOTE:** DHCP/DHCPv6 is supported and can manage the IPv4 and IPv6 addresses in the LAN and the NetExtender client address ranges.

To set your NetExtender address range:

- 1 Navigate to the **NetExtender > Client Settings** page.
- 2 Enter an address range in the **Client Address Range Begin** and **Client Address Range End** fields.
- 3 Click **Accept** to add the Client Address Range.

Scenario A	192.168.200.100 to 192.168.200.200 (default range)
Scenario B	An unused range within your DMZ subnet.
Scenario C	An unused range within your LAN subnet.

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 DMZ or LAN is configured in NAT mode with a small subnet space, such as 255.255.255.224, or more commonly if your DMZ or 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.

Adding a New SMA Custom Zone

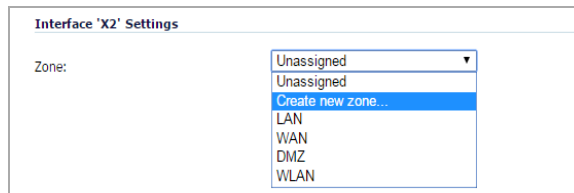
Adding a new SMA custom zone on your gateway appliance is a necessary step in deploying your SMA appliance using Scenarios A and C. For more information, see the following sections:

- [Scenario A: Connecting the SMA on a New DMZ](#) on page 40
- [Scenario C: Connecting the SMA on the LAN](#) on page 49

To add a new SMA custom zone on the gateway appliance:

- 1 Log into your gateway appliance as an administrator and navigate to the **Network > Interfaces** page.

- 2 Click the **Configure** icon for the interface connected to your SMA, such as X2.
- 3 Select **Create new zone** in the **Zone** field.



The Add Zone window opens.

- 4 Enter **SMA** in the **Name** field.
- 5 Select **Public** from the **Security Type** drop-down menu.
- 6 Clear the **Allow Interface Trust** check box.
- 7 Select the following check boxes:
 - **Enable Gateway Anti-Virus Service**
 - **Enable IPS**

- **Enable Anti-Spyware Service**

The screenshot shows the 'Guest Services' configuration window. Under 'General Settings', the 'Name' field contains 'SMA' and the 'Security Type' dropdown is set to 'Public'. The following services are listed:

- Allow Interface Trust
- Auto-generate Access Rules to allow traffic between zones of the same trust level
- Auto-generate Access Rules to allow traffic to zones with lower trust level
- Auto-generate Access Rules to allow traffic from zones with higher trust level
- Auto-generate Access Rules to deny traffic from zones with lower trust level
- Enforce Content Filtering Service
 - CFS Policy:
- Enable Client AV Enforcement Service
- Enable Client CF Service
- Enable SSLVPN Access
- Create Group VPN
- Enable SSL Control
- Enable Gateway Anti-Virus Service
- Enable IPS
- Enable Anti-Spyware Service
- Enable App Control Service

- 8 Click **OK**.
- 9 In the Edit Interface window again, enter the IP address for this interface in the **IP Address** field.

For example:

Scenario A	Use an IP address in the default SMA X0 subnet (default 192.168.200.x)
Scenario C	Use an IP address in the gateway LAN subnet (default 192.168.168.x)

- 10 Enter your **Subnet Mask**.
- 11 Optionally enter the **Default Gateway**, which is the WAN address of the gateway appliance.
- 12 If you want to allow management of the gateway appliance over this interface, select the desired management options.
- 13 If you want to allow users to log in to the gateway appliance using this interface, select the desired user login options.
- 14 Click **OK** to apply changes.

Scenario A: Connecting the SMA on a New DMZ

The following procedures explain how to configure your gateway appliance based on Scenario A:

- [Connecting the SMA to the Gateway](#) on page 40
- [Allowing a WAN to SMA Connection](#) on page 40
- [Allowing an SMA to LAN Connection](#) on page 42

Connecting the SMA to the Gateway

To connect the SMA 200/400 using Scenario A:

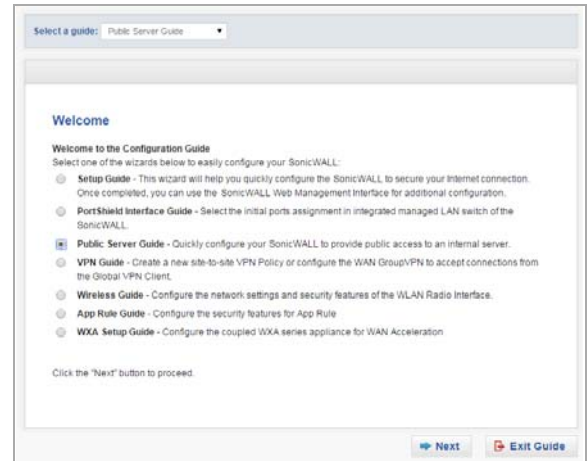
- 1 Connect one end of an Ethernet cable to an unused port on your SonicWall gateway appliance.
- 2 Connect the other end of the Ethernet cable to the X0 port on the front of your SonicWall Secure Mobile Access 200/400. The X0 Port LED lights up indicating an active connection.
- 3 Configure the SMA X0 IP address. Refer to [Configuring the X0 IP Address](#) on page 34.

Allowing a WAN to SMA Connection

- i** **NOTE:** Before continuing, you must add a new SMA custom zone. Refer to [Adding a New SMA Custom Zone](#) on page 38 for more information.

To allow a WAN to SMA connection:

- 1 Click the **Wizards** icon in the top right corner of the gateway appliance management interface.
- 2 On the Welcome page, select the **Public Server Guide**, and then click **Next**.

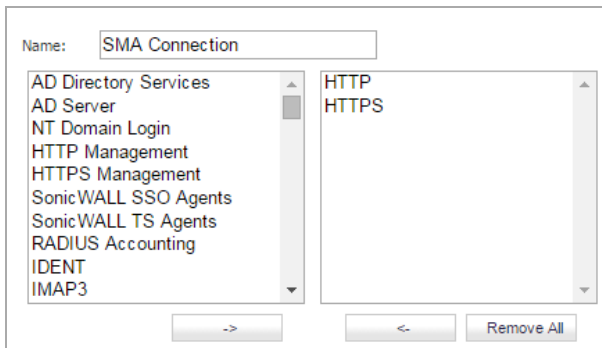


3 On the Public Server Guide, select these options:

Service Type	Other
Services	Create new group

4 In the Add Service Group dialog box, create a service group for HTTP and HTTPS:

- Enter a **Name** for the service.
- Select both **HTTP** and **HTTPS** and click the arrow button to move them to the right column.
- Click **OK**.



5 On the Server Private Network Configuration page, enter the following server and SMA information, and then click **Next**:

Server Name	Specify the name for the SMA appliance
Server Private IP Address	SMA appliance X0 IP address
Server Comment	Brief description of the server

6 On the Server Public Information page, accept the default IP address, or enter an IP address in your allowed public IP range. Click **Next**.

NOTE: The default IP address is the WAN IP address of your SonicWall security appliance. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SMA appliance.

7 The Public Server Configuration Summary page displays all the configuration actions that will be performed. Click **Apply** to create the configuration and allow access from the WAN to the SMA on the DMZ.

Allowing an SMA to LAN Connection

When users have connected to the SMA, they need to be able to connect to resources on the LAN.

To allow an SMA to LAN connection:

- 1 Navigate to the **Network > Address Objects** page on the gateway appliance.
- 2 In the Address Objects tab, click **Add**.
- 3 In the Add Address Object dialog box, create an address object for the X0 interface IP address of your SMA appliance:

Name	Name of the SMA appliance
Zone Assignment	SMA
Type	Host
IP Address	SMA appliance X0 IP address (default 192.168.200.1)

Name:	<input type="text" value="SMA Appliance"/>
Zone Assignment:	<input type="text" value="SMA"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text" value="192.168.200.1"/>

- 4 Click **Add** to create the object. Once done, click **Close**.
- 5 Click **Add** again to create an address object for the NetExtender range.
- 6 In the Add Address Object dialog box, create an address object for the NetExtender range:

Name	Name for NetExtender
Zone Assignment	SMA
Type	Range
Starting IP Address	Start of the NetExtender IP address range (default 192.168.200.100)
Ending IP Address	End of the NetExtender IP address range (default 192.168.200.200)

Name:

Zone Assignment:

Type:

Starting IP Address:

Ending IP Address:

Ready

- 7 Click **Add** to create the object. Once added, click **Close**.
- 8 On the **Network > Address Objects** page, click the **Address Groups** tab.
- 9 Click **Add Group**.
- 10 In the Add Address Object Group dialog box, create a group for the X0 interface IP address of your SMA appliance and the NetExtender IP range:

- Enter a name for the group.
- In the left column, select the address objects you created and click the right arrow button.

- Click **OK** to create the group when both objects are in the right column.

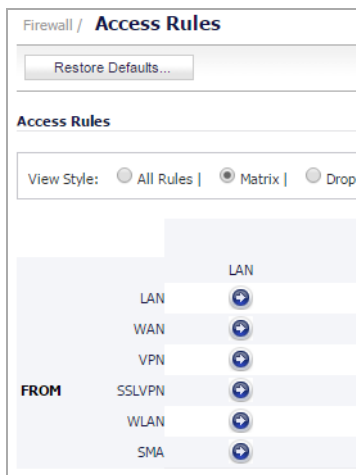
Name:

<ul style="list-style-type: none"> All Authorized Access Points All Interface IP All Interface IPv6 Addresses All Rogue Access Points All Rogue Devices All SonicPoints All U0 Management IP All W0 Management IP All WAN IP All X0 Management IP 	<input type="button" value="→"/> <input type="button" value="←"/>	<ul style="list-style-type: none"> NetExtender Connection SMA Appliance
---	--	---

Ready

- 11 Navigate to the **Firewall > Access Rules** page, and select the Matrix view style.

12 Click the **SMA > LAN** icon.



13 On the page that displays for SMA to LAN, click **Add**.

14 In the Add Rule window, create a rule to allow access to the LAN for the address group you just created:

From	SMA
To	LAN
Source Port	Any
Service	Any

Source	The address group you just created, such as SMA and NetExtender.
Destination	Any
Users Allowed	All
Users Excluded	None
Schedule	Always on
Select the following check box(es)	<ul style="list-style-type: none">• Enable Logging• Allow Fragmented Packets

15 Click **OK** to create the rule.

This completes Scenario A. Continue to [Testing and Troubleshooting Your Remote Connection](#) on page 52.

i **NOTE:** Some gateway appliances have a default zone named SSLVPN. Do **not** select this zone when configuring for the SMA appliance. The SSLVPN zone is intended for use with the more limited SSLVPN features that are included in the firewall products.

Scenario B: Connecting the SMA on an Existing DMZ

The following procedures explain how to configure your gateway appliance based on Scenario B:

- [Connecting the SMA to the Gateway](#) on page 45
- [Allowing WAN to DMZ Connection](#) on page 45
- [Allowing DMZ to LAN Connection](#) on page 47

Connecting the SMA to the Gateway

To connect the SMA using Scenario B:

- 1 Connect one end of an Ethernet cable to your DMZ, either directly to the corresponding port on your existing SonicWall gateway appliance, to a hub, or to a switch on your DMZ.
- 2 Connect the other end of the Ethernet cable to the X0 port on your SonicWall Secure Mobile Access 200/400. The X0 Port LED lights up indicating an active connection.

- 3 Configure the SMA X0 with an IP address in the DMZ subnet. Refer to [Configuring the X0 IP Address](#) on page 34.

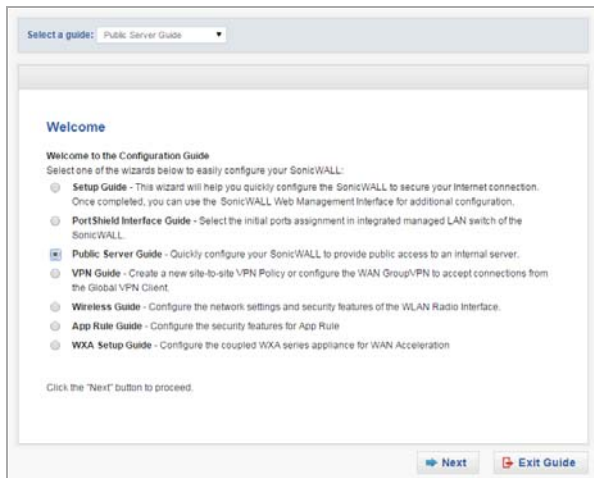
Allowing WAN to DMZ Connection

If you are already forwarding HTTP or HTTPS to an internal server and you only have a single public IP address, you will need to select different (unique) ports of operation for either the existing servers or for the SMA appliance, because both cannot concurrently use the same IP address and port combinations.

To allow a WAN to DMZ connection:

- 1 Log into your gateway appliance as an administrator and click the **Wizards** icon at the top right of the interface.

- On the Welcome page, select the **Public Server Guide**, and then click **Next**.



- On the Public Server Guide page of the Wizard, select:

Service Type	Other
Services	Create new group

The Add Service Group dialog box is displayed.

- In the Add Service Group dialog box, create a service group for HTTP and HTTPS:
 - Enter a name for the service.
 - Select both **HTTP** and **HTTPS** and click the arrow button to move to the right column.
 - Click **OK**.
- On the Server Private Network Configuration page, enter the following Server information and click **Next**:

Server Name	Name for the SMA appliance
Server Private IP Address	The X0 IP address of the SMA appliance within your DMZ range, such as 10.1.1.10/24.
Server Comment	Brief description of the server

- On the Server Public Information page, accept the default IP address or enter a new IP address in your allowed public IP range. Click **Next**.

i **NOTE:** The default IP address is the WAN IP address of your SonicWall firewall. If you accept this default, all HTTP and HTTPS traffic to this IP address will be routed to your SMA appliance.

- The Public Server Configuration Summary page displays all configuration actions that will be performed. Click

Apply to create the configuration and allow access from the WAN to the SMA appliance on the DMZ.

Allowing DMZ to LAN Connection

When users have connected to the SMA, they need to be able to connect to resources on the LAN.

To allow a DMZ to LAN connection:

- 1 On your gateway appliance, navigate to the **Network > Address Objects** page.
- 2 In the **Address Objects** tab, click **Add**.
- 3 In the Add Object dialog box, create an address object for the X0 interface IP address of your SMA appliance:

Name	Name for the SMA appliance
Zone Assignment	DMZ
Type	Host
IP Address	X0 IP address of the SMA appliance within your DMZ range, such as 10.1.1.10.

Name:	<input type="text" value="SMA Appliance 2"/>
Zone Assignment:	<input type="text" value="DMZ"/>
Type:	<input type="text" value="Host"/>
IP Address:	<input type="text" value="10.1.1.10"/>

- 4 Click **OK** to create the object. Once added, click **Close**.
- 5 Click **Add** again to create an address object for the NetExtender range.
- 6 In the Add Object dialog box, create an address object for the NetExtender range using the following options, then click **Add**:

Name	Name for NetExtender
Zone Assignment	DMZ
Type	Range
Starting IP address	Start of the NetExtender IP address range within your DMZ range, such as 10.1.1.220.
Ending IP address	End of the NetExtender IP address range within your DMZ range, for example 10.1.1.249.

Name:

Zone Assignment:

Type:

Starting IP Address:

Ending IP Address:

- 7 On the **Network > Address Objects** page, click the **Address Groups** tab.
- 8 Click **Add Group**.
- 9 In the Add Address Object Group dialog box, create a group for the X0 interface IP address of your SMA appliance and the NetExtender IP range:
 - Enter a name for the group.
 - In the left column, select the address objects you created and click the right arrow button.

- Click **OK** to create the group when both objects are in the right column.

Name:

<ul style="list-style-type: none"> All Authorized Access Points All Interface IP All Interface IPv6 Addresses All Rogue Access Points All Rogue Devices All SonicPoints All U0 Management IP All W0 Management IP All WAN IP All X0 Management IP 	<input type="button" value="→"/> <input type="button" value="←"/>	<ul style="list-style-type: none"> NetExtender 2 SMA Appliance 2
---	--	--

Ready

- 10 On the **Network > Interfaces** page, verify that the assigned zone is DMZ for the interface connected to your SMA appliance.
- 11 Navigate to the **Firewall > Access Rules** page, and select the Matrix view style.
- 12 Click the **DMZ > LAN** icon.
- 13 On the page that displays for DMZ to LAN, click **Add**.

- 14 In the Add Rule window, create a rule to allow access to the LAN for the address group you just created:

From	DMZ
To	LAN
Service Port	Any
Service	Any
Source	The address group you just created, such as SMA and NetExtender 2.
Destination	Any
Users Allowed	All
Users Excluded	None
Schedule	Always on
Select the following check box(es)	<ul style="list-style-type: none">• Enable Logging• Allow Fragmented Packets

- 15 Click **OK** to create the rule.
This completes Scenario B. Continue to [Testing and](#)

[Troubleshooting Your Remote Connection](#) on page 52.

i **NOTE:** Some gateway appliances have a default zone named SSLVPN. Do **not** select this zone when configuring for the SMA appliance. The SSLVPN zone is intended for use with the more limited SSLVPN features that are included in the firewall products.

Scenario C: Connecting the SMA on the LAN

The following procedures explain how to configure your gateway appliance based on Scenario C:

- [Connecting the SMA to the Gateway](#) on page 49
- [Configuring SMA to LAN Connectivity](#) on page 50

Connecting the SMA to the Gateway

To connect the SMA using Scenario C:

- 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 SonicWall Secure Mobile

Access 200/400. The X0 Port LED lights up indicating an active connection.

- 3 Configure the SMA X0 IP address. Refer to [Configuring the X0 IP Address](#) on page 34.

Configuring SMA to LAN Connectivity

NOTE: Before continuing, you must add a new SMA custom zone. Refer to [Adding a New SMA Custom Zone](#) on page 38 for more information.

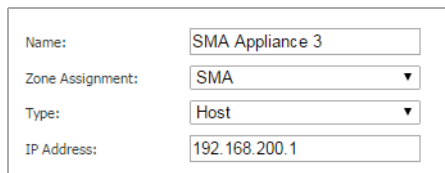
In order for users to access local resources through the SMA appliance, you must configure your gateway device to allow an outside connection through the SMA into your LAN.

To allow an SMA to LAN connection:

- 1 Log into your gateway appliance as an administrator and navigate to the **Network > Address Objects** page.
- 2 In the **Address Objects** tab, click **Add**.

- 3 In the Add Object dialog box, create an address object for the X0 interface IP address of your SMA:

Name	Name for the SMA appliance
Zone Assignment	SMA
Type	Host
IP Address	SMA appliance X0 IP address (default 192.168.200.1)



The screenshot shows a dialog box with four fields: Name (SMA Appliance 3), Zone Assignment (SMA), Type (Host), and IP Address (192.168.200.1). Each field is a text input or a dropdown menu.

- 4 Click **Add** to create the object. After adding, click **Close**.
- 5 Click **Add** again to create an address object for the NetExtender range.
- 6 In the Add Object dialog box, create an address object for the NetExtender range, using the following options:

Name	Name for NetExtender
Zone Assignment	SMA
Type	Range

Starting IP Address Start of the NetExtender IP address range (default 192.168.200.100)

Ending IP Address End of the NetExtender IP address range (default 192.168.200.200)

Name:	<input type="text" value="NetExtender 3"/>
Zone Assignment:	<input type="text" value="SMA"/>
Type:	<input type="text" value="Range"/>
Starting IP Address:	<input type="text" value="192.168.200.100"/>
Ending IP Address:	<input type="text" value="192.168.200.200"/>

- 7 Click **Add** to create the object. Once added, click **Close**.
- 8 On the **Network > Address Objects** page, click the **Address Group** tab.
- 9 Click **Add Group**.
- 10 In the Add Address Object Group dialog box, create a group for the X0 interface IP address of your SMA and the NetExtender IP range:

- Enter a name for the group.
- In the left column, select the two address objects you created and click the right arrow button.
- Click **OK** to create the group when both objects are in the right column.

Name: <input type="text" value="SMA to LAN"/>	
<input type="text" value="NetExtender Connection"/> <input type="text" value="Node License Exclusion List"/> <input type="text" value="Prefixes from DHCPv6 Delega"/> <input type="text" value="Public Mail Server Address Gr"/> <input type="text" value="RADIUS Accounting Clients"/> <input type="text" value="RBL User Black List"/> <input type="text" value="RBL User White List"/> <input type="text" value="SMA Appliance"/> <input type="text" value="SMA Appliance 2"/> <input type="text" value="SMA Interface IP"/>	<input type="text" value="NetExtender 3"/> <input type="text" value="SMA Appliance 3"/>
Ready	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- 11 Navigate to the **Firewall > Access Rules** page, and select the Matrix view style.
- 12 Click the **SMA > LAN** icon.
- 13 On the page that displays for SMA to LAN, click **Add**.

- 14 In the Add Rule window, create a rule to allow access to the LAN for the address group you just created:

From	SMA
To	LAN
Source Port	Any
Service	Any
Source	The address group you just created, such as SMA to LAN.
Destination	Any
Users Allowed	All
Users Excluded	None
Schedule	Always on
Select the following check box(es)	Enable Logging Allow Fragmented Packets

- 15 Click **OK** to create the rule.
This completes Scenario C. Continue to [Testing and Troubleshooting Your Remote Connection](#) on page 52.

NOTE: Some gateway appliances have a default zone named SSLVPN. Do **not** select this zone when configuring for the SMA appliance. The SSLVPN zone is intended for use with the more limited SSLVPN features that are included in the firewall products.

Testing and Troubleshooting Your Remote Connection

You have now configured your SonicWall gateway appliance and SMA appliance for secure remote access.

This section provides information on the following topics:

- [Verifying a User Connection from the Internet](#) on page 52
- [Firewall > Access Rules Matrix View](#) on page 53

Verifying a User Connection from the Internet

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

To verify a User Connection from the Internet:

- 1 From a WAN connection outside of your corporate network, launch a Web browser and enter the following:

https://<WAN_IP_address_of_gateway_device>

- When prompted, enter the **User Name** and **Password** created in [Adding a Local User](#) on page 19 of this guide.
- Select **LocalDomain** from the drop-down menu and click **Login**. The SonicWall Virtual Office screen displays in your Web browser.



- Click **NetExtender** to start the NetExtender client installation.
- If prompted, click **Install** to complete the client installation.
- Ping a host on your corporate LAN to verify your remote connection.

You have now successfully set up your SMA appliance.

i 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.

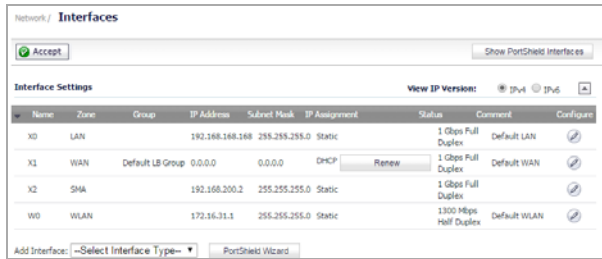
Firewall > Access Rules Matrix View

If the SMA zone does not appear in the Firewall > Access Rules matrix view, verify that it is selected as the zone for the gateway interface connected to the SMA appliance.

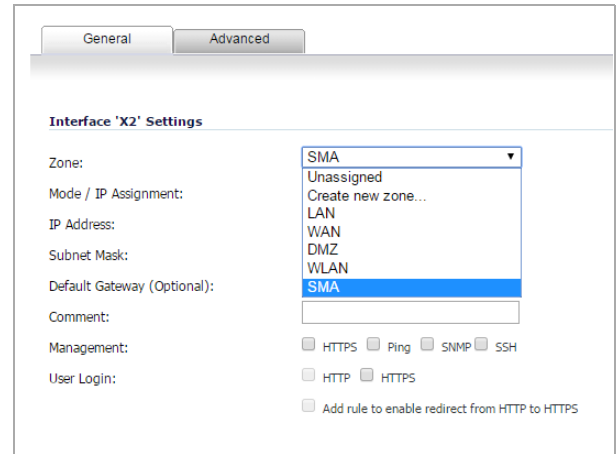
To ensure the SMA zone displays in the matrix view:

- In the administrative interface of your SonicWall appliance, navigate to the **Network > Interfaces** page.

- 2 Click the Configure icon for X2 or the port you assigned as the SMA zone.



- 3 Select **SMA** as the **Zone** from the drop-down list.



- 4 Click **OK**.

Safety and Regulatory Information

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

- [Safety and Regulatory Information](#) on page 56
- [Appliance Mounting Information](#) on page 56
- [Lithium Battery Warning](#) on page 57
- [Cable Connections](#) on page 57
- [Sicherheitsanweisungen](#) on page 57
- [Hinweis zur Lithiumbatterie](#) on page 59
- [Kabelverbindungen](#) on page 59
- [安全說明](#) on page 59
- [鋰電池警告](#) on page 60
- [纜線連結](#) on page 60
- [台灣 RoHS / 限用物質含有情況標示資訊](#) on page 61
- [Warranty Information](#) on page 62

Safety and Regulatory Information

Regulatory Model / Type	Product Name
1RK33-0BB	SMA 200
1RK33-0BC	SMA 400

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 mm².
- 15 The following statement applies only to rack-installed products that are GS-Marked: 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 200/400 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 200/400 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 other wiring that exits the building where the SonicWall appliance is located.

Sicherheitsanweisungen

Für eine ordnungsgemäße Montage sollten die folgenden Hinweise beachtet werden:

- 1 Das SonicWall Modell ist für eine Montage in einem standardmäßigen 19-Zoll-Rack konzipiert.

- 2 Vergewissern Sie sich, dass das Rack für dieses Gerät geeignet ist und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- 3 Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- 4 Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- 5 Achten Sie darauf, dass sich die Netzkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden.
- 6 Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- 7 Wenn das Gerät in einem geschlossenen 19"-Gehäuse oder mit mehreren anderen Geräten eingesetzt ist, wird die Temperatur in der Gehäuse höher sein als die Umgebungstemperatur. Achten Sie darauf, daß die Umgebungstemperatur nicht mehr als 40° C beträgt.
- 8 Bringen Sie die SonicWall waagrecht im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- 9 Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an. Wählen Sie einen Ort im 19-Zoll-Rack, wo alle vier Befestigungen der Montageschienen verwendet werden.
- 10 Ein angemessen dimensionierter und geprüfte Sicherung, sollte Bestandteil der Haus-Installation sein. Bitte folgen die den lokalen Richtlinien beim Einkauf von Material oder Komponenten.
- 11 Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts. Überlasten Sie nicht den Stromkreis.
- 12 Eine sichere Erdung der Geräte im Rack muss gewährleistet sein. Insbesondere muss auf nicht direkte Anschlüsse an Stromquellen geachtet werden wie z. B. bei Verwendung von Mehrfachsteckdosen.
- 13 Das im Lieferumfang enthaltenen bzw. Netzkabel sind nur für die Verwendung in bestimmten Ländern und

Regionen zugelassen. Überprüfen Sie bitte vor der Verwendung eines Netzkabels, ob es für die Verwendung in Ihrem Land oder Ihrer Region zugelassen ist und den geforderten Normen entspricht.

- 14 Mindest Stromkabel Bewertung für die Europäische Union (CE): Zertifizierte Netzkabel nicht leichter als leichte PVC-Schlauchkabel nach IEC 60227, Bezeichnung oder H05 VV-F oder H05 VVH2-F2 und bewertet für mindestens 3G 0,75 mm².
- 15 Der folgende Hinweis gilt nur für rackmontierte Produkte mit GS-Kennzeichen: Dieses Gerät ist nicht zur Verwendung an Arbeitsplätzen mit visuellen Anzeigegeräten gemäß § 2 der deutschen Verordnung für Arbeitsplätze mit visuellen Anzeigegeräten vorgesehen.

Hinweis zur Lithiumbatterie

Die in der SMA 200/400 Appliance von SonicWall verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die SonicWall in ein von SonicWall autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei

einer Entsorgung der Batterie oder der SonicWall SMA 200/400 Appliance die diesbezüglichen Anweisungen des Herstellers.

Kabelverbindungen

Alle Ethernet- und RS232-C-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWall keine Kabel an, die aus dem Gebäude in dem sich das Gerät befindet herausgeführt werden.

安全說明

需要滿足以下條件以進行正確安裝：

- 1 SonicWall 設備被設計成安裝在一個標準的 19 吋機架安裝櫃。需要滿足以下條件以進行正確安裝。
- 2 使用機架製造商推薦的裝載硬體，確認機架足夠裝置所需。
- 3 請確認裝置內不會滲入水分或過多的濕氣。
- 4 裝置週邊請保持通風，特別是裝置通風口側。建議裝置與牆壁間至少要有 1 英吋 (25.44 公釐) 的淨空。

- 5 纜線的路徑應遠離電源線、日光燈，以及會產生雜訊的來源，如無線電、發送器與寬頻放大器。
- 6 架設位置需遠離陽光直射與熱源。建議周圍溫度最高溫不要超過 104°F (40°C)。
- 7 如果是安裝於封閉式或多組機架配件，機架環境的周圍操作溫度可能會高過室內周遭。因此，在與上述建議之最高周圍溫度相容的環境中安裝設備時，應將此列入考量。
- 8 將 SonicWall 裝置平坦地裝設在機架中，如此才能避免因不均勻的機械負荷造成危險狀況。
- 9 必須使用四顆與機架設計相容的安裝螺釘，並用手鎖緊螺釘，確定安裝牢固。選擇一個安裝位置，將四個裝載洞孔對齊 19 吋架設機櫃的安裝桿。
- 10 應當提供一個合適額定值並且已被認可的分支電路斷路器作為安裝該裝置的一部分。在購買材料或部件時，應遵循當地安全代碼。
- 11 必須留心裝置與電源電路的連接問題，電路過載對過電流保護與電路電線的影響需降至最低。解決這個問題時，需正確考慮裝置銘牌額定值。不要過載電路。
- 12 必須維護可靠的機架裝載設備接地。必須特別留意電源供應器連線，而不是直接連接到電源板之類的分支電路。

- 13 隨附的電源線僅限於特定的國家或地區使用。使用前，請確認電源線的額定值且已被認可在你的地區上使用。

鋰電池警告

使用者不得自行更換 SonicWall 網際網路安全性裝置中使用的鋰電池。必須將 SonicWall 裝置送回 SonicWall 授權的服務中心，以更換相同的鋰電池或製造商推薦的同類型鋰電池。若因任何原因必須丟棄電池或 SonicWall 網際網路安全性裝置，請嚴格遵守電池製造商的指示。

纜線連結

所有乙太網路與 RS232 (主控台) 線路都是為與其他裝置進行內建連接所設計的。請不要將這些連接埠直接連接至通訊線路，或其他連出 SonicWall 裝置 所在建築的線路。

台灣 RoHS / 限用物質含有情況標示資訊

單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr ⁺⁶)	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
機箱 / 檔板 (Chassis/ Bracket)	-	0	0	0	0	0
機械部件 (風扇、散熱器 等) (Mechanical parts (fan, heatsink etc.)	-	0	0	0	0	0
電路板組件 (PCBA)	-	0	0	0	0	0
電線 / 連接器 (Cable/ connector)	-	0	0	0	0	0
電源設備 (power supply)	-	0	0	0	0	0
配件 (Accessories)	-	0	0	0	0	0
備考 1. “0” 係指該項限用物質之百分比含量未超出百分比含量基準值。						
備考 2. “-” 係指該項限用物質為排除項目。						

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://support.sonicwall.com/>.

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

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 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, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, 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.

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

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

The Support Portal enables you to:

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

To contact SonicWall Support, refer to <https://support.sonicwall.com/contact-support>.

SMA 200/400 Getting Started Guide
Updated - March 2017
232-003789-50 RevA



SONICWALL™