

SonicWall™ Secure Mobile Access 6200/7200

Getting Started Guide

Regulatory Model Numbers:

1RK31-0B0 – SMA 6200

1RK30-0AF – SMA 7200



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, 232-003431-52 Rev Af 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.

In this Guide

This *Getting Started Guide* provides instructions for basic installation and configuration of the SonicWall™ Secure Mobile Access 6200/7200 appliances.

For Quick Policy Setup Charts, refer to [Quick Policy Setup](#) on page 57.

Contents

Chapter 1

Sections included:

[In this Guide](#) on page 3

[Contents](#) on page 3

Chapter 2

Sections included:

[Introduction to the SMA 6200/7200](#) on page 7

[SMA 6200/7200 Package Contents](#) on page 8

[SMA 6200/7200 Front Panels](#) on page 10

[SMA 6200/7200 Back Panels](#) on page 11

Chapter 3

Sections included:

Preparing to Deploy the SMA 6200/7200 on page 13

Network Architecture on page 14

Preparing for the Installation on page 16

About Installation and Deployment on page 19

Chapter 4

Sections included:

Installation and Configuration on page 21

Connecting the Appliance on page 22

Starting the Appliance on page 22

Entering Network Settings Using the LCD on page 23

Running the Setup Wizard on page 23

Connecting to AMC on page 25

Configuring Basic WorkPlace Portal Access on page 26

Chapter 5

Sections included:

Registering and Obtaining a License on page 31

Using MySonicWall on page 32

Creating a MySonicWall account on page 32

Registering your Appliance on page 33

Downloading your License File on page 33

Importing your Licenses on page 34

Chapter 6

Sections included:

[Rack Mounting the Appliance](#) on page 37

[Attaching Inner Rails to the Appliance](#) on page 40

[Installing the Outer Rails](#) on page 40

[Installing the Appliance in the Rack](#) on page 42

[Removing the Appliance from the Rack](#) on page 42

Chapter 7

Sections included:

[Safety and Regulatory Information](#) on page 45

[Safety Instructions](#) on page 46

[Sicherheitsanweisungen](#) on page 48

[安全說明](#) on page 51

[Declaration of Conformity](#) on page 53

[Warranty Information](#) on page 53

[台灣 RoHS / 限用物質含有情況標示資訊](#) on page 54

For general support information, see [SonicWall Support](#) on page 55.

Introduction to the SMA 6200/7200

This section describes the items shipped with the SonicWall Secure Mobile Access 6200/7200 appliances and provides front and rear illustrations of the appliances.

- [SMA 6200/7200 Package Contents](#) on page 8
- [SMA 6200/7200 Front Panels](#) on page 10
- [SMA 6200/7200 Back Panels](#) on page 11

SMA 6200/7200 Package Contents

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

- 1 One SMA 6200 or SMA 7200 appliance
- 2 One rack mounting kit
- 3 One RJ45 to DB9 console cable
- 4 One Ethernet cable
- 5 One power cord for SMA 6200 or two power cords for SMA 7200*
- 6 One *SonicWall Secure Mobile Access 6200/7200 Getting Started Guide*

*The included power cord(s) 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. The power cords are for AC mains installation only. See [Safety and Regulatory Information](#) on page 45 for minimum power cord rating and additional safety information.

添付の電源コードに関して

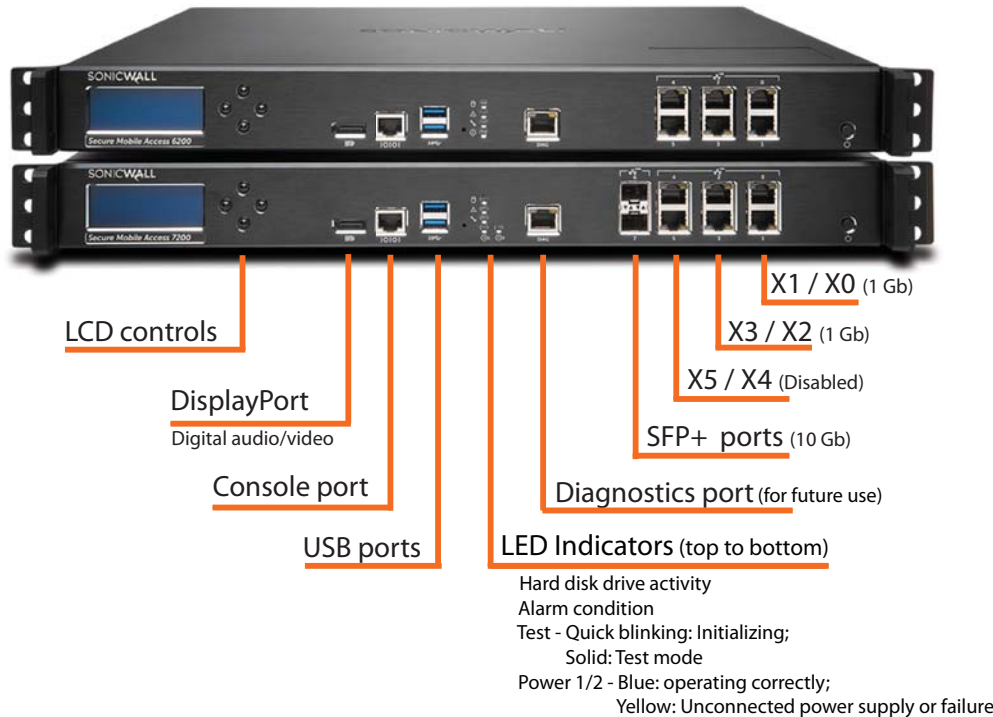
電気安全を確保するために、弊社製品にご使用いただく電源コードは必ず製品同梱の電源コードをご使用ください。この電源コードは他の製品では使用できません。

Package contents



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

SMA 6200/7200 Front Panels

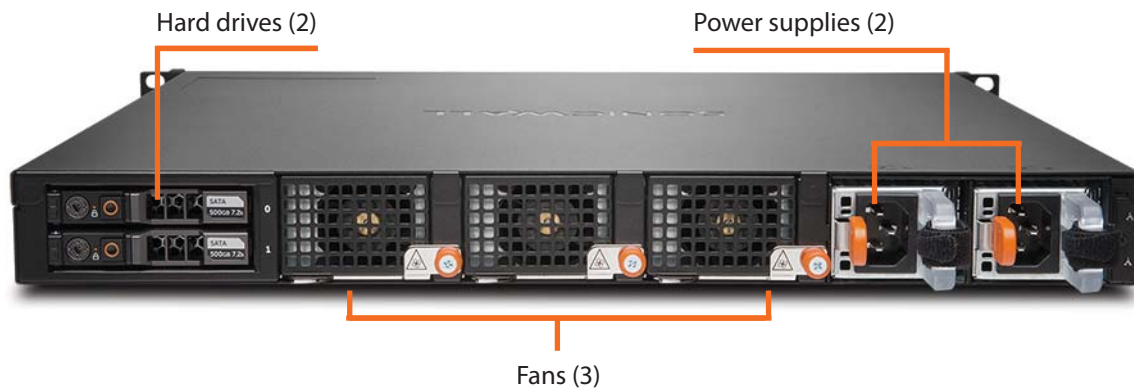


SMA 6200/7200 Back Panels

SMA 6200:



SMA 7200:



Preparing to Deploy the SMA 6200/7200

This section provides an overview of single-homed and dual-homed network architecture and discusses firewall settings and other information you need about components of your network to successfully deploy the SMA 6200/7200.

- [Network Architecture](#) on page 14
- [Preparing for the Installation](#) on page 16
- [About Installation and Deployment](#) on page 19

Network Architecture

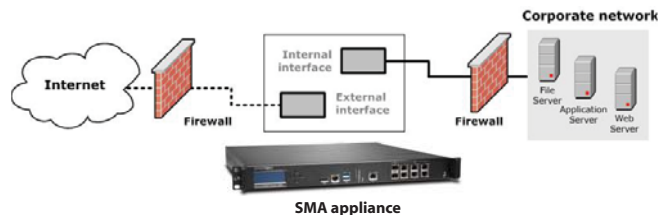
All SMA 6200/7200 appliances can be set up in either a dual interface or single interface configuration, also known as dual-homed and single-homed.

In either configuration, appliance management with AMC is accomplished by accessing the internal (X0) interface.

This guide steps you through a basic single-homed interface configuration. For the highest level of security and performance, SonicWall recommends a dual-homed configuration. Refer to the *Deployment Planning Guide* and *SMA Administration Guide* for further information.

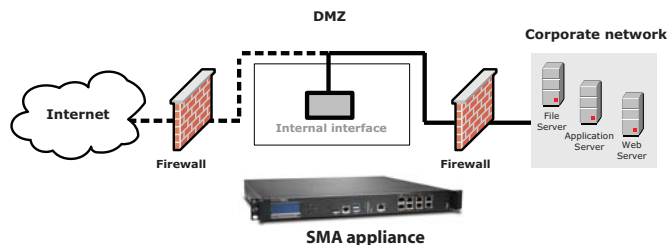
Dual-Homed Configuration (Internal and External Interfaces)

One network interface is used for external traffic (that is, to and from the Internet), and the other interface is used for internal traffic (to and from your corporate network).



Single-Homed Interface Configuration (Internal Interface)

A single network interface is used for both internal and external traffic. In this configuration, the appliance is usually installed in the demilitarized zone (or DMZ, also known as a perimeter network).



In both configurations, incoming requests to the SMA 6200/7200 services—including HTTP/S traffic for the Web proxy service—are sent over port 80 (HTTP) and port 443 (HTTPS). Traffic from the OnDemand agent is always sent over port 443. Because most networks are configured to enable traffic over these ports, you should not need to reconfigure firewalls on your network.

You should install the appliance in a location where it can connect to resources on your network, including:

- Application servers and file servers, including Web servers, client/server applications, and Windows file servers.
- External authentication repositories (such as an LDAP, Microsoft Active Directory, or RADIUS server).
- One or more Domain Name System (DNS) servers.
- Optionally, a Windows Internet Name Service (WINS) server. This is required for browsing Windows networks using WorkPlace.



CAUTION: The SMA 6200/7200 appliance does not provide full firewall capabilities and should be secured behind a firewall. Running without a firewall makes the appliance vulnerable to attacks that can compromise security and degrade performance.

Although not required, enabling the appliance to communicate with these additional resources provides greater functionality and ease of use:

- Network Time Protocol (NTP) server for synchronizing the time on the appliance.
- External server for storing syslog output.
- Administrator's workstation for secure shell (SSH) access.

You can configure the appliance to use a self-signed server certificate, or, for enhanced security, you can obtain a certificate from a commercial certificate authority (CA). For more information, refer to the *SMA Administration Guide*.

Preparing for the Installation

Before beginning the installation, you need to gather information about your networking environment and verify that your firewalls are properly configured to permit traffic to and from the appliance as explained in the following sections:

- [Gathering Information](#) on page 16
- [Verifying your Firewall Policies](#) on page 17

Gathering Information

Before configuring the appliance, you need to gather the following information. You are prompted for some of this information when running the Setup Wizard, but most of it will be used when you configure the appliance in the Appliance Management Console (AMC). Refer to the *SMA Administration Guide*.

Settings required to start Appliance Management Console

- The root password for administering the appliance
- The name for the appliance (because this name is used only in log files, you do not need to add it to DNS)
- The internal IP address and, optionally, an external IP address

- Select a routing mode and supply IP addresses for the network gateways to the Internet, and your corporate network.

Certificate information

Several pieces of information are used to generate the server and AMC certificates:

- A fully qualified domain name (FQDN) for the appliance and for any WorkPlace sites that use a unique name. These names should be added to your public DNS; they are also visible to users when they connect to Web-based resources.
- A FQDN for the Appliance Management Console (AMC) server. The AMC server name is used to access AMC, which is a Web-based tool for administering the appliance.

Name lookup information

- Internal DNS domain name of the network to which the appliance is connected
- Primary internal DNS server address (additional DNS servers are optional)
- IP address for an internal WINS server and the name of your Windows domain (required to browse files on a Windows network using WorkPlace, but are otherwise optional)

Authentication information

Server name and login information for your authentication servers (LDAP, Active Directory, or RADIUS)

Virtual Address pool information

If you are planning to deploy either network tunnel client (Connect Tunnel or OnDemand Tunnel), you must allocate IP addresses for one or more address pools. For more information, refer to the *SMA Administration Guide*.

Optional configuration information

- To enable SSH access from a remote machine, you need to know the remote host’s IP address.
- To synchronize with an NTP server, you need to know the IP addresses for one or more NTP servers.
- To send data to a syslog server, you need to know the IP address and port number for one or more syslog servers.

Verifying your Firewall Policies

For the appliance to function correctly, you must open ports on your external (Internet-facing) and internal firewalls.

External Firewall

For secure access to the appliance from a Web browser or OnDemand, you must make sure that ports 80 and 443 are open on firewalls at your site. Opening your firewall to permit SSH access is optional, but can be useful for performing administrative tasks from a remote system.

External Firewall

Traffic Type	Port/ protocol	Usage	Required?
ESP	4500/UDP	ESP Tunnel	Yes
HTTP	80/tcp	Unencrypted network access	Yes
HTTPS	443/tcp	Encrypted network access	Yes
SSH	22/tcp	Administrative access to the application	No

Internal Firewall

If you have a firewall on the internal network, you may need to adjust its policy to open ports for back-end applications with which the appliance must communicate. In addition to opening ports for standard network services such as DNS and email, you may need to modify your firewall policy before the appliance can access the following services.

Internal Firewall

Traffic Type	Port/protocol	Usage
Microsoft networking	138/tcp and 138/udp	Used by WorkPlace to perform WINS name resolution, browse requests, and access file shares
	137/tcp and 137/udp	
	139/udp	
	162/snmp	
	445/smb	
LDAP (unencrypted)	389/tcp	Communicate with an LDAP directory or Microsoft Active Directory

Internal Firewall

Traffic Type	Port/protocol	Usage
LDAP over SSL (encrypted)	636/tcp	Communicate with an LDAP directory or Microsoft Active Directory over SSL
RADIUS	1645/udp or 1812/udp	Communicate with a RADIUS authentication server
NTP	123/udp	Synchronize the appliance clock with an NTP server
Syslog	514/tcp	Send system log information to a syslog server
SNMP	161/udp	Monitor the appliance from an SNMP management tool

About Installation and Deployment

This section outlines the process of installing, configuring, and testing the appliance, and then deploying it in a production environment. The [Installation and Deployment Process](#) table provides an overview of the steps.

Installation and Deployment Process

Installation Step	Description
Make a note of your appliance serial number and authentication code.	You'll need this information when you register your product on MySonicWall. The serial number and authentication code are printed on your appliance label; they are also displayed on the General Settings page in AMC.
Rack-mount the appliance and connect the cables.	See Rack Mounting the Appliance on page 37 and Connecting the Appliance on page 22.

Installation and Deployment Process

Installation Step	Description
Turn on the appliance and begin configuration.	To connect to your appliance on your internal network you must specify an internal IP address and the subnet mask. Use the controls on the front of the appliance. See Entering Network Settings Using the LCD on page 23.
Run Setup Wizard.	The wizard guides you through the process of initial setup for your SMA appliance. See Running the Setup Wizard on page 23.
Register your appliance on MySonicWall.	Register your appliance on MySonicWall. Product registration gives you access to essential resources, such as your license file and updates. To register, you need both the serial number for your appliance and its authentication code.

Installation and Configuration

This section provides the steps to perform the initial installation and settings configuration of the SonicWall Secure Mobile Access 6200/7200. For more detailed information, the *SMA Administration Guide* has complete instructions for installing your SMA 6200/7200 appliance.

- [Connecting the Appliance](#) on page 22
- [Starting the Appliance](#) on page 22
- [Entering Network Settings Using the LCD](#) on page 23
- [Running the Setup Wizard](#) on page 23
- [Connecting to AMC](#) on page 25
- [Configuring Basic WorkPlace Portal Access](#) on page 26

Connecting the Appliance

Use the following instructions to connect the appliance to your network.

For a diagram of the appliance, refer to [SMA 6200/7200 Front Panels](#) on page 10.

For rack mounting instructions, refer to [Rack Mounting the Appliance](#) on page 37.

To connect the SMA6200/7200 appliance:

- 1 Connect a network cable from your internal network to the internal interface on the appliance (X0).
- 2 Optionally, connect a cable from your external network to the external interface on the appliance (X1).

Starting the Appliance

The SMA 6200 contains a single AC power supply and comes with a single power cord. The SMA 7200 includes dual power supplies for redundant AC power and added reliability. Two power cords are included with the SMA 7200 appliance. Refer to [Safety and Regulatory Information](#) on page 45 for information.

The included power cord(s) 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.

To connect the power of the SMA 6200, plug in the power cord to the power supply socket on the back of the appliance, and then connect the cord to an AC outlet.

For the SMA 7200, plug the power cords to the power supply sockets on the appliance back and then connect the cords to AC outlets. For best reliability, connect the two cords of the SMA 7200 to outlets on different circuits.

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☑且已被認可在你的地區上使用。



CAUTION: Remove any USB devices from the appliance before you reboot it. If a USB device is plugged in to your appliance when it is rebooted, the appliance tries to use it as a boot device. As a result, the boot information stored in the BIOS on the appliance is overwritten, and the device becomes unusable.

Entering Network Settings Using the LCD

Before you can run the Setup Wizard, you must first enter basic network settings so that you can use a Web browser to connect to the appliance. The LCD screen on the front bezel is used for this part of the initial configuration.

To the right of the LCD screen on the front of your appliance are four buttons used to enter your settings.

To configure settings using the LCD controls:

- 1 Press Up and Down to read the welcome screen, and press Right to continue past it.

NOTE: SMA 7200 only: select either a 1GB or a 10 GB port.

- 2 Enter the IP address for your internal interface.

The default internal (X0) IP address is 192.168.0.10. To change the IP address, use the Left and Right buttons to position your cursor over the number you want to change, and then use Up and Down to change the number. Press Right to continue to the next screen.

- 3 Enter your subnet mask.

The default subnet mask is 255.255.255.0. To change the subnet mask, use the buttons as described in the previous step. Press Right to continue to the next screen.

- 4 Review your settings and apply them, then wait until the LCD screen displays *Setup is complete*.

Running the Setup Wizard

After the LCD configuration steps, the Setup Wizard continues the initial setup for your SMA 6200/7200 appliance.

To run the Setup Wizard:

- 1 Configure your management computer with a static IP address on the same subnet as your internal (X0) interface. If you kept the default X0 IP address, set your computer to an IP address on the 192.168.0.0/24 subnet, such as 192.168.0.20, and set the subnet mask to 255.255.255.0 and the default gateway to 192.168.0.1.
- 2 Using an Ethernet cable, connect the appliance X0 interface to your management computer.
- 3 Access the wizard by starting a Web browser and typing: `https://<IP address>:8443` where

<IP address> matches the address you defined for the internal network interface. The default X0 IP address is 192.168.0.10.

i | **NOTE:** Accept the certificate warning and continue.

- 4 Follow the instructions in the wizard to enter your configuration settings:
 - a Accept the license agreement.
 - b Create an administrator password of at least 8 characters.
 - c Configure the time zone.
 - d Enter a name for the appliance without spaces or underbars.
 - e Configure settings for either dual interfaces or a single interface.
 - f For routing, configure the internal (X0) gateway IP address and optionally select dual gateway and set the external (X1) gateway IP address. The default internal gateway address is 192.168.0.1.
 - g For name resolution, enter the default domain for your network.

- h Enter user access settings and an initial access policy for users, which you can refine later in AMC. Select **Allow authenticated users access to all defined resources**. (This automatically allows users access and is the least secure, but can always be changed later when more security is needed. For the most secure, select **Initially deny all access**.)

- 5 When ready, click **Finish** to apply your settings. The appliance restarts, which causes you to lose your current connection. Wait a few minutes and then point your browser to the X0 IP address and port 8443 to connect to the Appliance Management Console (AMC). For example:

`https://<IP address>:8443`

Connecting to AMC

AMC is the Web-based application used to administer the appliance.

NOTE: Appliance management with AMC is accomplished by accessing the internal interface. The appliance cannot be managed by a direct connection to the external interface.

To access the login page after the Setup Wizard finishes, point your browser to `https://<IP address>:8443`, where `<IP address>` matches the address you defined for the internal network interface. The default X0 IP address is 192.168.0.10.

AMC login screen

The screenshot shows the SonicWall Secure Mobile Access Management Console login interface. At the top, the SonicWall logo is followed by "Secure Mobile Access" and "Management Console". Below this, the text "Please log in" is centered. There are three input fields: "Username:" with a text box, "Password:" with a text box, and "Log in using:" with a dropdown menu showing "Management Console" and a downward arrow. At the bottom, there are two buttons: "Login" and "Clear".

SONICWALL™ Secure Mobile Access | Management Console

Please log in

Username:

Password:

Log in using: ▼

Login Clear

Type **admin** in the **Username** field, and then enter the password you created with the Setup Wizard. Both are case-sensitive. For **Log in using**, select the **Management Console** realm. Click **Login** to log into the Management Console.

Configuring Basic WorkPlace Portal Access

For access from the WAN, you need an authentication server, a realm, a user, and an access rule.

This section describes how to configure a local authentication server and user on the appliance itself, and create a realm and access rule to go with them. This allows you to quickly create a portal while gathering the information needed for a full production deployment.

This same sequence of steps also applies if you are configuring an external authentication server and more advanced settings for your realm or access rules.

Creating a Local Authentication Server

To create a local authentication server:

- 1 In AMC, navigate to the **System Configuration > Authentication Servers** page.
- 2 In the **Authentication servers** section, click **New**.
- 3 In the **User Store** section, under **Local user storage**, select the **Local users** radio button.

- 4 Click **Continue**.
- 5 In the **Name** field, type in a name for the local authentication server.
- 6 Click **Save**.

Creating a Basic Realm

A realm references an authentication server and determines which access agents are provisioned to your users and what end point control restrictions are imposed.

To create a basic realm that uses your local authentication server:

- 1 Navigate to the **User Access > Realms** page.
- 2 Select **click here**.
- 3 Click **New realm** on the Realms page.
- 4 In the **Name** field, type in a name for the realm.
- 5 In the **Authentication server** drop-down list, select the local authentication server you just configured.
- 6 Click **Finish**.

The Realms page displays your new realm and shows it as associated with your local authentication server.

Creating a Local User

To create a local user:

- 1 Navigate to the **Security Administration > Users & Groups** page.
- 2 Click the **Local Accounts** tab.
- 3 Click **New** and select **User**.
- 4 In the **Username** field, type in a name for the local user.
- 5 In the **Password** field, type in a password for the local user.
- 6 Clear the **User must change password at next login** checkbox.
- 7 Click **Save**.

Configuring the Default WorkPlace Site

To configure the Default WorkPlace Site:

- 1 Navigate to the **User Access > WorkPlace** page and click on the **WorkPlace Sites** tab.
- 2 Click **Default**.
- 3 In the **Custom FQDN** field, type in the configured internal or external IP address of the appliance.

This field should match the IP address or hostname of the appliance as the user would access it.

WorkPlace Sites > Configure WorkPlace Site

General Advanced

Name this WorkPlace site and assign a domain name (which determines the URL used to access WorkPlace).

Name:* Description:

Default Default WorkPlace site

Fully qualified domain name

Specify the host and domain name used to access this WorkPlace site.

Custom FQDN:*

172.24.25.209

Login page appearance

Select a style that has the logo, color scheme, and text you want for the WorkPlace login page. You can also modify an existing style, or create a new one. The style and layout for other WorkPlace portal pages is specified during community configuration.

Style: Default Style New Modify ID: DefaultWorkplaceTheme

Save Cancel

- 4 Click **Save**.

Configuring an Access Rule

The SMA 6200/7200 appliance uses a granular access policy to determine what backend resources a given user is allowed to access.

To configure a default access rule to allow any user to access resources through the appliance:

- 1 Navigate to the **Security Administration > Access Control** page.
- 2 Click **New**.
- 3 Optionally type in a **Description**.
- 4 Click **Finish**.

Applying the Pending Changes

To apply all your changes:

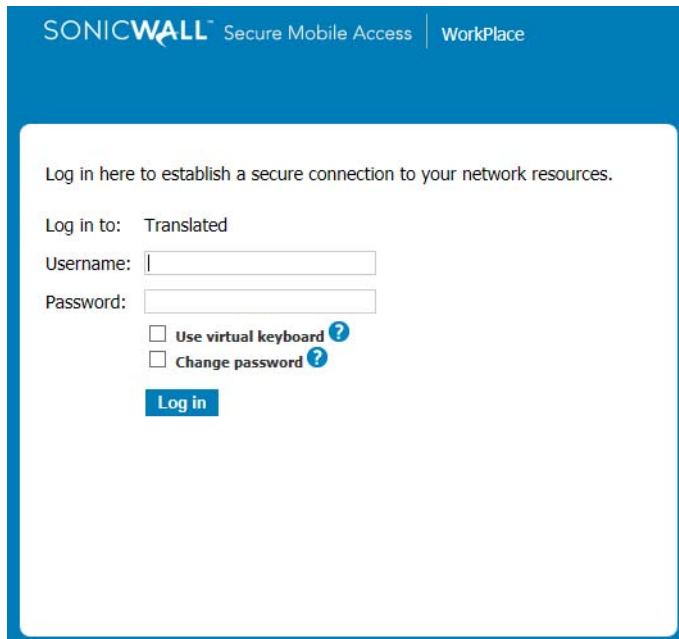
- 1 Click **Pending changes** at the top right corner of the page.
- 2 In the pop-up dialog box, click **Apply changes**.

Logging into the WorkPlace Portal

After the appliance finishes applying the changes, you can log into the WorkPlace portal using the local user credentials.

To log in as the local user:

- 1 Point your browser to `https://<IP address>` where `<IP address>` matches the address you defined for the internal or external network interface. The default internal IP address is 192.168.0.10.



The screenshot shows the SonicWall Secure Mobile Access WorkPlace login interface. At the top, the header reads "SONICWALL™ Secure Mobile Access | WorkPlace". Below the header, a message states: "Log in here to establish a secure connection to your network resources." The login section is titled "Log in to: Translated". It contains two input fields: "Username:" and "Password:". Below the password field, there are two checkboxes: "Use virtual keyboard" and "Change password", each followed by a question mark icon. At the bottom of the login section is a blue "Log in" button.

- 2 In the portal login screen, enter the username and password for the local user.
- 3 Click **Login**.

Registering and Obtaining a License

This section describes how to register your SonicWall Secure Mobile Access 6200/7200 and then download the license file from MySonicWall.

You can register your SMA 6200/7200 appliance before or after you initialize or deploy it. Registration provides access to essential resources, such as your license file, firmware updates, documentation, and technical support information.

- [Using MySonicWall](#) on page 32
- [Creating a MySonicWall account](#) on page 32
- [Registering your Appliance](#) on page 33
- [Downloading your License File](#) on page 33
- [Importing your Licenses](#) on page 34

Using MySonicWall

SonicWall requires a MySonicWall account prior to configuring your appliance. If you already have a MySonicWall account, you can continue to the [Registering your Appliance](#) on page 33.

MySonicWall is used during registration of your SonicWall appliance and to activate or purchase licenses for security services, support, or software specific to your SonicWall device.

MySonicWall registration information is not sold or shared with any other company.

Creating a MySonicWall account

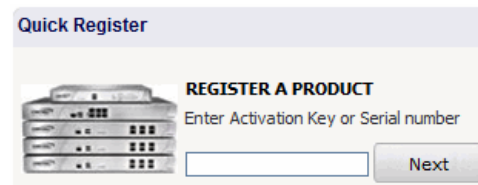
A MySonicWall account is required in order to register the appliance.

To create a MySonicWall account from any computer:

- 1 In your Web browser, navigate to <https://www.mysonicwall.com>.

The image shows a screenshot of the MySonicWall login interface. At the top, it says "SONICWALL | MySonicWall" with a question mark icon in the top right corner. Below this is a login form with the label "Username/Email" and a text input field containing "Username/Email". To the right of the input field is a link that says "Forgot?". Below the input field is a "Next" button. Underneath the button, it says "Not a registered user? Register Now". At the bottom of the form area, there are several links: "Privacy Policy", "Conditions for use", "Feedback", "Live Demo", "SonicALERT", "Document Library", and "Report Issues". The footer of the page is dark blue and contains the text "Version: 12.5", "©2017 SonicWall", and "S1MSW07". At the very bottom, there are three circular icons for Android, Apple, and Windows.

- 2 In the login screen, click the **Register Now** link.
- 3 Complete the Registration form, and then click **Register**.
- 4 Verify that the information is correct, and then click **Submit**.
- 5 To confirm your account was created, click **Continue**.
- 3 Enter the appliance serial number into the **Register A Product** field and then click **Next**.



- 4 Enter a friendly name for this appliance.
- 5 Click **Register** to continue, and follow the online prompts to fill out the survey and complete the registration process.

Continue with the next section to download the appliance license file from MySonicWall.

Registering your Appliance

To register your appliance on MySonicWall:

- 1 Locate your appliance serial number and authentication code, which is printed on your appliance label. The serial number and authentication code are also displayed in the AMC on the General Settings page once you initialize and connect to your appliance.
- 2 In your Web browser, navigate to <https://www.mysonicwall.com> and log in to your MySonicWall account with your username and password.

Downloading your License File

You can download an initial user license from MySonicWall that is valid for one user (the administrator plus one end user) for an unlimited number of days. You can use this limited license until ready to deploy the appliance to production with full licensing.

To become familiar with the AMC and test it in your environment with additional users, request a lab license.

To retrieve the license file for your appliance, perform the following steps:

- 1 In your Web browser, go to <https://www.mysonicwall.com> and log in with your username and password.
- 2 Click **My Products** to view the list of your registered appliances.
- 3 Click the link for the appliance that requires a license.
- 4 On the Service Management page, click the **Click here for the License File** link.
- 5 In the View License dialog box, select **10.5 or later (Base)** in the drop-down list, and then click the **Click here for the License File** link.
- 6 Select the option to save the license file, or copy the license text to your clipboard and save it as an XML file (.xml) on your computer. You must import this license file using AMC.

Importing your Licenses

The SMA appliance uses a few different types of licenses. All license files must be retrieved from <https://mysonicwall.com> and imported to the appliance, as follows:

- Administration test license: To begin setting up your SMA appliance, log in to MySonicWall to retrieve your initial user license, which is valid for one user (the administrator plus one end user) for an unlimited number of days. To become familiar with the AMC and test it in your environment with additional users, either retrieve an appliance license, or request a lab license to add a few more users.
- Appliance licenses: The number of concurrent users supported with the appliance license varies, depending on the appliance model you have:
 - SMA 7200: up to 10,000 users
 - SMA 6200: up to 2,000 users
- Component licenses: If the license for an appliance component (such as OnDemand) has expired, users attempting to use that component see an error message in WorkPlace. In the case of a Spike License, the date on which it was activated and how many days still remain is displayed in AMC.

- If a license is about to expire, the AMC displays a license warning message in the status area that links to the Licensing page.

When you are ready to move the appliance into production after initial setup and testing, download your appliance license file from MySonicWall and then use the AMC to import it to the appliance. The process for importing an appliance license file is described in detail in the online help for the AMC.

To import an appliance license:

- 1 Log in as admin to the AMC.
- 2 Click **General Settings**.
- 3 Click the **Edit** link in the Licensing area. The Manage Licenses page appears.
- 4 Click **Import License**.
- 5 In the License file box, click **Browse** to locate the license file you retrieved from your MySonicWall account, and double-click on it.
- 6 Click **Upload** to copy the license to the appliance.

- 7 Apply the change by clicking the **Pending changes** link in the upper-right corner and then clicking **Apply changes**.

i **NOTE:** When you upload a Spike License, the countdown of the number of days it is valid begins once you activate it and apply the pending change in the AMC. Do not click the **Activate** link until you are ready to start using it.

Rack Mounting the Appliance

This section provides instructions and illustrations for rack mounting the SonicWall Secure Mobile Access 6200/7200.

The SMA 6200/7200 appliance is designed to be mounted in a standard 19-inch rack. The product packaging contains a slide rail kit for mounting the appliance in a four-post cabinet. Before installing the appliance in an equipment rack, the rails must be attached to the appliance and to the rack posts.

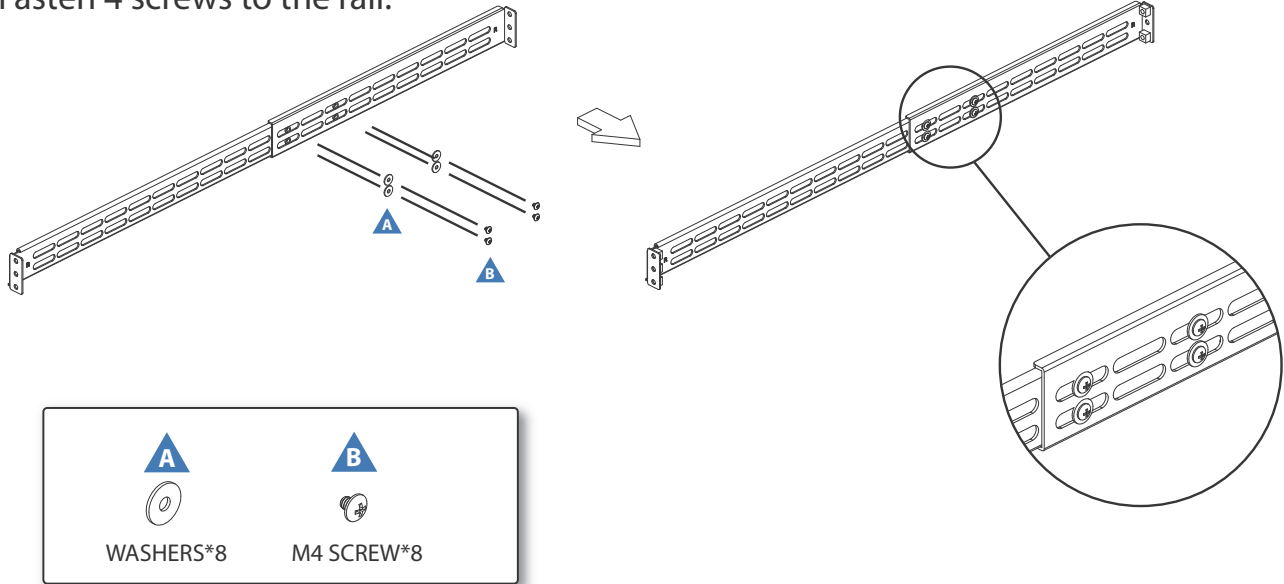
You will need the following tools and hardware for installation:

- Phillips (cross head) screwdriver (#1 bit and #2 bit)
- Anti-static wrist strap and conductive foam pad (recommended)
- Two outer rails
- Four inner rails
- Crosshead threaded screws

 **CAUTION:** Do not use slide/rail mounted equipment as a shelf or a work space.

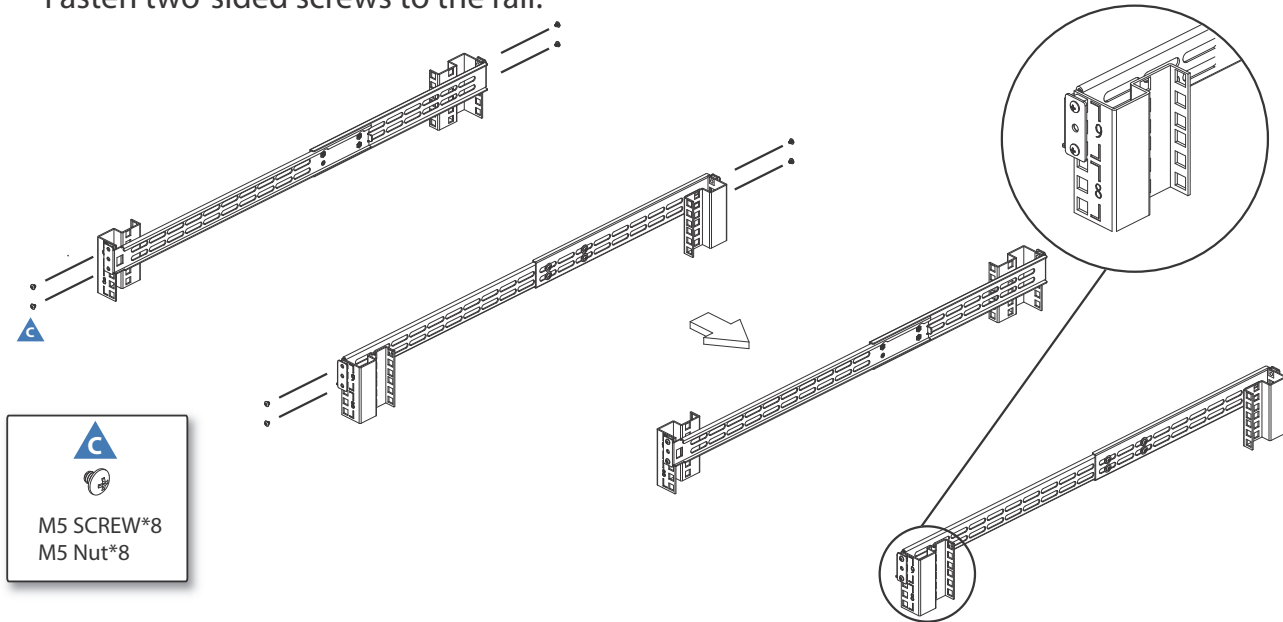
Assemble the Slide Rail

Fasten 4 screws to the rail.



Assemble the Slide Rail

Fasten two-sided screws to the rail.



Attaching Inner Rails to the Appliance

To attach the inner rails to the appliance:

- 1 Position the inner rail alongside the side of the appliance with the finger tab facing outward.
- 2 Align the screw holes of the rail and the mounting holes of the appliance and then attach the inner rail to the appliance with crosshead threaded screws.
- 3 Repeat the above steps to attach another rail on the same side of the appliance.
- 4 Attach the front bracket to the system.
- 5 Repeat to attach the other inner rails and front bracket to the other side of the appliance.

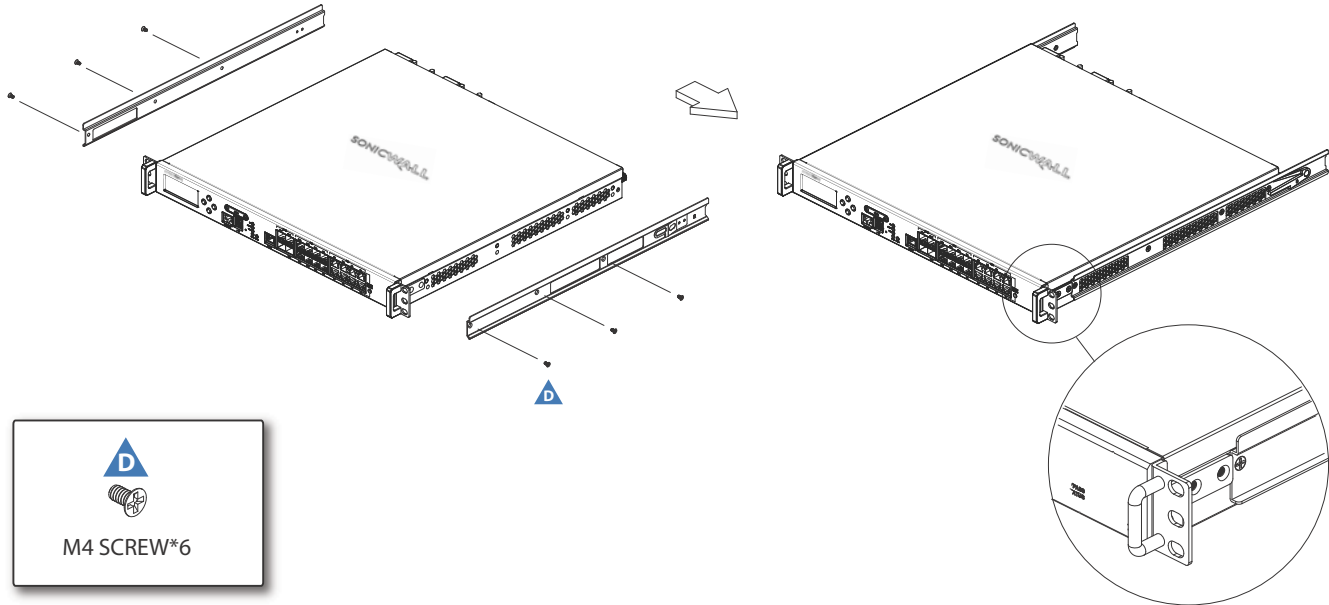
Installing the Outer Rails

To install the outer rail:

- 1 Attach the rail to the posts of the rack by using three rack screws.
- 2 Extend the outer back rail to the back of the rack and firmly attach it with two rack screws.
- 3 Repeat step 1 and 2 to install the other rail.

Assemble Inner Rail to Chassis

Fasten 6 screws to attach the inner channel onto the chassis.



Installing the Appliance in the Rack

- 1 Holding the appliance with its front facing you, lift it and carefully insert the inner rail into the outer rail.
- 2 Push the appliance all the way in until the front brackets contact the rack.
- 3 Optionally attach the front brackets to the rack.

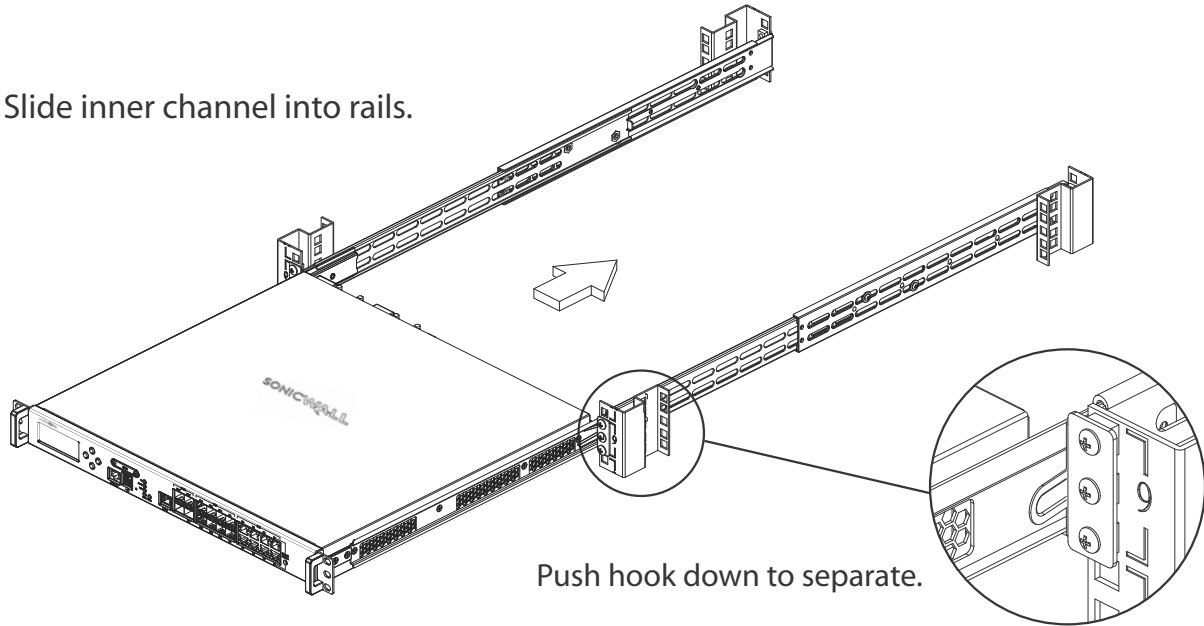
Removing the Appliance from the Rack

- 1 Pull the appliance half way out to the lock position.
- 2 Press the rail lock release tabs on both sides while pulling the appliance towards you until past the tabs.

Continue to pull the appliance until it is fully removed from the outer rails.

Insert Chassis to Frame

Slide inner channel into rails.



Safety and Regulatory Information

This section provides safety and regulatory information.

Regulatory Model/Type	Product Name
1RK31-0B0	SMA 6200
1RK30-0AF	SMA 7200

- [Safety Instructions](#) on page 46
- [Sicherheitsanweisungen](#) on page 48
- [安全說明](#) on page 51
- [Declaration of Conformity](#) on page 53
- [Warranty Information](#) on page 53
- [台灣 RoHS / 限用物質含有情況標示資訊](#) on page 54

Safety Instructions

- [Installation Requirements](#) on page 46
- [Lithium Battery Warning](#) on page 48
- [Cable Connections](#) on page 48

Installation Requirements

WARNING:

The following conditions are required for proper installation:

- 1 The SonicWall SMA 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 application.
- 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 (26mm) 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 appliances 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 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.
- 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.
- 16 This product is not intended to be installed and used in a home or public area accessible to the general

population. When installed in schools, this equipment must be installed in a secure location accessible only by trained personnel.

- 17 Thumbscrews should be tightened with a tool after both installation and subsequent access to the rear of the product.
- 18 Before replacing the fan unit, carefully read and follow the instructions provided with the unit.



Warning of Potential Hazard from Fan

- 19 When using a Fiber Optic Small-Form Pluggable (SFP) module, ensure it is IEC 60825 certified.

For SMA 7200 only:

- 1 As shipped from the factory this SonicWall product includes two power supplies for redundant AC power and added reliability.
- 2 To disconnect AC power, both power cords must be removed.

- 3 Never remove or install a power supply with the AC power cord attached to the power supply being removed or installed.

Lithium Battery Warning

The Lithium Battery used in the SonicWall SMA Internet security 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 Internet security 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 SMA is located.

Sicherheitsanweisungen

- [Anforderungen an die Installation](#) on page 48
- [Hinweis zur Lithiumbatterie](#) on page 50
- [Kabelverbindungen](#) on page 51

Anforderungen an die Installation

Verwarnung:

Für eine ordnungsgemäße Montage sollten die folgenden Hinweise beachtet werden:

- 1 Das SonicWall SMA 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, das 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 SMA 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 Sie 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 enthaltene bzw. die im Lieferumfang enthaltenen 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.
- 16 Dieses Produkt ist nicht dafür entwickelt, um in Bereichen mit öffentlichem Zugang betrieben zu werden. Wenn es in Schulen betrieben wird, stellen Sie sicher, dass das Gerät in einem abgeschlossenen Raum installiert wird, der nur von speziell ausgebildetem Personal betreten werden kann.
- 17 Vergewissern Sie sich, dass die Schrauben nach dem Austausch mit entsprechendem Werkzeug fest angezogen werden.
- 18 Lesen Sie vor dem Austausch der Lüftereinheit die Anleitung, die mit dem Gerät geliefert wurde und befolgen Sie die Anweisungen.



**Achtung—Lüfter Potentielle
Gefahrenquelle**

- 19 Bei der Verwendung von Lichtwellenleiter-Small-Form Pluggable (SFP) Modul zu gewährleisten, ist IEC 60825 zertifiziert.

Nur für SMA 7200:

- 1 Dieses Produkt wird mit zwei Wechselstrom-Netzteilen zur redundanten Stromversorgung fuer erhöhte Verfügbarkeit ausgeliefert.
- 2 Um den Wechselstrom (AC) zu unterbrechen muessen beide Stromkabel entfernt werden.
- 3 Wenn Sie das Netzteil wechseln, entfernen Sie unbedingt die Stromversorgung von dem zu wechselnden Netzteil.

Hinweis zur Lithiumbatterie

Die in der Internet Security 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 Internet Security 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

- [安裝要求](#) on page 51
- [鋰電池警告](#) on page 52
- [纜線連結](#) on page 52

安裝要求

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。
- 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 (26 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。
- 14 本產品的設計目的不是安裝並使用於住家或一般大眾可接觸到的公共區域。如果是安裝在學校，本設備只能安裝在受訓人員能接觸到的安全位置。
- 15 當安裝及後續接觸產品背面之後，必須用工具將指旋螺釘鎖緊。
- 16 更換風扇部件前，請仔細閱讀，並遵循所提供的指示。



風扇潛在危險警告

- 17 當使用光纖小型可插拔（SFP）模塊，確保它是 IEC60825 認證。

僅適用於 SMA 7200:

- 1 從工廠運出時，這個 SonicWall 產品包括為後備交流電源和增加可靠性而附帶的兩個電源。
- 2 要斷開交流電源，兩條電源線都必須被拔除。
- 3 切勿在交流電源線還連接著電源時移除或安裝電源。

鋰電池警告

使用者不得自行更換 SMA 網際網路安全性裝置中使用的鋰電池。必須將 SMA 送回 SMA 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 SMA 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 SMA 所在建築的線路。

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>



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

Warranty Information

All SonicWall appliances come with a 1-year Limited Hardware Warranty which provides delivery of critical replacement parts for defective parts under warranty. Visit the Warranty Information page details on your product’s warranty:

<https://support.sonicwall.com>

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
儲存裝置 (硬碟等) (Storage (Hard Disk, etc.)	-	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。						

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>.

Quick Policy Setup

Admission Control	How do you define trust level for user?	How are users authenticated?	<div>Authentication server AD.example.com</div> <div></div> <div>Realm Company XYZ</div>		A realm allows users to authenticate using credentials stored on an external authentication server.
		Who is authenticating?	<div><div>Employee's Community Group = "Marketing/Finance/Sales"</div><div>Partner's Community Group = "Partners"</div></div>		Communities allow you to group realm members based on different security needs as well as what access agents the user will use to interact with the network.
	How do you define trust level for device?	What WorkPlace Site will the users access?	<div><div>Employee Portal Corporate layout, Corporate Style</div><div>Partner Portal Corporate layout, Partner Style</div></div>		WorkPlace sites determine what Web-based interface the user will interact with.
		What zones are available for each community?	<div><div>Zones enabled for employee community</div><div>Devices that don't fall into the first three zones will automatically be assigned to the quarantine zone.</div></div> <div><div>Zones enabled for partner community</div><div>Partner devices that don't match the first two zones will automatically be assigned to the quarantine zone.</div></div>		Security zones are used to allow or deny access to members of each community.
Access Control	How do you define what resources individual users can access?	<div><div>Access Control Rule Inventory Applications</div><div>Device trust: </div><div>User trust: Finance and Sales</div></div> <div><div>Access Control Rule Outlook Web Access</div><div>Device trust: </div><div>User trust: Marketing, Finance and Sales</div></div> <div><div>Access Control Rule Order Entry Application</div><div>Device trust: </div><div>User trust: Partners, Sales</div></div>			Access control rules define which resources can be accessed by which users, when, and in which zones.
Define Policy	How do you define zones and trust levels?	<div>Define trust levels</div> <div>Allow access —</div> <div> Trusted: all access to all resources; could use device profiles 1 and 2.</div> <div> Semi-trusted: allow limited access to resources; could use device profiles 3 and 4.</div> <div> Deny access —</div> <div>Not trusted: deny access to resources; could use device profile 5.</div> <div>Quarantine —</div> <div>Suspends access until user completes remediation steps needed to match device profiles.</div>			Lets you allow, quarantine, or deny access based on matching device profiles and optionally require data protection.
	How do you define device profiles?	<div>Device Profile Examples</div> <div>IT-issued laptop —</div> <div> Running McAfee® AntiVirus Corporate Edition with current updates and scanned within the last 14 days, member of the company domain, encrypted text file named "itlaptop.txt".</div> <div>IT-issued mobile device —</div> <div> Device watermarked with a company-issued user certificate, encrypted text file named "itpocketpc.txt".</div> <div> Home Macintosh —</div> <div> Running either McAfee or Kaspersky® anti-virus program.</div> <div> Home PC —</div> <div> Running a McAfee, Symantec® or Kaspersky anti-virus program, running either McAfee or Kaspersky spyware program, and running Microsoft® Windows® Firewall.</div> <div> Running Google® Desktop Search — Deny access.</div>			Device profiles enable you to identify and determine the integrity of access devices based on device attributes—such as registry keys, processes running, or anti-virus state—and associate devices to Allow and Deny Zones. You can create as many device profiles as necessary.

This setup guide assumes that basic network configuration has been completed. If you used the Setup Wizard for your initial evaluation, you can modify the access control policy you have already created, or use this quick setup guide as an introduction to the SonicWall Appliance Management Console (AMC).

Reference

See these sections in the *SonicWall SMA Deployment Planning Guide*.

Admission Control	Define trust level for user	How are users authenticated?	1. Select Realms from the main AMC navigation menu. <ul style="list-style-type: none"> • Create a new realm (or modify the realm created with the Setup Wizard). • Select a new authentication server to specify a directory for user information and how users will authenticate. 	• Establishing an Authentication Realm
		Who is authenticating?	2. Create a new community for your employees from within the Configure Realm page. <ul style="list-style-type: none"> • Add your employee users and groups to your community (you can set this broadly to all employees now, and then further refine your users and groups later). 	• Creating an Employee Community
	How do you define trust level for device?	What access methods are available?	3. Select access methods for your Employee's Community in the Access methods section of the Configure Community page. <ul style="list-style-type: none"> • Select the network tunnel client option. • Configure Smart tunnel access and specify an IP address pool (for a quick evaluation, start with the Translated address pool option). 	• Specifying Access Methods for the 'Employees' Community
		What zones are available for each community?	4. Select the zones available for this community in the End Point Control section in the main AMC navigation menu. <ul style="list-style-type: none"> • Create one or more standard zones to set conditions for when users will be allowed access to the SMA appliance based on device identity and integrity. • Define one or more device profiles that will define the types of devices classified against your standard zone (for a quick evaluation, select a built-in anti-virus profile that matches your corporate A/V standard). • Create a quarantine zone to serve as the fallback for those who do not match the conditions you set in your standard zones. • Set your quarantine zone as a fallback by modifying the community you created above in the End Point Control restrictions section. 	• End Point Control for the 'Employees' Community
Access Control	How do you define what resources individual users can access?	5. Define resources that will be made available via the SMA appliance. Select Resources from the AMC navigation menu. <ul style="list-style-type: none"> • Define open access by specifying a domain, host or IP range resource. • Define narrow access by specifying a URL- or file-based resource (to display links on the Workplace portal, enable the shortcut check box). 	6. Define Access Control rules. Select Access Control from the AMC navigation menu. <ul style="list-style-type: none"> • Select New and then specify a community, user, or group that will have access. • Select the resource you want users to access. • <i>Optional:</i> To place a zone restriction on the resource, associate the rule with a zone defined in step 4. 	• Adding Resources • Access Control Lists

SMA 6200/7200 Getting Started Guide
Updated - June 2017
232-003431-52 Rev A

