SonicWall™ SuperMassive™ 9200/9400/9600

Getting Started Guide

Regulatory Model Numbers:

1RK28-0A6 – SuperMassive 9200
1RK28-0A7 – SuperMassive 9400
1RK28-0A8 – SuperMassive 9600

SONICWALL™

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.

SuperMassive Getting Started Guide
Updated - February 2017
232-000344-50 Rev A

1

In this Guide

This *SonicWall™ SuperMassive™ 9200/9400/9600 Getting Started Guide* provides instructions for basic installation and configuration of SonicWall SuperMassive appliances in single-unit or High Availability deployments.

- Contents on page 4
- Using this Getting Started Guide on page 7

These SonicWall SuperMassive appliances support:

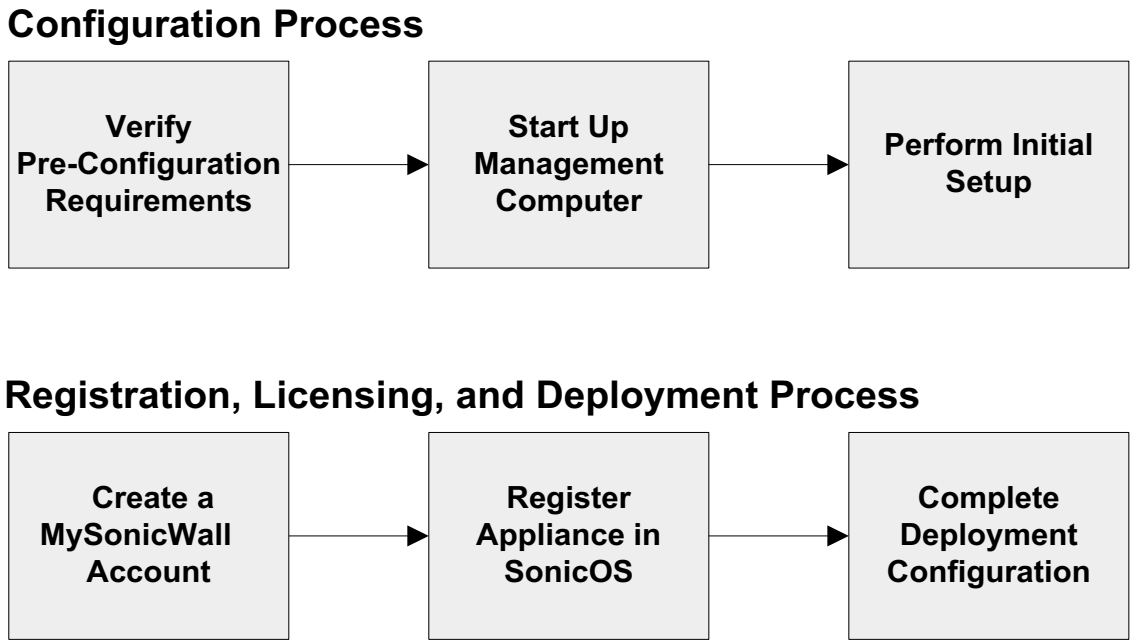
- Up to 20 Gbps of high-performance business firewall throughput
- Up to 5 Gbps of malware protection and up to 11.5 Gbps of application inspection with intrusion prevention
- Gateway and client services, including Capture Advanced Threat Protection, application monitoring & control, deep packet inspection over SSL, content filtering, anti-virus, anti-spyware, intrusion prevention, SSL VPN and IPsec VPN access, stateful high availability and high availability clustering

For more product information, see https://www.sonicwall.com/products/sonicwall-supermassive-9000.

Contents

Using this Getting Started Guide

The following flow chart illustrates the necessary steps in the process of getting started with your new SonicWall SuperMassive appliance.



2

Hardware Overview

This section describes the items shipped with the SonicWall SuperMassive 9200/9400/9600 appliance and provides front and rear illustrations of the SuperMassive.

SuperMassive Package Contents

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

1 One SuperMassive appliance

2 One rack mounting kit

3 One serial CLI cable

4 One Ethernet cable

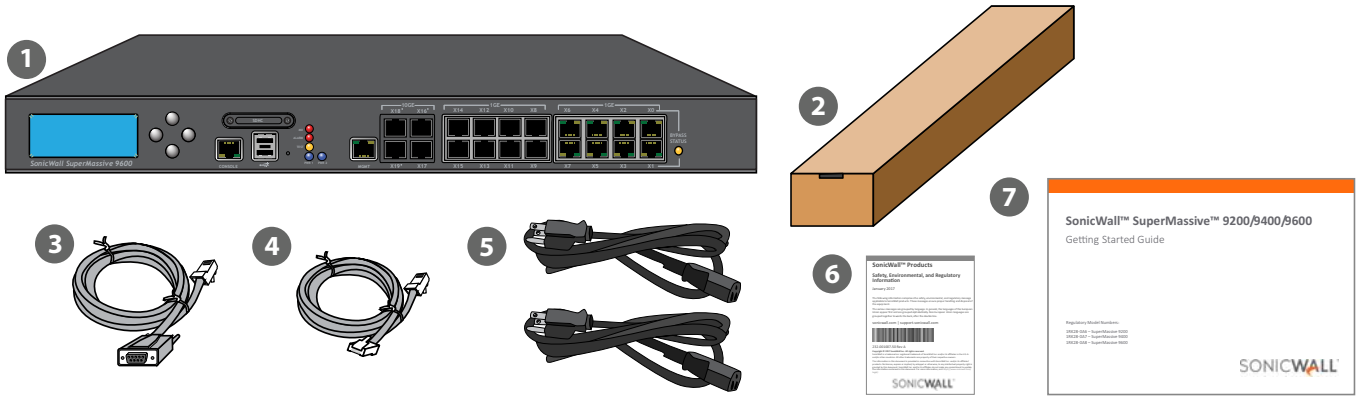
5 Two power cords*

6 One *Safety, Environmental, and Regulatory Information* document

7 One *SonicWall SuperMassive 9200/9400/9600 Getting Started Guide*

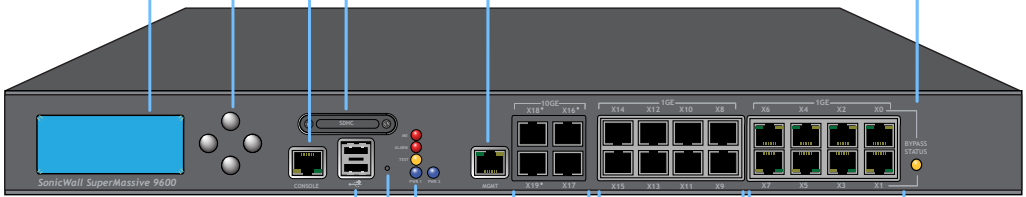
*The included power cords are approved for use only in specific countries or regions. Before using a power cord, verify that it is rated and approved for use in your location. The power cords are for AC mains installation only. Field conversion DC power cable is different, see Installation Requirements on page 62 for more information.

SuperMassive Package Contents



Missing Items? If any items are missing from your package, contact SonicWall Support at:
https://support.sonicwall.com/contact-support

SuperMassive Front Panel



Console Port
Access the SonicOS Command Line Interface (CLI) using the serial CLI cable

Control Buttons
Navigates the LCD screen; for future use

LCD Screen
Display screen

SDHC Port
Secure Digital High-Capacity (SDHC) port for future use

Bypass Status
Turns on when fail-to-wire bypass mode is active

MGMT Port (1 GE)
1 Gigabit Ethernet Management Interface

USB Ports (2)
For 3G/4G/Analog modem adaptor support

SafeMode Button
Press and hold until Test LED starts blinking to set the appliance into SafeMode.

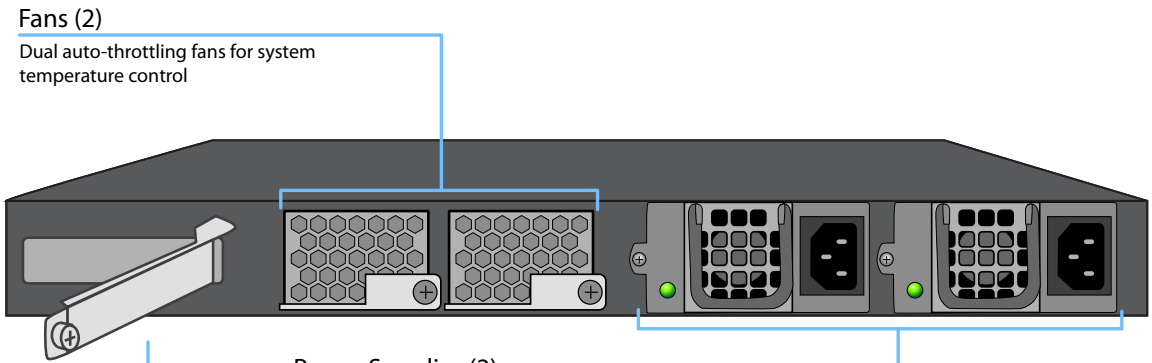
LED Indicators
Power: Blue: Indicates power supplies are operating correctly
Yellow: Indicates a disconnected power supply
Test: Quick Blinking Yellow: Initializing
Slow Blinking Yellow: SafeMode
Solid Yellow: Test mode
Alarm: Indicates alarm activity in Red LED
M0: Indicates Expansion Module 0 activity in Red LED

X0-X7 (1 GE)
High-speed copper Gigabit Ethernet ports

X8-X15 (1 GE SFP)
1 Gigabit Ethernet hot-pluggable SFP interfaces for high-speed fiber or copper Ethernet communication

X16-X19 (10 GE SFP+)
10 Gigabit Ethernet hot-pluggable ports
*X16, X18, and X19 are designated with a 'dot' to signify ports with a direct uplink to the appliance CPU for maximum throughput; X17 shares the CPU uplink with X0-X15.

SuperMassive Back Panel



WARNING: Potential Hazard from Fan

This manual contains specific warning and caution statements where they apply. Please read the Safety Instructions before use! See Product Safety and Regulatory Information on page 61.

3

Initial Setup

This section provides an overview of available WAN types, a section to record configuration information, and initial setup information and procedures.

Determining the WAN Type

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

- **Static**—Configures the appliance for a network that uses static IP addresses.
- **DHCP**—Configures the appliance to request IP settings from a DHCP server on the Internet.
- **PPPoE**—Point-to-Point Protocol over Ethernet (PPPoE) is typically used with a DSL modem. If your ISP requires desktop software with a username and password, select NAT with PPPoE mode.
- **PPTP**—Point-to-Point Tunneling Protocol (PPTP) is used to connect to a remote server. PPTP typically supports older Microsoft Windows implementations that require tunneling connectivity.
- **L2TP**—Layer 2 Tunneling Protocol (L2TP) is used to transmit Layer 2 data over IP or other Layer 3 routed networks. Internet Service Providers (ISPs) often use it to enable virtual private networks (VPNs) for customers over the Internet. It does not encrypt network traffic itself. If L2TP is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.

NOTE: For more information regarding other supported WAN types such as Wire Mode or Tap Mode, refer to the *SonicOS Administration Guide*.

System Requirements

Before beginning the setup process, verify that you have:

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

Supported Browsers

	Accepted Browser	Browser Version Number
	Internet Explorer	9.0 and higher
	Chrome	18.0 and higher
	Firefox	16.0 and higher
	Safari	5.0 and higher, running on non-Windows machines

Recording Configuration Information

Use this section to record your configuration information. Be sure to keep it for future reference.

NOTE: The default MGMT interface IP address is 192.168.1.254.

Registration Information

Serial Number:	Record the serial number found on the bottom panel of your SuperMassive appliance.
Authentication Code:	Record the authentication code found on the bottom panel of your SuperMassive appliance.

Networking Information

LAN IP Address:	Select a static IP address for your SuperMassive appliance that is within the range of your local network. (default for X0 is *192.168.168.168*)
Subnet Mask:	Record the subnet mask for the local network (default mask is *255.255.255.0*). Client devices connecting through the appliance LAN interface are assigned IP addresses in this network (default client addresses assigned by the SonicOS DHCP server are on the 192.168.168.0/24 subnet).
WAN IP Address:	Select a static IP address for your Ethernet WAN interface (X1). This setting only applies if you are using an Internet Service Provider (ISP) that assigns a static IP address.

Administrator Information

Admin Name:	Select an administrator account name. (default is *admin*)
Admin Password:	Select an administrator password. (default is *password*)

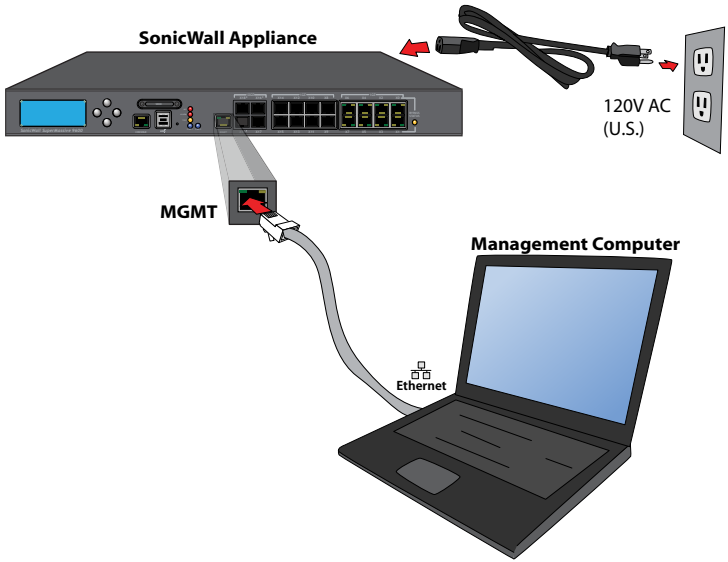
Internet Service Provider (ISP) Information

Record the following information about your current Internet service:

If you are connecting with DHCP	No information is usually required. However, some providers may require a host name. Host Name:
If you are connecting with a Static IP address	IP Address: _____._____._____._____ Subnet Mask:_____._____._____._____ Default Gateway: _____._____._____._____ Primary DNS: _____._____._____._____ DNS 2 (optional): _____._____._____._____ DNS 3 (optional): _____._____._____._____

Initial Configuration

The diagram below illustrates how to connect your management computer to the SuperMassive appliance for initial setup.



The following sections provide initial configuration information and instructions for connecting your SonicWall SuperMassive appliance for initial setup:

Connecting to the MGMT Port

The MGMT port is a dedicated 1 gigabit Ethernet interface for appliance management and SafeMode access.

1. Using the provided Ethernet cable, connect one end of the cable to the computer you are using to manage the SuperMassive appliance.
2. Connect the other end of the Ethernet cable to the MGMT port on your SuperMassive appliance.

Applying Power to the SuperMassive

Connect the AC power cords from the SonicWall SuperMassive appliance into appropriate power outlets.

For further information regarding power requirements, refer to Product Safety and Regulatory Information on page 61 of this document.

SuperMassive LED Activity

The Power LEDs on the front panel illuminate blue when the appliance is powered on.

The Test LED or Alarm LED may illuminate and blink while the appliance performs a series of diagnostic tests. When these LEDs are no longer illuminated and the Power LEDs remain steadily lit, the SonicWall SuperMassive appliance is ready for configuration. This typically occurs within a few minutes of turning on the power.

If the Test or Alarm LEDs remain lit after the SuperMassive has completed powering on, restart the appliance by disconnecting the power, waiting 1 minute, and then connecting the power again.

For a connected MGMT or X0 - X7 port, the Link LED for the port illuminates green or amber depending on the link throughput speed, indicating an active connection:

- Amber indicates 1 Gbps
- Green indicates 100 Mbps
- An unlit left LED with the right LED lit indicates 10 Mbps

Using the Setup Wizard

When you are ready to begin initial setup, configure your management computer with a static IP address on the 192.168.1.0/24 subnet, such as 192.168.1.20. This allows your computer to connect to SonicOS via the MGMT interface.

NOTE: Be sure to disable pop-up blocking software, or set your web browser to allow pop-ups and cookies.

To configure initial settings using the Setup Wizard:

1 With your computer connected to the appliance MGMT port, start your web browser and navigate to the default MGMT interface IP address: **http://192.168.1.254**

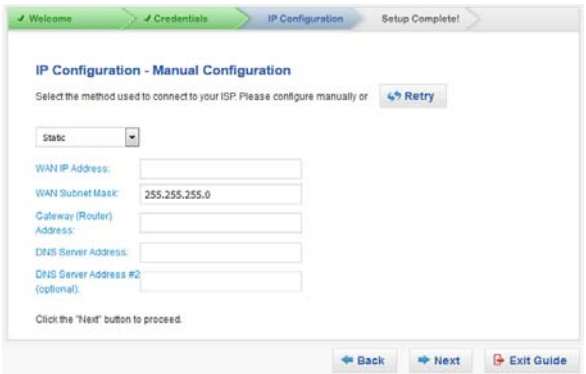
The initial screen displays the options to launch the Setup Wizard or configure the appliance manually.

2 Launch the SonicOS Setup Wizard by clicking the first **here** link. This wizard helps you quickly configure the SonicWall appliance to secure your Internet connection.

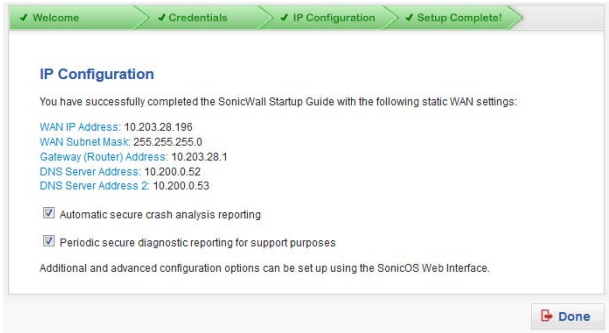
3 Follow the on-screen prompts to configure the admin password and network settings.

If a DHCP server is available on the network, the wizard requests IP settings from it. You can click **Next** to accept these or click **Manual Config** to enter a static IP address and other network settings.

In the Manual Configuration screen, click **Retry** to revert to DHCP, or enter your own settings and then click **Next**.



4 Once completed, click **Done** in the Setup Complete screen.



5 Continue to Connecting to the Internet on page 20 to connect the appliance for Internet access.

Then, refer to Registering, Licensing, and Upgrading on page 25 to begin the registration process.

Connecting to the Internet

After initial setup is complete, physically connect the SuperMassive LAN and WAN interfaces to the appropriate network devices in your environment to provide access to external networks or the Internet.

NOTE: Internet connectivity is needed for the recommended product registration process. For initial Internet access, connect your computer to the LAN subnet.
You cannot reach the Internet or other external destinations while connected to the MGMT interface without first configuring a default gateway in its interface settings.

Connecting the LAN Port

1 Connect one end of an Ethernet cable to your local network switch or other networking device, or to your computer.

2 Connect the other end of the Ethernet cable to the X0 (LAN) port on your SonicWall SuperMassive appliance.

Connecting the WAN Port

1 Connect one end of an Ethernet cable to your Internet connection.

If you have a router, DSL modem, or cable modem, connect the Ethernet cable to a LAN port on the router or modem.

2 Connect the other end of the Ethernet cable to the X1 (WAN) port on your SonicWall SuperMassive appliance.

Testing Your Internet Connection

To test your Internet connection:

1 After you exit the Setup Wizard, connect your computer to the LAN subnet or directly to the X0 (LAN) port.

2 Point your browser to the X0 IP address configured during initial setup (default: *192.168.168.168*).

3 When the login page appears, log into the SonicOS management interface as *admin*, using the configured password (default: *password*).

4 Open a command prompt window on your computer and enter the command: `ping sonicwall.com`

5 Open another web browser and navigate to: https://www.sonicwall.com

If you can view the SonicWall home page, you have configured your SuperMassive appliance correctly.

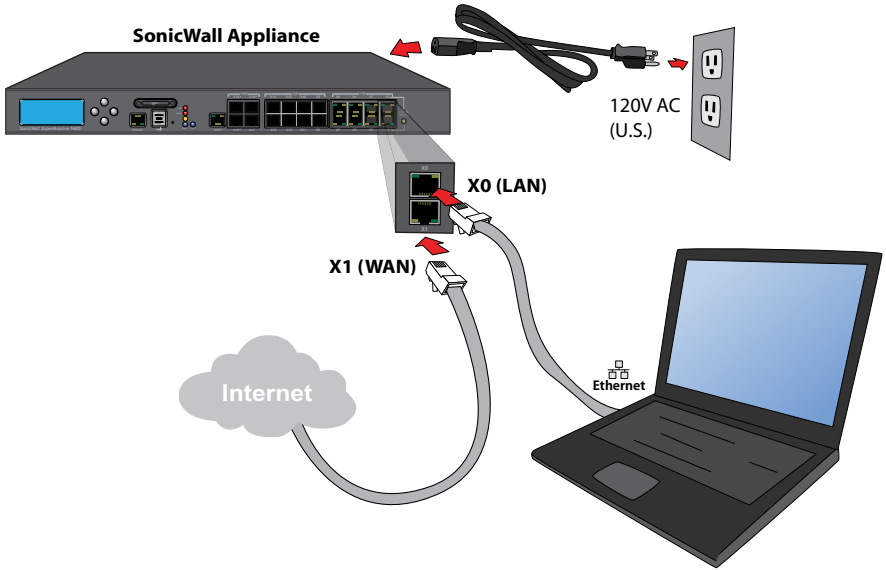
If you cannot view the SonicWall home page, try one of these solutions:

- Verify that the Local Area Connection settings on your computer are set to use either DHCP or a static IP on the LAN subnet.
- Renew your computer's DHCP address or restart your computer to accept new network settings from the DHCP server in the SonicWall appliance.
- Restart your Internet router to communicate with the DHCP client in the SonicWall appliance.
- Check Troubleshooting Connections on page 23 for more suggestions.

NOTE: WAN connectivity issues are unrelated to completion of the MySonicWall registration process.

Internet Access

The diagram below illustrates how to connect your computer to the SonicWall SuperMassive appliance for Internet access.



Troubleshooting Connections

Use the suggestions in this section to troubleshoot your MGMT and LAN connections.

Troubleshooting Your MGMT Connection

If you cannot connect to the SonicWall SuperMassive appliance or the Setup Wizard does not display, consider the following:

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

Troubleshooting Your LAN Connection

If you do not see the SonicOS login prompt when you point your browser to the X0 (LAN) IP address, consider the following:

- Did you correctly enter the IP address for the SonicWall SuperMassive X0 interface into your web browser, beginning with “http://” or “https://”?
- Did you try restarting your management station while it is connected to the SonicWall appliance?
- Are the Local Area Connection settings on your computer set to one of the following?:
  - Obtain an IP address automatically using DHCP
  - A static IP address on the default LAN subnet (192.168.168.0/24)
  - A static IP address on the configured LAN subnet, if you changed it during initial setup
  - Do you have the Ethernet cable connected to your computer and to the X0 (LAN) port on your appliance?
- Is the connector clip on your network cable properly seated in the port of the security appliance?

4

Registering, Licensing, and Upgrading

This section provides instructions for registering on MySonicWall, licensing security services, and upgrading firmware on your SonicWall SuperMassive appliance.

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

Using MySonicWall

SonicWall requires a MySonicWall account prior to configuring your appliance. If you already have a MySonicWall account, you can continue to Registration Overview on page 27.

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.

For a High Availability configuration, MySonicWall provides a way to associate a secondary unit that can share security service licenses with your primary appliance.

NOTE: 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 SonicWall SuperMassive appliance. You can create a new MySonicWall account from any computer by navigating to: https://www.mysonicwall.com

To create a MySonicWall account:

1. In your Web browser, navigate to: https://www.mysonicwall.com
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**.

Registration Overview

Although there are several ways to register your new SonicWall appliance, SonicWall recommends registering your appliance through the SonicOS management interface.

This section describes how to register and license your appliance through SonicOS, as well as the alternate options available on MySonicWall.

NOTE: If you haven't created a MySonicWall account, see Creating a MySonicWall Account on page 26.

Registering in SonicOS

After you have completed the Setup Wizard and can successfully connect to your SonicWall SuperMassive appliance, you are ready to register the security appliance.

1. Log into your SonicWall appliance. Use the LAN (X0) defaults (*https://192.168.168.168* and *admin / password*), or if you changed these fields during the initial setup process, use the new IP address and credentials. Then, click **Login**.
2. Navigate to the **System > Status** page.
3. The screen displays a message that your SonicWall appliance is not registered. Click the **Register** link.
4. Enter your MySonicWall username (your email address) and password in the appropriate fields. Then, click **Submit**.

   If you haven't created a MySonicWall account, see Creating a MySonicWall Account on page 26.
5. The licensing server acquires the necessary information directly from the appliance. If asked, optionally specify a **Friendly Name** or **Product Group** for the SonicWall appliance.
6. Acknowledge the registration completion notification by clicking **Continue**. The **Licenses > License Management** page now lists all the Security Services associated to your appliance.

Alternative Registration Options

If you have registered your SonicWall appliance through the SonicOS interface, you can continue to Licensing Security Services on page 29.

Although SonicWall strongly recommends registering your appliance using the SonicOS interface, you can optionally use MySonicWall to register your appliance.

Registering on MySonicWall

To register your appliance directly on MySonicWall:

1. Log into your MySonicWall account. If you do not have an account, create one at: https://www.mysonicwall.com
2. Type the SonicWall appliance serial number in the **Register a Product** field. The serial number is displayed in the **System > Status** page and is also on the bottom panel of your appliance.
3. Click **Next**.
4. Type a **Friendly Name** for the appliance.
5. Select the **Product Group** from the drop-down list, if available.
6. Enter the appliance **Authentication Code**. The authentication code is displayed in the **System > Status** page and is also on the bottom panel of your appliance.
7. Click **Register**.

Synchronizing Licenses Manually

To manually synchronize licenses with MySonicWall from the SonicOS interface:

1. Log into your appliance and navigate to the **System > Licenses** page.
2. Scroll to the **Manage Security Services Online** section.
3. Click the **Synchronize** button to synchronize licenses with MySonicWall.

Using the License Keyset

MySonicWall provides an encrypted license keyset for each registered appliance. You can use the license keyset to manually apply all active licenses to your SonicWall appliance.

To obtain and apply the license keyset:

1. Log into your MySonicWall account and click the link for your appliance.
2. On the **Services Management** page, click the **View License Keyset** link.
3. Click the encrypted text, then press **Ctrl+A** to select the entire keyset, and then copy it to your clipboard.

4 Log into your appliance and navigate to the **System > Licenses** page.

5 Scroll down to the **Manual Upgrade** section and paste the keyset in the appropriate field.

6 When finished entering the keyset, click **Submit**.

Licensing Security Services

To license a security service, first access the **Service Management** page in MySonicWall. The **Service Management** page is specific to your product and lists security services, support options, and software that you can purchase or try with a free trial.

To access the **Service Management** page, do one of the following:

- Log into your appliance, navigate to **System > Licenses**, click the **To Activate, Upgrade, or Renew services, click here** link, and then enter your MySonicWall credentials.
- Point your browser to https://www.mysonicwall.com and enter your MySonicWall credentials, then navigate to **My Products > Product Management** and click on your appliance name or serial number.

Next, scroll down to the **Applicable Services** section to select a free trial or purchase the service:

- **Free Trial of Service**—Click the **Try** icon in the **Action** column for the security service you wish to try for a 30-day free trial. The free trial immediately activates and notifies you of the trial expiration date. The **Service Management** page displays updated information about the free trial service.
- **Purchase a Service**—Click the **Cart** icon to purchase a security service. In the **Buy Service** page, specify the desired quantity of licenses, then click **Add to Cart**. Once the item(s) have been added, click the **Checkout** button. Follow the instructions to complete your purchase.

Applicable Services and Software

On the **Service Management** page in MySonicWall, the **Applicable Services** section lists the services available for your product.

The **Status** column indicates whether the service is *Licensed*, *Not Licensed*, or *Expired*. The **Action** column lets you purchase or activate additional services.

The following products and services are available for SonicWall SuperMassive appliances:

- Service Bundles:
  - Advanced Gateway Security Suite (AGSS)
  - Comprehensive Gateway Security Suite (CGSS)
  - McAfee: Client/Server Anti-Virus Suite
- Gateway Services:
  - Capture Advanced Threat Protection
  - Gateway AV / Anti-Spyware / Intrusion Prevention
  - Application Visualization and Control
  - Deep Packet Inspection for SSL (DPI-SSL)
  - Deep Packet Inspection for SSH (DPI-SSH)
  - Content Filtering: Premium Edition
  - Botnet Filter
  - Stateful High Availability
  - Active/Active Clustering Service
- Desktop & Server Software:
  - McAfee: Enforced Client Anti-Virus and Anti-Spyware
  - Kaspersky: Enforced Client Anti-Virus and Anti-Spyware
  - Global VPN Client
  - Content Filtering Client
  - Analyzer
  - SSL VPN
  - Virtual Assist
  - WAN Acceleration Software
  - WAN Acceleration Client
- Support Services:
  - 24x7 Support
  - Premier Support
  - Software and Firmware Updates
  - Hardware Warranty

NOTE: Applicable services per platform sometimes change. Please check on MySonicWall for the current list of services available for your appliance.

Activating Licenses Using a Key

If you registered your appliance through SonicOS, all licensed services are already activated. You can continue to Upgrading Firmware on page 31.

If you purchased a service subscription or upgrade from a sales representative separately, you will have an *Activation Key* for the service. 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 your service licenses using the key:

1 Log into your MySonicWall account

2 In the **My Products** page, click the appliance name to open the **Service Management** page. The **Applicable Services** table displays a list of services that are already licensed or are available to license on your SonicWall appliance.

Note that your initial purchase may have included security services or other software bundled with the appliance. These licenses are enabled on MySonicWall when the appliance is delivered to you.

3 Locate the service in the **Applicable Services** section and click the *key* icon.

4 Type or paste your key into the **Activation Key** field, and then click **Submit**.

After activating the service, the **Status** and **Expiration** columns display updated information when you return to the **Service Management** page.

Upgrading Firmware

SonicWall recommends that you run the latest available firmware on your security appliance. You will need to upgrade the factory-installed firmware to the latest version available on MySonicWall.

See the following sections to upgrade an existing SonicOS firmware image to a newer version:

- Saving a Backup and Exporting Settings on page 32
- Obtaining the Latest Firmware on page 32
- Upgrading the Firmware on page 33
- Using SafeMode to Upgrade Firmware on page 33

Saving a Backup and Exporting Settings

Before beginning the update process, make a system backup on your SonicWall appliance. The backup feature saves a copy of the current system state, firmware, and configuration settings on your SonicWall security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

You can also export the configuration settings (preferences) to a file on your local management station. This file serves as an external backup of the configuration settings, and can be imported back into the SonicWall security appliance if it is necessary to reboot the firmware with factory default settings.

To save a system backup on your appliance and export configuration settings:

1. On the **System > Settings** page, click **Create Backup**. SonicOS takes a "snapshot" of your current system state, firmware, and configuration settings, and makes it the new System Backup firmware image. Creating a new backup overwrites the existing System Backup image, if any. The **System Backup** entry is displayed in the **Firmware Management** table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.
3. In the popup window, click **Export**.

Obtaining the Latest Firmware

To obtain a new SonicOS firmware image file:

1. In a browser on your management computer, log into your MySonicWall account at: https://www.mysonicwall.com
2. In MySonicWall, click **Downloads** in the left navigation pane to display the Download Center screen.
3. Select **SuperMassive 9x00 Firmware** (where *9x00* is either *9200*, *9400*, or *9600*, depending on your platform) in the **Software Type** drop-down list to display available firmware versions.
4. Locate the firmware version you want, and click the link to download it to a convenient location on your computer. You can download the Release Notes and other associated files in the same way.

Upgrading the Firmware

The appliance must be properly registered before the firmware can be upgraded. Refer to Registering in SonicOS on page 27 for more information.

To upload new firmware to your SonicWall appliance and reboot with current configuration settings:

1. Download the SonicOS firmware image file from MySonicWall and save it to a convenient location on your local computer.
2. Point your browser to the appliance IP address, and log in as an administrator.
3. On the **System > Settings** page, click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS firmware image file, select the file and click the **Upload** button.

   After the firmware finishes uploading, it is displayed in the **Firmware Management** table.
5. Click the Boot icon in the row for **Uploaded Firmware - New!** to restart the appliance with the new firmware using your existing configuration settings.
6. In the confirmation dialog box, click **OK**. The appliance restarts and then displays the login page.
7. Enter your user name and password. The new SonicOS image version information is displayed on the **System > Status** page.

Using SafeMode to Upgrade Firmware

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

The SafeMode procedure uses a recessed *SafeMode* button in a small pinhole near the USB ports on the front of the SonicWall appliance.

To use SafeMode to upgrade firmware on a SonicWall security appliance:

1. Connect your computer to the MGMT port on the appliance and configure your computer with an IP address on the 192.168.1.0/24 subnet, such as 192.168.1.20.

2 Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the SafeMode button on the front of the SonicWall appliance for more than 20 seconds (possibly in the range of 90 seconds).

The Test light begins blinking when the appliance has rebooted into SafeMode.

3 Point your browser to **http://192.168.1.254** to access the SafeMode management interface.

NOTE: Use **http** rather than **https** in SafeMode.

4 Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file and click **Upload**.

5 Click the Boot icon in the row for one of the following:

- **Uploaded Firmware - New!**

  Use this option to restart the appliance with your current configuration settings.

- **Uploaded Firmware with Factory Default Settings - New!**

  Use this option to restart the appliance with factory default configuration settings.

6 In the confirmation dialog box, click **OK** to proceed.

CAUTION: Do not power off the appliance while it is rebooting.

7 After successfully booting the firmware, the login screen displays.

After a factory default, you will see the initial login screen, which displays options to launch the Setup Wizard or to log into SonicOS and configure the appliance manually. If you choose the latter, enter the default user name and password (*admin / password*) to access the SonicOS management interface.

8 You can continue to manage the appliance from the MGMT interface at 192.168.1.254.

If you prefer to connect to SonicOS through the WAN or LAN interface of the appliance:

a Disconnect your computer from the appliance.

b Reconfigure your computer to automatically obtain an IP address and DNS server address, or reset it to its normal static values.

c Connect the computer to your network or to the desired interface on the appliance.

d Point your browser to the WAN or LAN IP address of the appliance.

5

Deployment Scenarios

This section provides configuration overviews, as well as deployment scenarios for your SonicWall SuperMassive appliance.

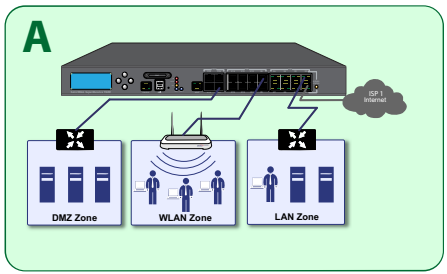
TIP: ***Wire Mode*** is another deployment option for the SuperMassive, not fully covered in this guide. See the *SonicOS Administration Guide* for detailed information. There are four settings for Wire Mode:

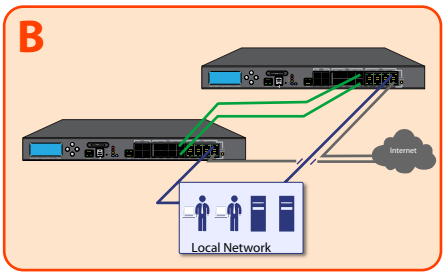
- **Bypass Mode**—The firewall is inserted into the physical data path without turning on inspection. Bypass Mode can easily be reconfigured later as Inspect Mode or Secure Mode.
- **Inspect Mode**—Packets pass through the firewall and are also mirrored to the SonicWall ReAssembly-Free Deep Packet Inspection™ (RF-DPI) engine, providing passive inspection, classification, and flow reporting.
- **Secure Mode**—Provides full RF-DPI inspection and control of network traffic. Secure Mode affords the same level of visibility and enforcement as conventional NAT or L2 Bridged Mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior.
- **Tap Mode**—A firewall interface that is configured in Tap Mode receives mirrored packets from an adjacent switch SPAN port. Similar to Inspect Mode, but with a single port and not in the physical path of traffic.

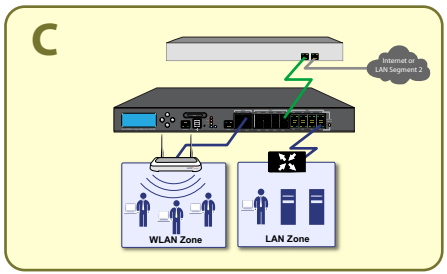
Advanced Deployment Scenarios

Select a deployment scenario that best fits your network environment. Refer to the table below and the diagrams here and on the following pages for help in choosing a scenario.

Current Gateway Configuration	New Gateway Configuration	Use Scenario
No gateway appliance	Single SuperMassive appliance as a primary gateway.	Scenario A: NAT Mode Gateway on page 37
No gateway appliance	Pair of SuperMassive appliances for high availability.	Scenario B: Stateful HA Pair on page 38
Existing Internet gateway appliance	SuperMassive as replacement for an existing gateway appliance.	Scenario A: NAT Mode Gateway on page 37
Existing Internet gateway appliance	SuperMassive in addition to an existing gateway appliance.	Scenario C: L2 Bridged Mode on page 39
Existing SonicWall gateway appliance	SuperMassive appliance in addition to an existing SonicWall gateway appliance.	Scenario B: Stateful HA Pair on page 38







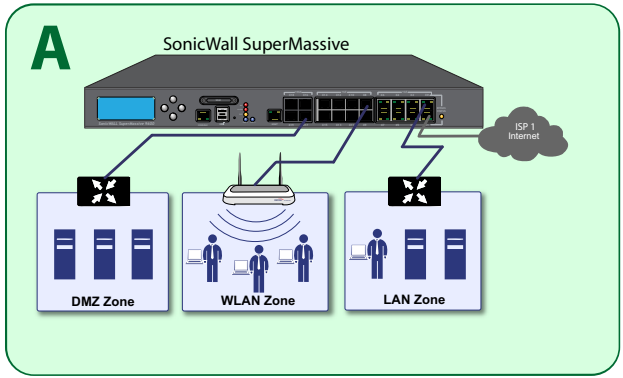
Scenario A: NAT Mode Gateway

For new network installations or installations where the SuperMassive appliance is replacing the existing network gateway.

In this scenario, the SuperMassive appliance is configured in NAT mode to operate as a single network gateway. Multiple Internet connections may be routed through the SonicWall appliance for load balancing and failover purposes. Because only a single SonicWall appliance is deployed, the added benefits of high availability with a stateful synchronized pair are not available.

To set up this scenario, follow the steps covered in:

- Configuring NAT Mode Gateway on page 40



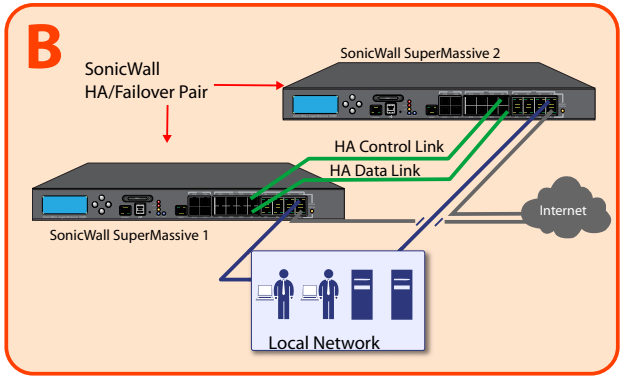
Scenario B: Stateful HA Pair

For network installations with two SonicWall SuperMassive appliances configured as a stateful synchronized pair for redundant High Availability (HA) networking.

In this scenario, one SuperMassive operates as the Primary gateway device and the other SuperMassive is in Standby mode. All network connection information is synchronized between the two devices so that the Secondary appliance can seamlessly switch to Active mode without dropping connections if the Primary device loses connectivity.

To set up this scenario, follow the steps covered in:

- Configuring a Stateful HA Pair on page 41



Scenario C: L2 Bridged Mode

For network installations where the SonicWall SuperMassive appliance is running in tandem with an existing network gateway.

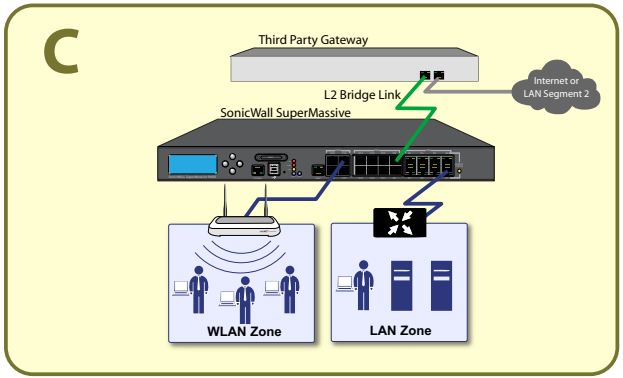
In this scenario, the original gateway is maintained. The SonicWall SuperMassive is integrated seamlessly into the existing network, providing the benefits of deep packet inspection and comprehensive security services on all network traffic.

NOTE: Wire Mode also provides this functionality. For more information about Wire Mode, see the *SonicOS Administration Guide*.

L2 Bridged Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridged Mode, a SonicWall security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for TCP and UDP traffic.

To set up this scenario, follow the steps covered in:

- Configuring L2 Bridged Mode on page 47



Configuring NAT Mode Gateway

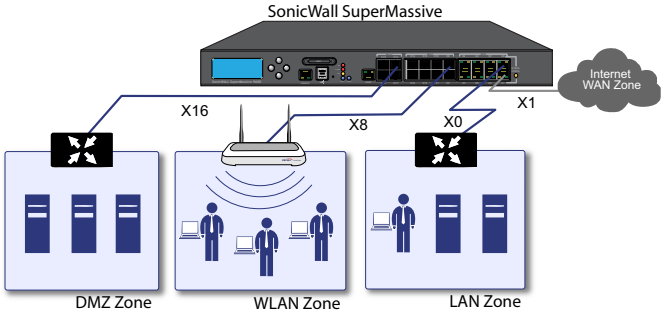
This section provides an overview of a SonicWall SuperMassive appliance operating as a single network gateway in NAT mode, which is the default mode for a newly configured SuperMassive appliance. This section is relevant to administrators following deployment **Scenario A**.

NOTE: No additional configuration is necessary to deploy your appliance as a single network gateway in Many-to-One NAT mode.

Overview of NAT Mode

Network Address Translation (NAT) allows private IP addresses on internal networks to be mapped to at least one public IP address on the WAN interface of the SonicWall security appliance. Outbound traffic from the internal network uses many-to-one NAT address mappings for their LANs, WLANs, and other internal networks.

All traffic in SonicOS must go through both an access rule and a NAT policy, a fundamental part of the NAT Mode architecture. The NAT policy is even used for traffic that needs no IP address translation, such as traffic traveling between two different LAN interfaces, traffic on the simplest types of VPNs, or through Layer 2 Bridged Mode / Transparent Mode configurations.



The SonicWall SuperMassive ships with the internal DHCP server active on the LAN port. However, if a DHCP server is already active on your LAN, the SonicWall appliance will disable its own DHCP server to prevent conflicts.

As shown in the illustration on this page, ports X1 and X0 are preconfigured as WAN and LAN, respectively. The remaining ports (X2-X17) can be configured to meet the needs of your network.

In the example diagram, certain interfaces are configured for specific zones:

- X1—WAN
- X0—LAN
- X8—Wireless LAN
- X16—DMZ

NAT policies allow the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously.

For configuration procedures and information regarding the different types of NAT policies, such as Many-to-One, One-to-One, or One-to-Many Load Balancing, refer to the *SonicOS Administration Guide*.

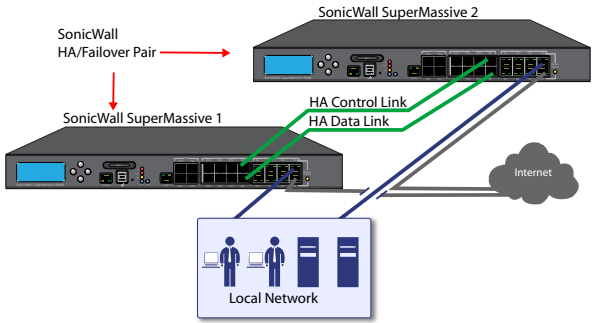
Configuring a Stateful HA Pair

This section provides instructions for configuring a pair of SonicWall SuperMassive appliances for Stateful High Availability (HA). This section is relevant to administrators following deployment **Scenario B**.

A Stateful HA pair operates in NAT mode by default, similar to Scenario A, with the added benefit of high availability.

See the following sections:

NOTE: Both units in a High Availability pair must be the same model running the same firmware version.



Initial High Availability Setup

Before you begin the configuration of HA on the Primary SonicWall security appliance, perform the following tasks:

- Determine which interfaces should be used as the HA Control Link and the HA Data Link. Remember, they must be the same ports on each appliance.
- Make a note of the serial number of the appliance that will run as the Secondary device. You can find this on the bottom of the appliance or in the **System > Status** page. You need to enter this number in the **High Availability > Settings > HA Devices** page.
- Verify that the Primary and Secondary appliances are registered on MySonicWall and are running the same SonicOS versions.
- Ensure that the Primary and Secondary security appliances' LAN, WAN, and other interfaces are properly connected for failover.
- Connect the HA Control and Data Links on the Primary and Secondary appliances with appropriate cables.
- Turn on the Primary SonicWall security appliance first. Then, turn on the Secondary SonicWall security appliance.

Configuring High Availability Settings

The first task in setting up HA after completing Initial Setup on page 13 is configuring the **High Availability > Settings** page on the Primary SonicWall security appliance. Once you configure HA on the Primary appliance, it communicates the settings to the Secondary appliance.

To configure HA settings on the Primary appliance:

1. Log into your Primary appliance as an administrator.
2. Navigate to the **High Availability > Settings** page.
3. On the **General** tab, select **Active / Standby** from the **Mode** drop-down list.
4. Click **OK** in the popup dialog about license and signature updates.
5. Select the **Enable Stateful Synchronization** checkbox.
6. Click **OK** in the popup dialog about the recommended settings for Heartbeat Interval and Probe Interval.
7. Click on the **HA Devices** tab and type in the serial number for the Secondary appliance.
8. Click on the **HA Interfaces** tab and select interfaces for **HA Control Interface** and **HA Data Interface**.

9 Click **Apply** to save these settings. All settings are synchronized to the Secondary appliance, and the Secondary appliance reboots.

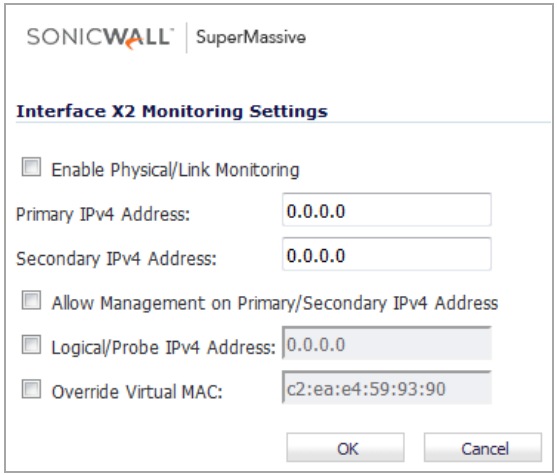
Configuring HA Monitoring Settings

After configuring the HA settings, you need to configure the Monitoring settings for the LAN or WAN. This includes configuring unique IP addresses for each appliance in the Stateful HA pair. You will need to log into the appliances using these IP addresses in order to complete the registration process from within SonicOS, which will allow license sharing and synchronization.

To configure HA monitoring on the Primary appliance:

1 Navigate to the **High Availability > Monitoring** page.

2 Click the Configure icon of the Interface for which you want to edit settings. The **Edit HA Monitoring** dialog box displays.



3 To enable physical/link monitoring, select the **Enable Physical / Link Monitoring** checkbox.

4 In the **Primary IP Address** field, enter the unique LAN or WAN management IP address of the Primary appliance.

5 In the **Secondary IP Address** field, enter the unique LAN or WAN management IP address of the Secondary appliance.

6 Select the **Allow Management on Primary/Secondary IP Address** checkbox.

7 To enable logical monitoring or probing, select the **Logical / Probe IP Address** checkbox and enter the IP address of the target host.

8 Click **OK**.

You can repeat these steps to configure monitoring on other interfaces.

For more information regarding the optional settings, see the *SonicOS Administration Guide*.

Configuring Optional HA Settings

The following settings are optional.

To configure optional settings on the High Availability > Settings page, General tab:

1 To backup the firmware and settings when you upgrade the firmware version, select the **Generate/Overwrite Backup Firmware and Settings When Upgrading Firmware** checkbox.

2 SonicWall does not recommend enabling the **Enable Preempt Mode** checkbox when using Stateful High Availability.

3 Select the **Enable Virtual MAC** checkbox to allow the Primary and Secondary appliances to share a single MAC address. This simplifies the process of updating network ARP tables and caches when a failover occurs. Only the WAN switch that the two appliances are connected to needs to be notified. All outside devices will continue to route to the single shared MAC address.

4 Click **Apply** to save any of the settings on this page.

Configuring HA Advanced Settings

The settings on the **High Availability > Advanced** page are optional.

To configure optional settings on the High Availability > Advanced page:

1 Adjust the **Heartbeat Interval** to control how often the two units communicate. The default and recommended minimum is 1000 milliseconds.

2 The **Failover Trigger Level** sets the number of heartbeats that can be missed before failing over. SonicWall recommends leaving this field at its default setting, and tuning it later if needed.

3 Set the **Probe Interval** for the interval in seconds between communication with upstream or downstream systems. The recommended setting is an interval of at least 5 seconds. You can set the **Probe IP**

Address(es) on the **High Availability > Monitoring** screen.

4 Set the **Probe Count**, which is the number of consecutive probes before the appliance considers the network path unreachable or broken. The default count is 3.

5 The **Election Delay Time** is the number of seconds allowed for internal processing between the two units in the HA pair before one of them takes the primary role. SonicWall recommends leaving this field at its default setting (3), then tuning it later if needed.

6 Enable the **Active / Standby Failover only when ALL aggregate links are down** checkbox to treat the aggregated link as down (causing a failover) only if all member links are down.

7 Select the **Include Certificates/Keys** checkbox to synchronize all certificates and keys when the **Synchronize Settings** button is clicked.

8 Click **Synchronize Settings** to synchronize the settings between the Primary and Secondary appliances.

9 Click **Synchronize Firmware** if you previously uploaded new firmware to your Primary appliance while the Secondary appliance was offline.

Synchronize Firmware is useful after taking your Secondary appliance offline while you test a new firmware version on the Primary appliance before upgrading both units.

10 Click **Force Active / Standby Failover** to force a failover between your Primary and Secondary appliances.

11 Click **Accept** to apply the settings on this screen.

HA License Configuration Overview

You can configure HA license synchronization by associating two SonicWall security appliances as HA Primary and HA Secondary on MySonicWall.

You must purchase a single set of security service licenses for the HA Primary appliance. To use Stateful HA, you must first activate the **Stateful High Availability** license for the primary unit in SonicOS. This is automatic if your appliance is connected to the Internet. See Registering, Licensing, and Upgrading on page 25.

License synchronization is used in a High Availability configuration so that the Secondary appliance can maintain the same level of network protection as the Primary, in case of a failover.

Completing HA Pair Association

The two appliances in an HA Pair must be associated on MySonicWall. Once they are associated, the Secondary appliance automatically shares the Security Services licenses of the Primary appliance.

If the Secondary appliance has not yet been registered, follow the steps listed in Registering in SonicOS on page 27 or Registering on MySonicWall on page 28 to register it. This is necessary to make it available for HA association with the Primary.

To associate two SonicWall appliances on MySonicWall:

1. Log into your MySonicWall account.
2. Click **My Products**.
3. On the My Products page, click the product **Name** or **Serial Number** of the appliance that you want to use as the Primary appliance.
4. On the Service Management page, scroll down to the **Associated Products** section.
5. Under Associated Products, click **HA Secondary**.
6. On the **My Product - Associated Products** page, select the appliance that you want to associate as the Secondary appliance from the **Serial Number** drop-down list.
7. Click **Associate**.
8. Log into the SonicOS management interface of the Primary appliance using the unique IP address assigned on the **High Availability > Monitoring** page.
9. Navigate to the **System > Licenses** page and click the **Synchronize Licenses** button. This allows the unit to synchronize with the SonicWall license server.
10. Log into the SonicOS management interface of the Secondary appliance using its unique IP address.
11. Navigate to the **System > Licenses** page and click the **Synchronize Licenses** button. This ensures license synchronization and sharing between the Primary and Secondary appliances.

This completes the HA association on MySonicWall and ensures that both appliances can share licenses.

Verifying High Availability Setup

Once you have configured the HA settings on the Primary SonicWall appliance, log into the Primary appliance's unique LAN/WAN IP address. Note that the management interface

displays **Logged Into: Primary SonicWall Status: Active** in the upper right-hand corner.

To verify that the Primary and Secondary SonicWall security appliances are functioning correctly, wait a few minutes, then turn off the Primary device. The Secondary appliance should quickly take over.

From your management workstation, test connectivity through the Secondary appliance by accessing a site on the public Internet – note that the Secondary appliance, when active, assumes the complete identity of the Primary, including its IP addresses and Ethernet MAC addresses.

Log into the Secondary SonicWall appliance's unique LAN/WAN IP address. The management interface should now display **Logged Into: Secondary SonicWall Status: Active** in the upper right-hand corner.

Now, turn the Primary appliance back on, wait a few minutes, then log back into the management interface. If stateful synchronization is enabled (automatically disabling preempt mode), the management interface should still display **Logged Into: Secondary SonicWall Status: Active** in the upper-right-hand corner.

If you are using the Physical/Logical Monitoring feature, experiment with disconnecting each monitored link to ensure correct configuration.

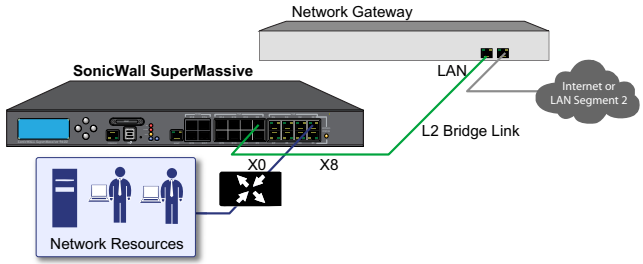
Configuring L2 Bridged Mode

This section provides instructions to configure the SonicWall SuperMassive appliance in tandem with an existing Internet gateway device. This section is relevant to users following deployment **Scenario C**.

Topics:

Connection Overview

Connect a WAN port (X8 shown here) on your SonicWall SuperMassive appliance to the LAN port on your existing Internet gateway device. Then connect the X0 port on your SonicWall appliance to your LAN resources.



Configuring the Primary Bridge Interface

The primary bridge interface is connected to your existing Internet gateway device. The requirements for the primary bridge interface are:

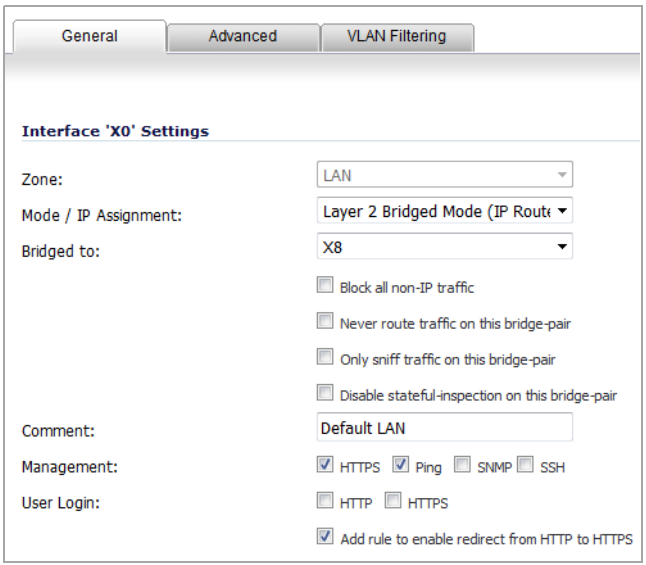
- The interface is in the WAN zone.
- The interface has a static IP address.
- The interface is ***not*** a member of a WAN Load Balancing group, such as the Default LB Group.

NOTE: The X1 WAN interface is automatically a member of the Default LB Group. For best results, configure another WAN interface for use as the primary bridge interface.

Configuring the Secondary Bridge Interface

1 In SonicOS, navigate to the **Network > Interfaces** page.

2 Click the Configure icon for the X0 (LAN) interface.



3 In the **Mode / IP Assignment** drop-down list, select **Layer 2 Bridged Mode**.

4 In the **Bridged to** drop-down list, select the WAN zone interface that you configured as the primary bridge interface.

5 Optionally enable the **Block all non-IP traffic** setting to prevent the L2 bridge from passing non-IP traffic.

NOTE: Do not enable **Never route traffic on this bridge-pair** unless your network topology requires that all packets entering the L2 Bridge remain on the L2 Bridge segments.

6 Enable the desired **Management** options (**HTTPS**, **Ping**, **SNMP**, **SSH**).

7 Enable the desired **User Login** options (**HTTP**, **HTTPS**).

8 Optionally enable the **Add rule to enable redirect from HTTP to HTTPS** option.

6

Support and Training Options

This section provides overviews of customer support and training options for SonicWall SuperMassive appliances. SonicWall offers a variety of online support and training options for your convenience.

Customer Support

SonicWall offers telephone, email and web-based support to customers who have a valid warranty or support contract.

Designed for business-critical environments, SonicWall 24x7 Support delivers the enterprise-class support features and quality of service that enterprise companies require to keep their networks running smoothly and efficiently. SonicWall 24x7 Support is an around-the-clock support service that includes phone, email and web-based technical support, ongoing software and firmware updates, direct access to a team of highly trained senior support engineers, advance exchange hardware replacement in the event of failure, and access to electronic support tools.

SonicWall also offers Value-Add Support with these options:

- Customer Success Manager - provides enterprise environments with a dedicated Customer Success Manager who works with your staff to help minimize unplanned downtime, optimize IT processes, and provide operational reports to drive efficiencies.
- Designated Support Engineer (DSE) - provides a named engineering resource to support your enterprise account.

For more information, visit:
https://support.sonicwall.com/essentials/support-offerings

Knowledge Base

The SonicWall Knowledge Base allows you to search by queries containing unique keywords, symptoms or details, filter results, view, rate, email and print articles.

For more information, visit:
https://support.sonicwall.com/kb-product-select

User Forums

The SonicWall User Forums provide a way for you to collaborate with peers and connect with experts to discuss a variety of security and appliance topics. To access the forums, log in using your MySonicWall credentials.

For more information, visit: https://forum.sonicwall.com

Training

SonicWall offers an extensive sales and technical training curriculum. SonicWall Training provides E-Training, instructor-led training, custom training, technical certifications, and uses authorized training partners.

For more information, visit:
https://support.sonicwall.com/training-product-select

Related Documentation

SonicWall technical documentation is available on MySonicWall and on the Support portal, including:

- SonicOS Administration Guides
- SonicOS Release Notes
- SonicOS Upgrade Guides
- SonicOS Configuration Guides
- SonicOS Deployment Guides
- SonicOS Reference Guides

For more information, visit:
https://support.sonicwall.com/sonicwall-supermassive-9000-series/9600/release-notes-guides

Additionally Supported Languages

SonicWall Getting Started Guides, Quick Start Guides, User Guides, appliance firmware, and various end-user clients are available in multiple languages.

After registering your product, you can check for applicable firmware or end-user client software on MySonicWall. New releases are posted as they become available, so please check periodically for additional firmware, software, and documents.

本地化固件和文档通知

SonicWall 《入门指南》、《快速入门指南》、《用户指南》、设备固件和多种终端用户客户端现已支持多种语言。请从 https://support.sonicwall.com/zh-cn 查找可用的中文文档。

请按照 《入门指南》或 《快速入门指南》中的说明，在 MySonicWall 网站 https://www.mysonicwall.com 注册您的设备。注册完成后，您可以在 MySonicWall 网站查看相应的固件和终端用户客户端软件。我们会在第一时间发布可用的新版本，请定期检查以获取最新的固件、软件和文档。

ローカライズ版ファームウェアおよびドキュメントについて

SonicWall 導入ガイド、クイック スタート ガイド、ユーザ ガイド、装置用ファームウェア、および多彩なエンドユーザ クライアントが複数の言語で利用できるようになりました。利用可能な日本語ドキュメントは、https://support.sonicwall.com/ja-jp をご覧下さい。

導入ガイドまたはクイック スタート ガイドの手順に沿って、MySonicWall (https://www.mysonicwall.com) で製品を登録します。製品の登録後に、利用可能なファームウェアまたはエンドユーザ クライアントを MySonicWall 上で確認できます。新しいリリースは利用可能になると公開されるので、ファームウェア、ソフトウェア、およびドキュメントを定期的に確認してください。

펌웨어 및 문서 한글화 안내

SonicWall Getting Started 가이드 , Quick Start 가이드 , 사용자 가이드 , 어플라이언스 펌웨어 및 다양한 엔드유져 클라이언트가 다국어를 지원합니다 . 다음에서 사용 가능한 한국어 문서를 찾아 보세요 ..

Getting Started 가이드 또는 Quick Start 가이드에 있는 절차에 따라 https://www.mysonicwall.com 에서 제품 등록을 하세요 . 제품 등록 후 , MySonicWall 에서 적용 가능한 한국어 펌웨어 또는 사용자 클라이언트 소프트웨어를 확인할 수 있습니다 . 새로운 버젼은 사용 가능할 때 등록됩니다 . 그러므로 , 추가되는 한국어 펌웨어 , 소프트웨어와 문서가 있는지 주기적으로 체크하세요 https://support.sonicwall.com/ko-kr.

Notificação de Firmware e Documentação Localizada

As Guias de noções básicas, Guias de início rápido, Guias de Usuário, firmware de aplicações, e varios clientes de usuário final de SonicWall estão agora disponíveis em varias línguas. Pode encontrar a documentação disponível em Português em https://support.sonicwall.com/pt-br.

Siga as instruções da Guia de noções básicas ou Guia de início rápido para registrar seu produto em MySonicWall no https://www.mysonicwall.com. Depois de registrar o produto, você pode procurar firmaware ou clientes de usuário final aplicáveis em MySonicWall. Novos lançamentos são publicados tão pronto estejam disponíveis, assim que por favor visite periodicamente esta página para ver firmware, software e documentos adicionais.

7

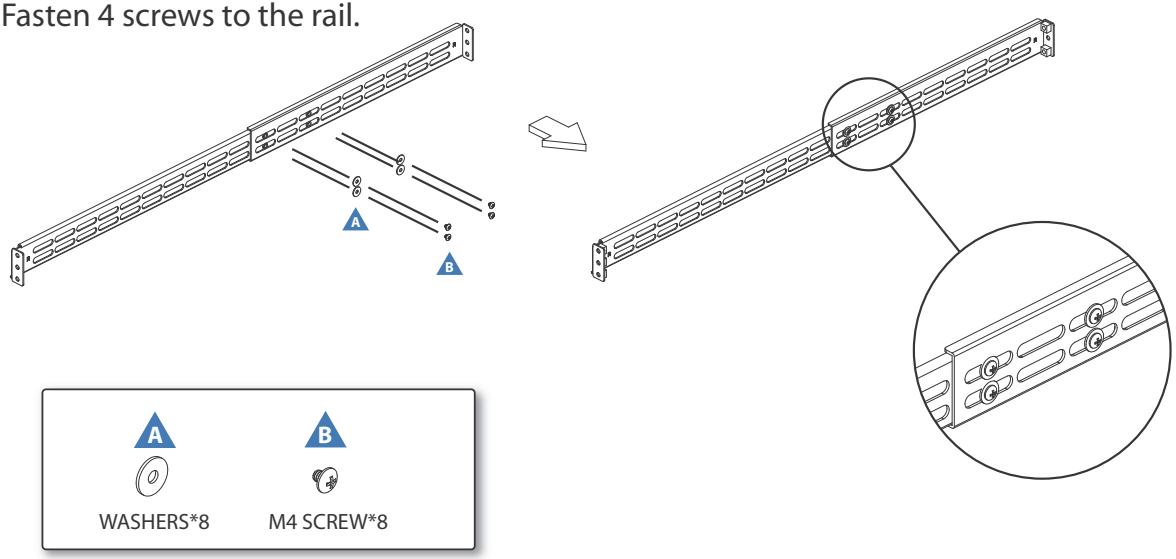
Rack Mounting Instructions

This section provides illustrated rack mounting instructions for SonicWall SuperMassive appliances. For safety information related to rack mounting and other aspects of product installation, see Product Safety and Regulatory Information on page 61.

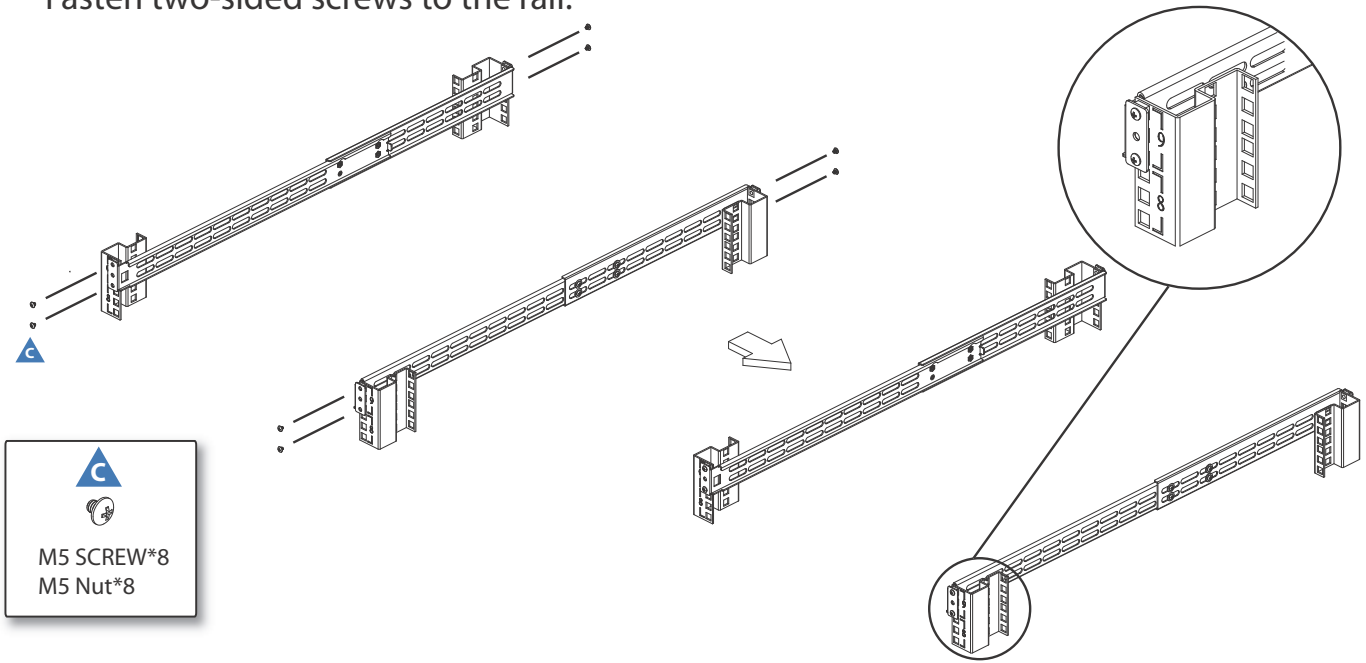
Rail Assembly and Rack Mounting

Assemble the Slide Rail

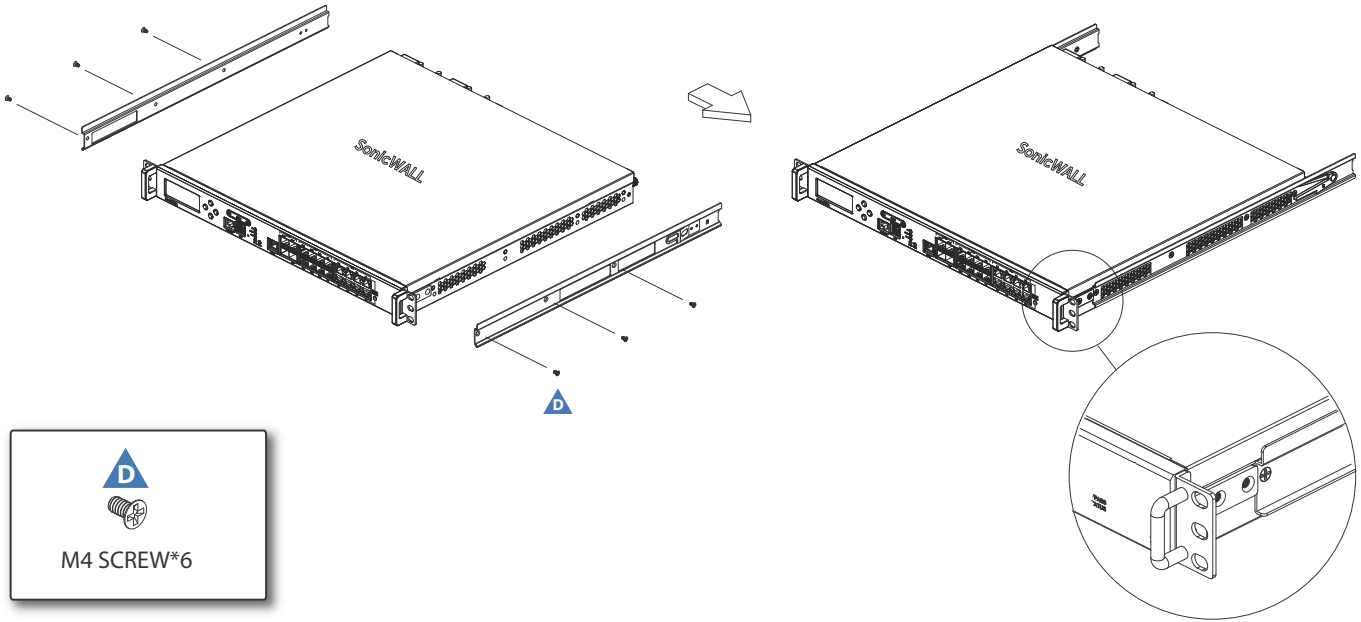
Fasten 4 screws to the rail.



Fasten two-sided screws to the rail.

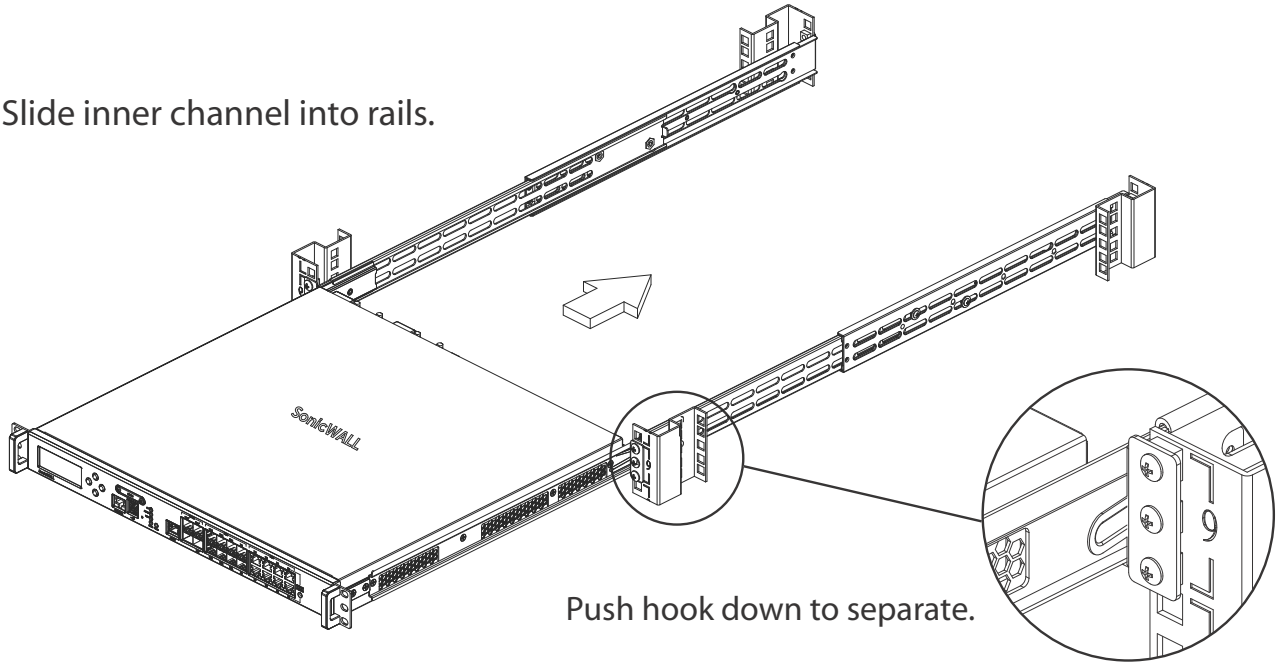


Fasten 6 screws to attach the inner channel onto the chassis.



Insert Chassis to Frame

Slide inner channel into rails.



Push hook down to separate.

Product Safety and Regulatory Information

This section provides product safety, regulatory, and warranty information.

Regulatory Model/Type	Product Name
1RK28-0A6	SuperMassive 9200
1RK28-0A7	SuperMassive 9400
1RK28-0A8	SuperMassive 9600

Safety Instructions

Installation Requirements

WARNING:

The following conditions are required for proper installation:

- The SonicWall appliance is designed to be mounted in a standard 19-inch rack mount cabinet.
- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application.
- Ensure that no water or excessive moisture can enter the unit.
- 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.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers.
- 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.
- 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.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- 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.
- Mount the SonicWall appliances evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.

- 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.
- 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.
- 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.
- 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.
- As shipped from the factory this SonicWall product includes two power supplies for redundant AC power and added reliability. A field conversion is available to convert to DC mains.
- To disconnect AC power, both power cords must be removed.
- 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.
- This model is shipped as AC mains configuration using standard 3 conductor appliance couplers. A field conversion is available to change to DC mains. The DC mains connector uses terminal posts with the polarity marked.
- To disconnect DC power, an external properly-related disconnect device must be provided by building or rack installation.
- Do not connect AC configured products to DC mains, and do not connect DC configured products to AC. Detailed instructions are provided with the DC conversion kit. Product must be configured as all DC or all AC.
- DC rating includes tolerances. Do not operate product outside of range shown on product label.
- DC configuration includes input cable with protective earthing conductor (Green and Yellow wire). This conductor is required to be connected to safety earth ground of circuit.
- Thumbscrews should be tightened with a tool after both installation and subsequent access to the rear of the product.

Warning—Potential Hazard from Fan

- Before replacing the fan unit, carefully read and follow the instructions provided with the unit.

Lithium Battery Warning

The Lithium Battery used in the SonicWall 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 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 appliance is located.

Sicherheitsanweisungen

Anforderungen an die Installation

Verwarnung:

Für eine ordnungsgemäße Montage sollten die folgenden Hinweise beachtet werden:

- Das SonicWall Modell ist für eine Montage in einem standardmäßigen 19-Zoll-Rack konzipiert.
- Vergewissern Sie sich, dass das Rack für dieses Gerät geeignet ist und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- 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.

- Achten Sie darauf, das sich die Netzwerkkabel nicht in der unmittelbaren Nähe von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern befinden
- 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.
- 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.
- 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.
- 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.
- Bringen Sie die SonicWall waagerecht im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- 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 Montageschien verwendet werden.
- Ein angemessen dimensionierter und geprüfte Sicherung, sollte Bestandteil der Haus-Installation sein. Bitte folgen die den lokalen Richtlinien beim Einkauf von Material oder Komponenten.
- 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.
- 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.
- Dieses Produkt wird mit zwei Wechselstrom-Netzteilen zur redundanten Stromversorgung fuer erhöhte Verfu¨gbarkeit ausgeliefert. Ein Umbaukit in Gleichstromversorgung ist verfu¨gbar

- Um den Wechselstrom (AC) zu unterbrechen muessen beide Stromkabel entfernt werden.
- 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.
- Die Wechselstrom Konfiguration verwendet standardisierte Kaltgerätekabel. Sie können einem Umbaukit für Gleichstrom bestellen. Der Gleichstrom (DC) Netzanschluss verwendet Polklemmen, bei denen die Polarität gekennzeichnet ist.
- Um den Gleichstrom (DC) zu unterbrechen, muss ein externes, ordnungsgemaess bewertetes Unterbrechungsgeraet durch die Stromzufuhr im Gebaeude oder das Rack zur Verfuegung gestellt werden.
- Schließen Sie kein Wechselstrom konfiguriertes Produkt an Gleichstrom an. Und schließen Sie kein Gleichstrom konfiguriertes Produkt an Wechselstrom an. Das Umbaukit beinhaltet eine detaillierte Beschreibung. Das Gerät muss komplett mit Gleichstrom oder Wechselstrom konfiguriert sein.
- Gleichstrom akzeptiert Toleranzen. Betreiben Sie das Gerät nicht außerhalb des Bereiches, der auf dem Aufkleber des Gerätes angegeben ist.
- Die Gleichstrom Konfiguration beinhaltet einen Anschlusskabel mit Erdung (Grün-Gelbes Kabel). Diese Kabel muss an den Erdungsschaltkreis angeschlossen werden.
- Vergewissern Sie sich, dass die Schrauben nach dem Austausch mit entsprechendem Werkzeug fest angezogen werden.

Achtung—Lüfter Potentielle Gefahrenquelle

- Lesen Sie vor dem Austausch der Lüftereinheit die Anleitung, die mit dem Gerät geliefert wurde und befolgen Sie die Anweisungen.

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 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 Appliance keine Kabel an, die aus dem Gebäude in dem sich das Gerät befindet herausgeführt werden.

安全說明

安裝要求

需要滿足以下條件以進行正確安裝：

- SonicWall 設備被設計成安裝在一個標準的 19 吋機架安裝櫃。
- 使用機架製造商推薦的裝載硬體，確認機架足夠裝置所需
- 請確認裝置內不會滲入水分或過多的濕氣。
- 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。
- 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。
- 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。

- 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)。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。
- 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。可用提供的地區電流轉換器轉換成直流電源。
- 要斷開交流電源，兩條電源線都必須被拔除。
- 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。
- 這個型號出貨時附帶的交流電源，是標準三芯器具耦合器的配置。可用提供的地區電流轉換器轉換成直流電源。
- 要斷開直流電源，必須有一個由建築物本身或機架安裝所提供的外部適當的額定斷路裝置。
- 不要把交流配置的產品連接到直流電源，也不要把直流配置的產品連接到交流電源。在直流轉換器套件中有詳細說明。產品必須設定為全直流或全交流。
- 直流讀數包括公差。不要在產品標籤標示的範圍以外操作產品。
- 直流配置包括帶有保護接地導體的輸入電纜（綠色和黃色電線）。此導體必須連接到安全接地電路。
- 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。

風扇潛在危險警告

- 更換風扇部件前，請仔細閱讀，並遵循所提供的指示。

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。

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)	-	O	O	O	O	O
機械部件 (風扇、散熱器等) (Mechanical parts (fan, heatsink etc.)	-	O	O	O	O	O
電路板組件 (PCBA)	-	O	O	O	O	O
電線 / 連接器 (Cable/connector)	-	O	O	O	O	O
電源設備 (power supply)	-	O	O	O	O	O
配件 (Accessories)	-	O	O	O	O	O
備考 1. “O” 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。						

SonicWall Support

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.

SuperMassive Getting Started Guide
Updated - February 2017
232-000344-50 Rev A

SONICWALL™