SonicWALL Email Security Solutions

EMAIL SECURITY | **SonicWALL Email Security**

SonicWALL Email Security 200, 300, 400, 500, 6000 Getting Started Guide

SONICWALL®

SonicWALL Email Security 200, 300, 400, 500, 6000 Getting Started Guide

This *Getting Started Guide* contains installation procedures and configuration guidelines for deploying a SonicWALL Email Security appliance on your network.

SonicWALL Email Security provides effective, high-performance and easy-to-use inbound and outbound email threat protection. Ideal for the small to medium size business, this self-running, self-updating solution delivers powerful protection against spam, virus and phishing attacks in addition to preventing leaks of confidential information. Combining anti-spam, anti-phishing, content filtering, policy management and content compliance capabilities in a single seamlessly integrated solution, SonicWALL Email Security solutions provide powerful protection without complexity.

Note: *SonicWALL TotalSecure Email provides complete protection from spam, virus attacks and phishing. Without TotalSecure Email, to use the spam and phishing protection provided by the SonicWALL Email Security appliance, you must have a subscription to SonicWALL Email Protection and Dynamic Support. If you need to purchase a subscription, contact your SonicWALL vendor.*

Please read this entire Getting Started Guide before setting up your SonicWALL Email Security 200, SonicWALL Email Security 300, SonicWALL Email Security 400, SonicWALL Email Security 500, or SonicWALL Email Security 6000 appliance.

Note: *An updated version of this guide may exist. Refer to SonicWALL's Documentation Web site for complete, updated documentation at:* <http://www.sonicwall.com/Support.html>.

Contents

This document contains the following sections:

1 Before You Begin

Check Package Contents

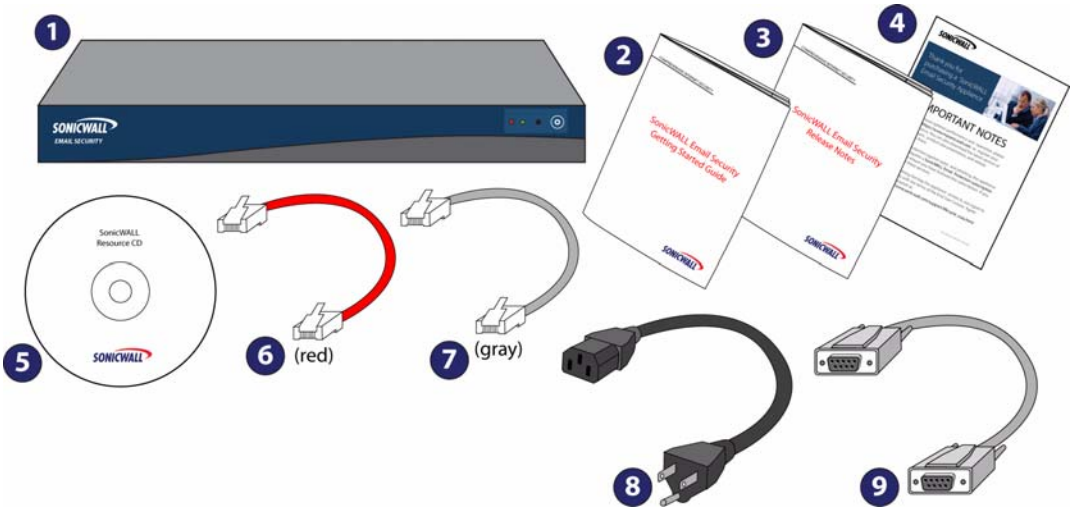
1. One SonicWALL Email Security appliance
2. One Getting Started Guide document
3. One Release Note document
4. One Thank You card
5. One SonicWALL Resource CD
6. One crossover cable (red)
7. One Ethernet cable (gray)
8. One power cord*
9. One RS232 CLI cable

Any Items Missing?

If any items are missing from your package, contact:
SonicWALL Support
<http://www.sonicwall.com/us/Support.html>
Email: customer_service@sonicwall.com

* *The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.*

* *Das eingeschlossene Netzkabel ist für Gebrauch in Nordamerikas nur vorgehabt. Für Europaïsche Union (EU) Kunden, ist ein Netzkabel nicht eingeschlossen.*



What You Need to Begin

- A computer to use as a management station for initial configuration of SonicWALL Email Security software
- Internet Explorer 5.0 or higher
- An Internet connection

Record Configuration Information

Before continuing, record the following configuration information for your reference:

Registration Information

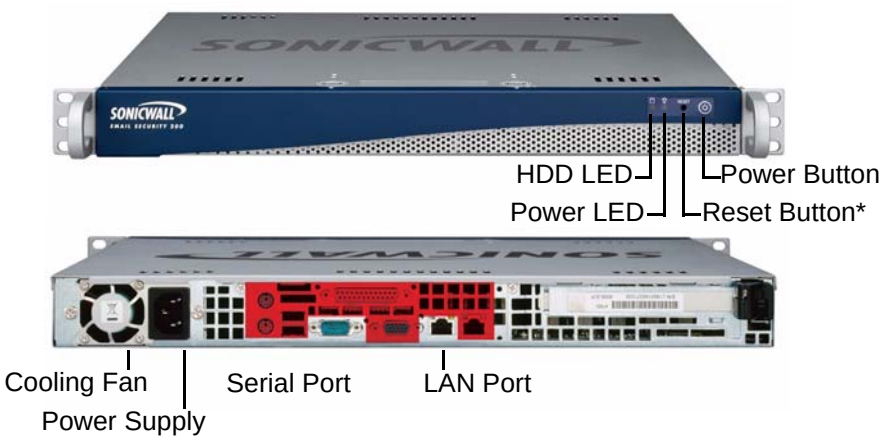
Serial Number: _____ (xxxxxx-xxxxxx)	Record the serial number found on the top right access panel of your SonicWALL Email Security appliance.
Authentication Code: _____ (xxx-xxx)	Record the authentication code found on the top right access panel of your SonicWALL Email Security appliance.

Networking Information

Email Security IP Address: _____	Select a free static IP address for your SonicWALL Email Security appliance that is within the range of your local subnet.
Email Security Subnet Mask: _____	Enter the subnet mask for the local subnet where you are installing your SonicWALL Email Security appliance.
Gateway IP Address: _____	Record the IP address of your network's gateway device (such as your perimeter firewall/router).
DNS Server 1: _____ **DNS Server 2** (optional): _____	Record your DNS Server information.
Host Name: _____	Record the fully qualified domain name within your network for your SonicWALL Email Security appliance (maximum 32 characters).
Password: _____	Select a password for your SonicWALL Email Security appliance (default is *password*).
Email Server IP: _____	Record the IP address or hostname of your email server.
LDAP Server IP: _____	Record the IP address or hostname of your directory services server, such as LDAP or Microsoft Active Directory.

Overview of the SonicWALL Email Security Appliance

SonicWALL Email Security Appliance



* Pressing the reset button for several seconds will result in a reboot of the SonicWALL Email Security appliance.

Alert: *Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty.*

HDD LED	Indicates data transfer to and from the hard disk drive.
Power LED	Indicates the SonicWALL Email Security appliance is powered on.
Reset Button	Allows reboot of the SonicWALL Email Security appliance.
Power Button	Allows the SonicWALL Email Security appliance to power on (one press) or power off.
Cooling Fan	Allows optimal air circulation.
Power Supply	Allows the SonicWALL Email Security appliance to connect to AC power using the supplied power cable.
LAN Port	Allows the SonicWALL Email Security appliance to connect to your local area network.
Serial Port	Allows you to connect directly to the appliance via terminal services to use the CLI.

2 Registering Your SonicWALL Email Security Appliance

Before you can use your SonicWALL Email Security appliance, you must first register your appliance and activate your licenses for the SonicWALL Email Protection Subscription and Dynamic Support.

This section contains the following sub-sections:

Before You Register

You need a mysonicwall.com account to register the SonicWALL Email Security appliance. If you already have a mysonicwall.com account, go to “Registering Your SonicWALL Email Security Appliance” on page 9 to register your appliance.

Note: *mysonicwall.com registration information is not sold or shared with any other company.*

Creating a mysonicwall.com Account

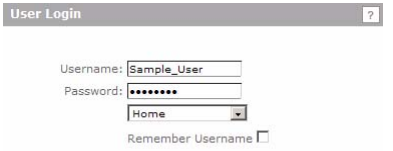
Creating a mysonicwall.com account is fast, simple, and FREE. Simply complete an online registration form.

1. In your Web browser, go to <https://www.mysonicwall.com/>.
2. In the User Login section, click **If you are not a registered user, Click here.**

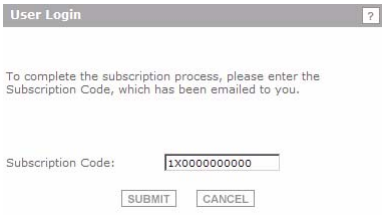
3. Enter the account information, personal information, and preferences and click **Submit**.

Note: *You must enter a valid email address.*

4. Follow the prompts to finish creating your account. SonicWALL will email a subscription code to the email address you entered in the personal information.
5. When you return to the login screen, log in with your new **username** and **password**.



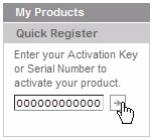
6. Confirm your account by entering the **subscription code** you received in the email.



Congratulations! You have created and logged into your mysonicwall.com account.

Registering Your SonicWALL Email Security Appliance

1. Locate your SonicWALL Email Security Software serial number. It should be printed on the label on the right-side of your SonicWALL Email Security appliance.
2. If you are not already logged into mysonicwall.com, go to <https://www.mysonicwall.com/> and log in.
3. Enter your serial number in the **Quick Register** field and click the small gray arrow. Follow the on-screen instructions.



4. Confirm your serial number, enter a friendly name for your appliance, and enter your authentication code in the **Quick Register > Add New Product** section.

5. Click REGISTER.
6. Follow the online prompts to fill out the survey and complete the registration process.

3 Initial Setup and Configuration

In this section, you will:

Apply Power to the SonicWALL Email Security Appliance

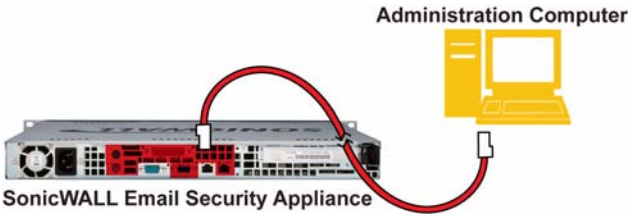
1. Plug the power cord into the back of the SonicWALL Email Security appliance and into an appropriate power outlet.
2. Turn on the power switch on the front, top, right corner of the appliance.

The Power LED on the front panel lights up green when you power on the SonicWALL Email Security appliance. The HDD LED lights up and may blink while the appliance performs a series of diagnostic tests. When the HDD LED is no longer lit, the SonicWALL Email Security appliance is ready for configuration.

Connect Directly to the SonicWALL Email Security Appliance

The SonicWALL Email Security appliance comes configured with an IP address of **192.168.168.169**. Before you can connect your management station to it, you must configure your management station to have an address in the same subnet.

1. Make a note of your computer’s current network settings.
2. Set the computer you use to manage the SonicWALL Email Security appliance to have a static IP address in the 192.168.168.x range, such as **192.168.168.50** and a netmask of **255.255.255.0**. For help with setting up a static IP address on your computer, refer to “Troubleshooting” on page 27.
3. Using the supplied crossover cable and the computer you are using to administer the SonicWALL Email Security appliance, connect the LAN port on the computer to the LAN port on the back of your SonicWALL Email Security appliance.



Login to the SonicWALL Email Security Appliance

1. Open a Web browser on the computer you are using to administer the SonicWALL Email Security appliance.
2. Enter **http://192.168.168.169** (the default IP address of the SonicWALL Email Security appliance) in the **Location** or **Address** bar. The SonicWALL Email Security Web management login screen displays.

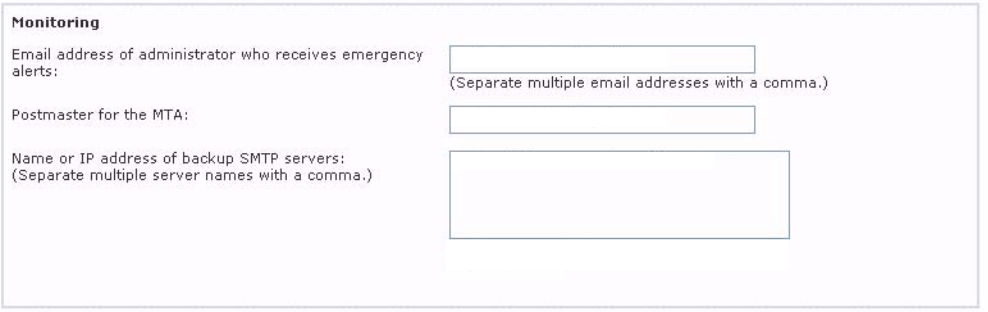
Note: *Depending on your browser settings, **one or more** security warnings may display while connecting to the Email Security Web management interface. Choose to accept the certificates in order to log into the SonicWALL Email Security appliance.*

3. Log into SonicWALL Email Security appliance using "**admin**" as the user name and "**password**" as the password.

Initial System Configuration

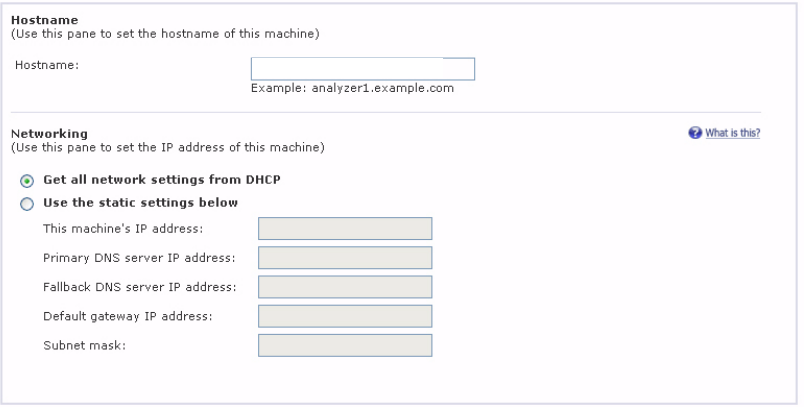
1. The first time you log in to the SonicWALL Email Security appliance, you are directed to the system configuration page. Configure your settings as follows:

Monitoring



Email address of the administrator who receives emergency alerts:	The email address of the mail server administrator. Enter the complete email address. For example, *user@example.com*
Postmaster for the MTA:	The email address of the Mail Transfer Agent administrator who will receive non-deliverable receipts. For example, *mail@example.com*
Name or IP address of backup SMTP servers:	Enter fully qualified domain names or IP addresses. For example, *mail2.example.com* or *10.100.0.1*

Hostname and Networking



Hostname:	Enter a hostname you can use within your network to address the SonicWALL Email Security appliance. Enter a fully qualified domain name. For example, *emailsecurity.example.com*
Get all network settings from DHCP:	Select this if you want your SonicWALL Email Security appliance to get dynamic IP settings from the DHCP server on your network.
Use the static settings below:	Select this to assign your SonicWALL Email Security appliance a static IP address. Enter: • This machine's IP address • Primary DNS server IP address (the local DNS server that has the MX record for your mail server) • Fallback DNS server IP address • Default gateway IP address • Subnet mask

Date and Time

System Date and Time:	Select the current year, month, day, hour, and minute.
Current Time Zone:	Displays the currently configured time zone.
Available Time Zones:	Select the time zone for your area.
Automatically Adjust for Daylight Savings Time:	Select this if your area observes Daylight Saving Time.

Note: *To ensure optimal network performance of your SonicWALL Email Security appliance, it is important that you select the proper time zone.*

2. Click the **Apply Changes** button to save this configuration. The appliance will reboot.
3. Disconnect the crossover cable from the SonicWALL Email Security appliance.
4. Reset your management computer's IP settings to work with your network. For example, if your network uses DHCP, reset your Local Area Connection to obtain an IP address and DNS settings dynamically from the server.
5. Reconnect your management computer to your network. You will use the network to access the SonicWALL Email Security appliance in the next steps.

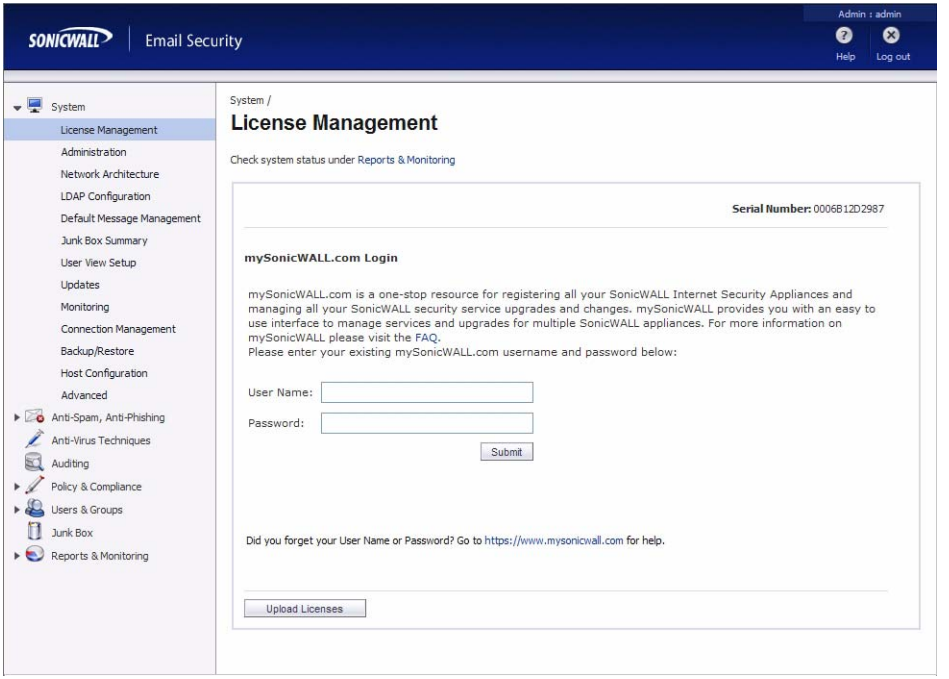
Activating the Email Security License Subscriptions

SonicWALL Email Security provides dynamic licensing, which allows you to activate your licenses by simply logging into your mysonicwall.com account. The mysonicwall.com server automatically uses the serial number and authentication code that came with your Email Security appliance.

Note: *If you purchased Total Secure Email, licensing is automatic and you do not need to take any action at all to activate your licenses.*

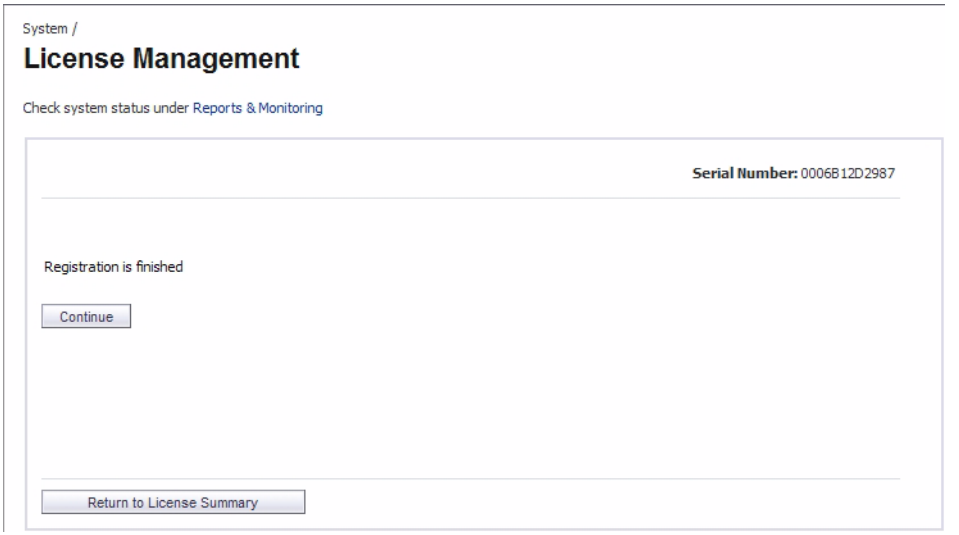
To activate Email Security license subscriptions:

1. Log in to the Email Security management interface.
2. In the System > License Management screen, type your mysonicwall.com **username** and **password** into the appropriate fields.

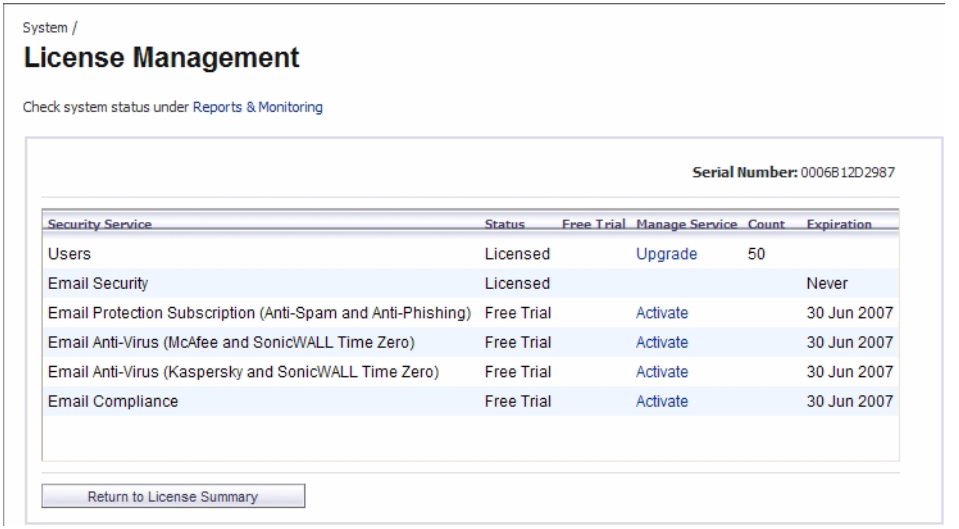


3. Click **Submit**.

4. In the next License Management screen, click **Continue**.



Licensing is now complete. The License Management screen displays the status, expiration date, and other information about your Email Security licenses.



4 Connecting and Configuring Network Settings

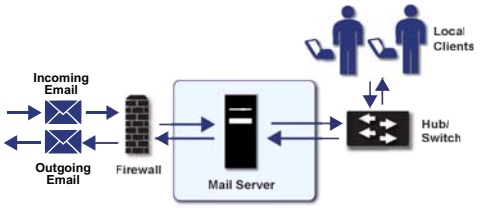
This section contains the following sub-sections:

Connecting the SonicWALL Email Security Appliance to Your Network

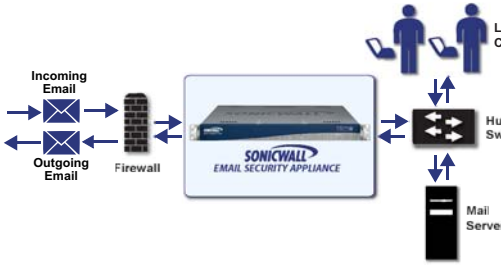
Your SonicWALL Email Security appliance is designed to operate in most network setups with minimal configuration. The diagrams below provide a "before" and "after" view of a network using SonicWALL Email Security.

Before and After

Mail Flow Before SonicWALL Email Security



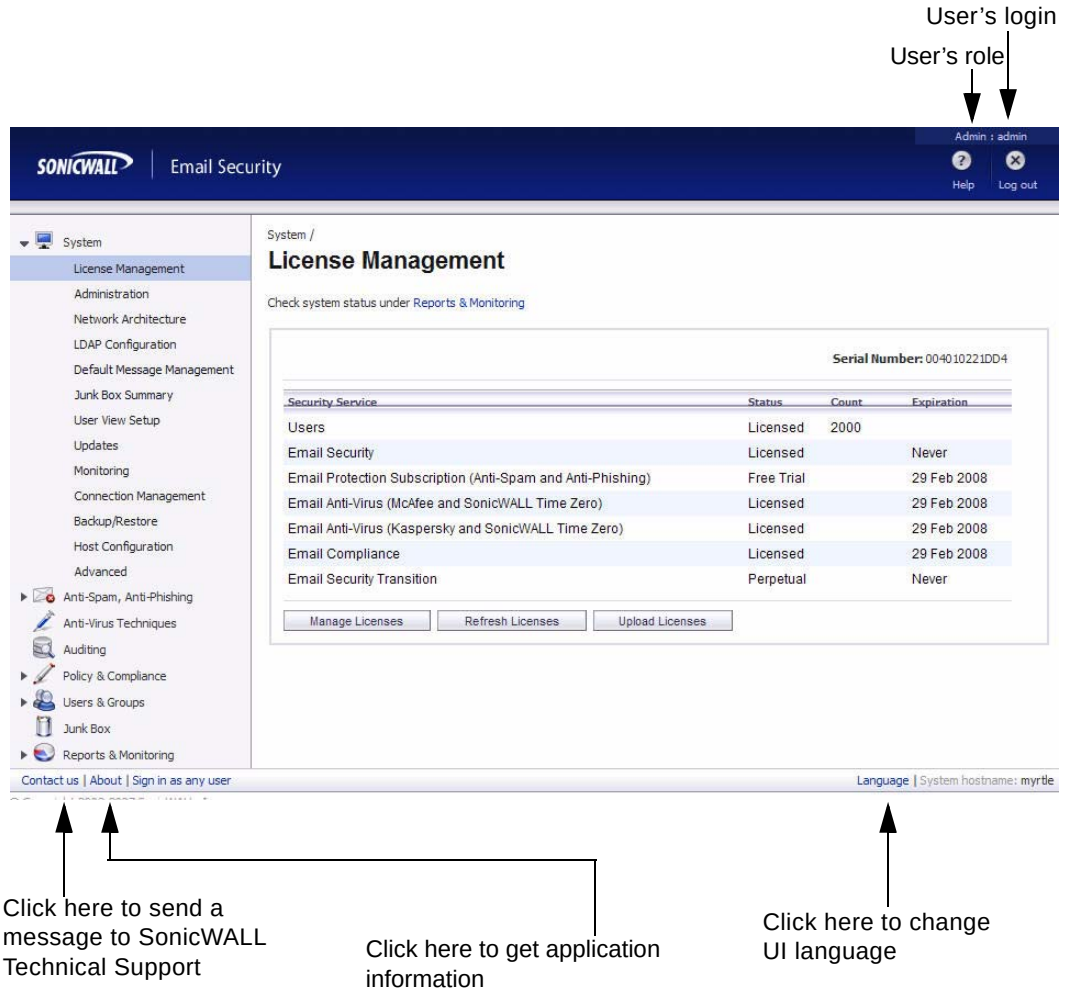
Mail Flow After SonicWALL Email Security



1. Plug one end of the provided Ethernet cable into the LAN port on the back of your SonicWALL Email Security appliance.
2. Plug the other end of the cable into an open port on your network hub or switch.

The SonicWALL Email Security Interface

This section describes how to navigate the SonicWALL Email Security Appliance user interface.



Change the Default Administrator Password

1. Login to the SonicWALL Email Security appliance using the IP address you entered in “Hostname and Networking” on page 13.
2. Navigate to the **System > Administration** page.
3. Enter a new management password into the **Password** field.
4. Enter it again in the **Confirm Password** field.
5. Click **Apply Changes**.

Using Quick Configuration to Set Up Email Management

The Quick Configuration page will walk you step-by-step through the configuration of your SonicWALL Email Security appliance. Use this window the first time you configure SonicWALL Email Security if you are installing SonicWALL Email Security as an All-In-One server and have only one downstream server.

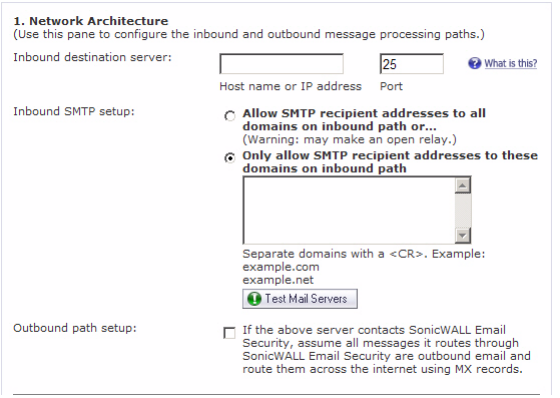
The information you enter for LDAP configuration is used to authenticate users as they log into their personal Junk Boxes.

Note: *For detailed configuration instructions, refer to the SonicWALL Email Security Administrator’s Guide.*

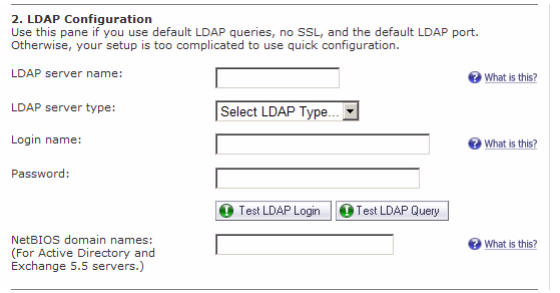
To use Quick Configuration:

1. Navigate to the **System > Administration** page.
2. Click **Click Here for Quick Configuration**.
3. In the Quick Configuration dialog box under **Network Architecture**, enter the host name or IP address and the port into the **Inbound destination server** fields.

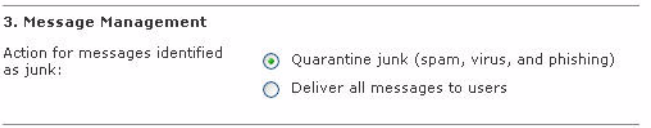
   The inbound destination server is the email server that will accept good email after SonicWALL Email Security removes and quarantines junk email. For example, this could be the IP address of a Microsoft Exchange server. The default port is 25.



4. For Inbound SMTP setup, select one of the following:
   - **Allow SMTP recipient addresses to all domains on inbound path or...**
     This option does not restrict incoming email to any domain.
   - **Only allow SMTP recipient addresses to these domains on inbound path**
     This option allows you to specify the domains to which incoming email will be delivered. In the text box, type the allowed domains one per line.
5. Optionally click **Test Mail Servers** to verify connectivity to the downstream Email Security server specified in preceding steps.
6. Select the **Outbound path setup** check box to route outbound email across the Internet using MX records.
7. Under LDAP Configuration, enter a hostname or IP address into the **LDAP server name** field.
   This is often your Exchange server or email server.



8. Select the type of LDAP server from the **LDAP server type** drop-down list.
9. Enter a valid LDAP login name and password into the **Login name** and **Password** fields. Click **What is this?** for more information.
10. Click **Test LDAP Login** and **Test LDAP Query** to verify your settings.
11. Enter one or more NetBIOS domain name in the **NetBIOS domain names** field. Click **What is this?** for more information.
12. Under Message Management, specify how junk mail will be handled by selecting one of the following:
    - **Quarantine junk** - sends junk mail to the user's junk box
    - **Deliver all messages to users** - does not separate junk mail from good email



13. Under Junk Box Summary, to send daily summary messages about junk mail caught by SonicWALL Email Security, select **Send daily summaries**.

14. To allow users to preview their junk mail messages with unjunking them, select **Users can preview their own quarantined junk mail**.

    Summaries will contain a preview link for each junk email.

15. Type the URL where users can view their email junk boxes in the **URL for user view** field. Click **Test this Link** to verify connectivity.
16. Under Updates, click **Test Connectivity to SonicWALL** to test your connection to mysonicwall.com for automated software updates.

17. Click **Apply Changes**.

5 Verification and Further Configuration

This section contains the following subsections:

Routing Mail to Your SonicWALL Email Security Appliance

In order for your SonicWALL Email Security appliance to start filtering and monitoring mail, you must re-route mail traffic through your SonicWALL Email Security appliance. Mail traffic must pass from the Internet to the appliance, and then the appliance sends the good mail on to your mail server.

You have two choices to route mail traffic to your SonicWALL Email Security appliance instead of to your mail server:

- Change the MX record in your DNS server to resolve to the IP address of your SonicWALL Email Security appliance. You may have to work with your ISP to change this record.
- Create a rule in your firewall or router to route all port 25 (SMTP mail) traffic to your SonicWALL Email Security appliance. Refer to your firewall or router documentation for instructions on creating rules to route traffic.

Verifying Mail from the Internet Through Your SonicWALL Email Security Appliance

1. Go to an external mail account, for example Yahoo mail or GMail.
2. Create a new email message:

To:	An email address where you receive email that is on the mail server for which you have configured the SonicWALL Email Security appliance.
Subject:	SonicWALL Email Security Verification Message
Body:	SonicWALL Email Security Verification Message

3. Send the message.
4. In the SonicWALL Email Security appliance administrative interface, click the **Auditing** button on the top.
5. Check the **Inbound** auditing reports to make sure the email appears as Delivered.
6. Check the mail account you sent the message to. If you received the message, you have correctly configured your SonicWALL Email Security appliance.

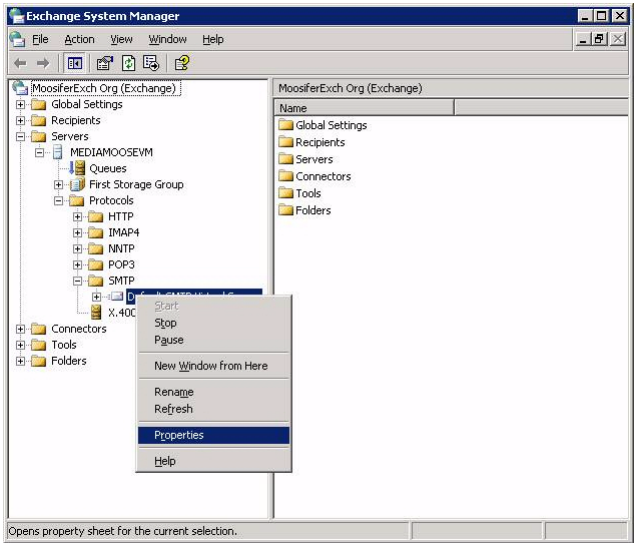
Configuring Outbound Mail Filtering

You can have your SonicWALL Email Security appliance filter outbound mail from your mail server to the Internet. To configure outbound mail filtering, you configure both your mail server and your SonicWALL Email Security appliance for the outbound mail path.

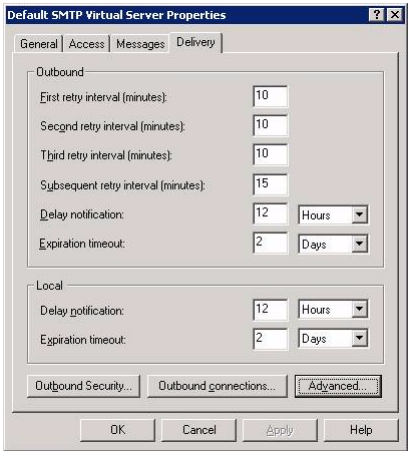
Configure the outbound mail destination of your mail server to point to the IP address or host name of your SonicWALL Email Security appliance. This is typically done by configuring a Smart Host on your mail server.

The configuration steps for Exchange Server 2003 are provided here. See the documentation on your mail server for specific instructions.

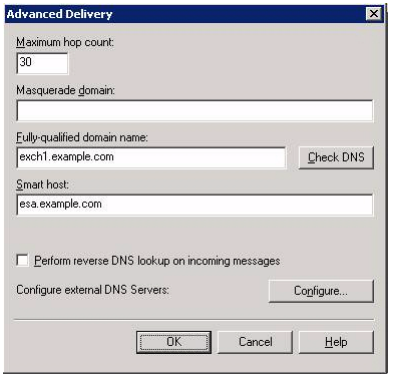
1. In the **Exchange System Manager**, navigate to **Servers > [servername] > Protocols > SMTP > Default SMTP Virtual Server** (or active server instance).
2. Right-click **Default SMTP Virtual Server**, and select **Properties**.



3. Browse to the **Delivery** tab, and click the **Advanced** button.



4. In the Smart Host field, enter the FQDN on your SonicWALL Email Security appliance (such as, esa.example.com). Note: The Exchange Server must be able to resolve this host name.



5. Click **OK**.

On your SonicWALL Email Security appliance, in the **Server Configuration > Network Architecture page**, configure a separate, outbound path to handle the outbound email flow at the appliance (if not already configured).

Configure the path to use the MTA (MX routing or SmartHost) under **Destination of Path**.

You need to configure something unique between the inbound and outbound path to distinguish inbound from outbound mail flow. A very simple way to do this is to have them listen on different ports or enter the IP address of the Exchange Server as the **Source IP Contacting Path** on the outbound path.

Example

Given this:

```
10.100.0.10: Exchange Server (exch1.example.com)
10.100.0.100: SonicWALL Email Security appliance (esa.example.com)
```

You might have two paths that look like this:

	Source IP	Listen On	Destination
Inbound	Any	Any:25	(proxy) exch1.example.com:25
Outbound	10.100.0.10	Any:25	MX

In this scenario, any message that arrives at the SonicWALL Email Security appliance from 10.100.0.10 will be treated as an outbound message, handed off to the MTA component in the system, which will deliver the message via MX-lookup on the domain in the **TO** field. Messages that arrive at the SonicWALL Email Security appliance from any other IP address will be treated as an Inbound message, and delivered directly to the Exchange server. The SonicWALL Email Security appliance always gives preference to specific matches (for example an exact IP address match takes precedence over “Any”).

Another example using port numbers to distinguish which path a message should take:

	Source IP	Listen On	Destination
Inbound	Any	Any:25	(proxy) exch1.example.com:25
Outbound	Any	Any:2525	MX

Another alternative would be to assign your SonicWALL Email Security appliance multiple IP addresses, and have it listen on one for inbound and one for outbound.

In all of the above cases, the admin will configure Exchange to deliver outbound email to the IP address and port number where the SonicWALL Email Security appliance is listening for outbound mail.To test your SonicWALL Email Security appliance, click the **Auditing** button at the top of the SonicWALL Email Security appliance user interface and search for your sent email to verify it has been sent and received.

Troubleshooting

This section contains the following subsection:

- Configuring a Static IP Address

Configuring a Static IP Address

Complete the following section based on your operating system in order to configure your management computer with a static IP address:

Windows XP

1. From the **Start** menu, highlight **Connect To** and then select **Show All Connections.**
2. Open the **Local Area Connection Properties** window.
3. Double-click **Internet Protocol (TCP/IP)** to open the **Internet Protocol (TCP/IP) Properties** window.
4. Select **Use the following IP address** and type **192.168.168.50** in the **IP address** field.
5. Type **255.255.255.0** in the **Subnet Mask** field.
6. Click **OK** for the settings to take effect.

Windows 2000

1. From your Windows **Start** menu, select **Settings**.
2. Open **Network and Dial-up Connections**.
3. Click **Properties**.
4. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Use the following IP address** and type **192.168.168.50** in the **IP address** field.
6. Type **255.255.255.0** in the **Subnet Mask** field.
7. Click **OK** for the settings to take effect.

Windows NT

1. From the **Start** menu, highlight **Settings** and then select **Control Panel**.
2. Open **Network**.
3. Double-click **TCP/IP** in the **TCP/IP Properties** window.
4. Select **Specify an IP Address** and type **192.168.168.50** in the **IP address** field.
5. Type **255.255.255.0** in the **Subnet Mask** field.
6. Click **OK**, and then click **OK** again.
7. Restart the computer for the changes to take effect.

Rack Mounting the SonicWALL Email Security 200 / 300 / 400 / 500 / 6000 Appliance

The above SonicWALL appliances are designed to be mounted in a standard 19-inch rack mount cabinet. The following conditions are required for proper installation:

- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application.
- 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.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104º F (40º C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters and broadband amplifiers.
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- 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.
- Mount the SonicWALL appliances evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- 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.

Weitere Hinweise zur Montage der Modell

Die oben genannten SonicWALL-Modelle sind für eine Montage in einem standardmäßigen 19-Zoll-Rack konzipiert. Für eine ordnungsgemäße Montage müssen die folgenden Bedingungen erfüllt werden:

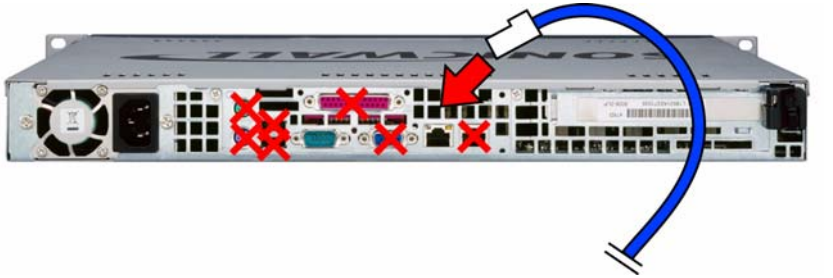
- Vergewissern Sie sich, dass das Rack für die Anwendung geeignet ist, und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an. Montieren Sie das Gerät so, dass sich die Anordnung der Montagelöcher mit den Löchern der Träger im 19-Zoll-Rack deckt.
- 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.
- Führen Sie die Kabel nicht entlang von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern.
- Das eingeschlossene Netzkabel ist für Gebrauch in Nordamerikas nur vorgehabt. Für Europaïsche Union (EU) Kunden, ist ein Netzkabel nicht eingeschlossen.
- 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.
- Bringen Sie die SonicWALL gerade im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- 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.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist. Insbesondere muss auf nicht direkte Anschlüsse an Stromquellen geachtet werden wie z. B. bei Verwendung von Mehrfachsteckdosen.

SonicWALL Email Security Appliance Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
1RK0F-04A, 1RK0E-041	Email Security 200 Email Security 300
1RK0F-04B, 1RK0E-041	Email Security 400 Email Security 500

Unauthorized Ports

Do not plug devices into any ports (other than those indicated) unless explicitly instructed to do so by a SonicWALL technical support representative. Doing so may void your warranty.



FCC Part 15 Class A Notice

Note: *This equipment was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. And if not installed and used in accordance with the instruction manual, the device may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.*

Notice About Modifying Equipment

Alert: *Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment.*

BMSI Statement

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，
可能會造成射頻干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－ A

Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à toutes la norme NMB-003 du Canada.

CISPR 22 (EN 55022) Class A

Complies with EN 55022 Class A and CISPR22 Class A.

Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Declaration of Conformity

Application of council Directive	Directive 89/336/EEC (EMC) and 72/23/EEC (LVD)

Declaration of Conformity

Standards to which conformity is declared	EN 55022 (1998) Class A EN 55024 (1998) EN 61000-3-2 (2000) + A2 EN 61000-3-3 (1995) + A1 EN 60950-1 (2001) +A11 National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

Regulatory Information for Korea

All products with country code “” (blank) and “A” are made in the USA.

All products with country code “B” are made in China.

All products with country code “C” or “D” are made in Taiwan R.O.C.

All certificates held by NetSonic, Inc.

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

Lithium Battery Warning

The Lithium Battery used in the SonicWALL Internet security appliance may not be replaced by the user. The SonicWALL 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 Internet security appliance must be disposed of, do so following the battery manufacturer's instructions.

Cable Connections

All Ethernet 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 is located.

German Language Regulatory and Safety Instructions

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 herausgeführt werden, in dem sich das Gerät befindet.

Copyright Notice

Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Java is a trademark or registered trademark of Sun Microsystems, Inc. om the U.S. or other countries.

Apache Tomcat is a trademark of Apache Software Foundation.

Firebird is a registered trademark of the Firebird Foundation, Inc.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

SonicWALL GPL Source Code

GNU General Public License (GPL)

SonicWALL will provide a machine-readable copy of the GPL open source on a CD. To obtain a complete machine-readable copy, please send your written request, along with a certified check or money order in the amount of US $25.00 payable to “SonicWALL, Inc.” to:

General Public License Source Code Request

SonicWALL, Inc. Attn: Jennifer Anderson

1143 Borregas Ave.

Sunnyvale, CA 94089

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

PN: 232-001159-00