▷ COMPREHENSIVE INTERNET SECURITY™

SonicWALL Email Security Appliances

SonicWALL Email Security 200 / 300 / 400 / 500 Getting Started Guide

SONICWALL

SonicWALL Email Security 200, 300, 400, 500 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: *In order 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, or SonicWALL Email Security 500 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/documentation.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

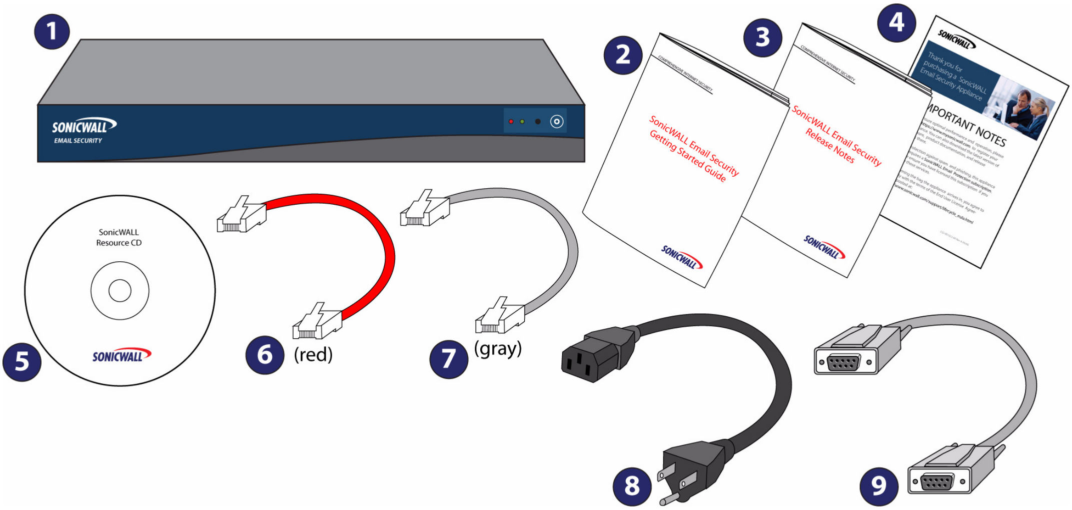
* *The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.*

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

Any Items Missing?

If any items are missing from your package, contact:

SonicWALL Support
Web: <http://www.sonicwall.com/support/>
Email: customer_service@sonicwall.com


1
SONICWALL
EMAIL SECURITY
2
SonicWALL Email Security Getting Started Guide
SONICWALL
3
SonicWALL Email Security Release Notes
SONICWALL
4
SONICWALL
Thank you for purchasing a SonicWALL Email Security Appliance
IMPORTANT NOTES
5
SonicWALL Resource CD
SONICWALL
6
(red)
7
(gray)
8
9

What You Need to Begin

- A computer to use as a management station for initial configuration of the SonicWALL Email Security appliance
- A Web browser supporting Java and HTTP uploads. Internet Explorer 5.0 or higher, Netscape Navigator 4.7 or higher, Mozilla 1.7 or higher, or Firefox are recommended
- An Internet connection

Record Configuration Information

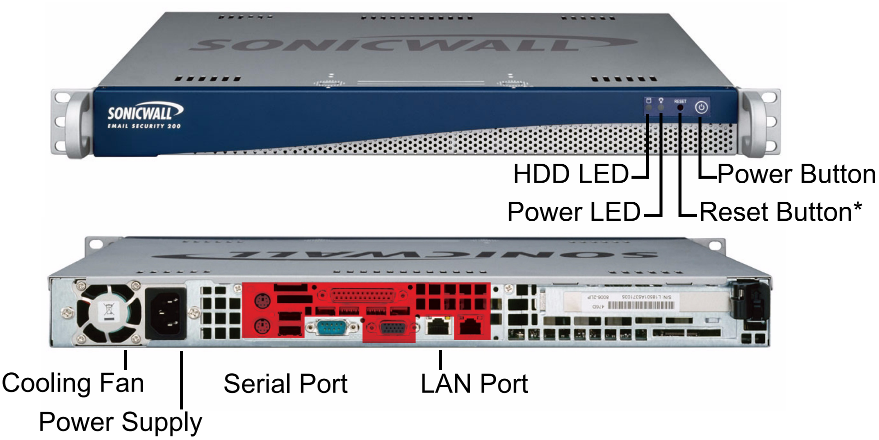
Before continuing, record the following configuration information for your reference:

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: __________________________	An easy to remember name for your SonicWALL Email Security appliance (maximum 32 characters).
Password: ___________________________	Select a password for your SonicWALL Email Security appliance (default is *password*).
Serial Number: _______________________	Record the serial number found on the back of your SonicWALL Email Security appliance.
Authentication Code: __________________	Record the authorization code found on the back of your SonicWALL Email Security appliance.
Email Server IP: ______________________	IP address of your email server.
LDAP Server IP: ______________________	IP address 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.

Before You Register

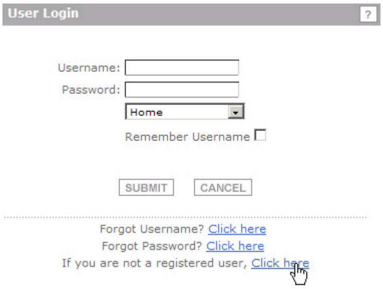
You need a mysonicwall.com account to register the SonicWALL Email Security appliance. If you already have a mysonicwall.com account, go to “Registering Your SonicWALL Email Security Appliance” on page 7 to register your appliance.

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 the “Click here” link in “If you are not a registered user, Click here.”



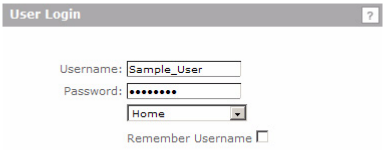
Forgot Username? Click here
Forgot Password? Click here
If you are not a registered user, Click here

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.



User Login

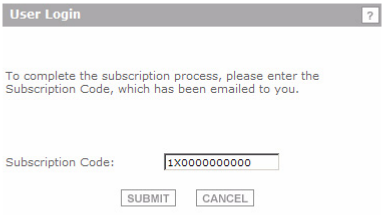
Username: Sample_User

Password: ••••••••

Home

Remember Username □

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



User Login

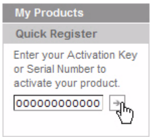
To complete the subscription process, please enter the Subscription Code, which has been emailed to you.

Subscription Code: 1X0000000000

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.



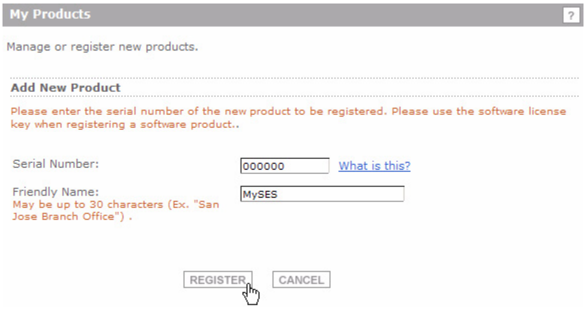
My Products

Quick Register

Enter your Activation Key or Serial Number to activate your product.

000000000000

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.



My Products

Manage or register new products.

Add New Product

Please enter the serial number of the new product to be registered. Please use the software license key when registering a software product..

Serial Number: 000000 What is this?

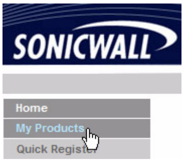
Friendly Name: MySES

May be up to 30 characters (Ex. "San Jose Branch Office") .

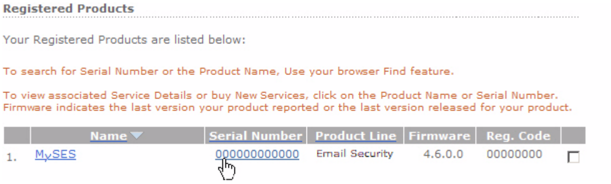
5. Click REGISTER .
6. Follow the online prompts to fill out the survey and complete the registration process.

Activating Your SonicWALL Email Protection Subscription and Dynamic Support

1. When you purchased your subscription to SonicWALL Email Protection Subscription and Dynamic Support, you should have received an activation code. If you have not purchased a subscription, contact your SonicWALL Sales representative.
2. If you are not already in the **Service Management** page, click on **My Products**.



Then click on the name or serial number link of your SonicWALL Email Security appliance in the Registered Products list to continue to the Applicable Services section.



Registered Products

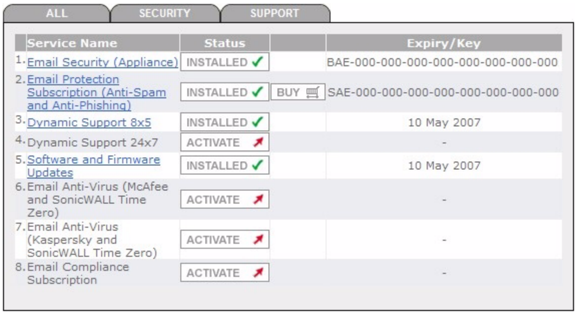
Your Registered Products are listed below:

To search for Serial Number or the Product Name, Use your browser Find feature.

To view associated Service Details or buy New Services, click on the Product Name or Serial Number.
Firmware indicates the last version your product reported or the last version released for your product.

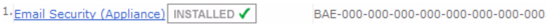
	Name	Serial Number	Product Line	Firmware	Reg. Code	
1.	MySES	000000000000	Email Security	4.6.0.0	00000000	□

3. The Applicable Services table should list all the services you purchased with your SonicWALL Email Security appliance.



	Service Name	Status		Expiry/Key
1.	Email Security (Appliance)	INSTALLED ✓		BAE-000-000-000-000-000-000-000-000
2.	Email Protection Subscription (Anti-Spam and Anti-Phishing)	INSTALLED ✓	BUY	SAE-000-000-000-000-000-000-000-000
3.	Dynamic Support 8x5	INSTALLED ✓		10 May 2007
4.	Dynamic Support 24x7	ACTIVATE		-
5.	Software and Firmware Updates	INSTALLED ✓		10 May 2007
6.	Email Anti-Virus (McAfee and SonicWALL Time Zero)	ACTIVATE		-
7.	Email Anti-Virus (Kaspersky and SonicWALL Time Zero)	ACTIVATE		-
8.	Email Compliance Subscription	ACTIVATE		-

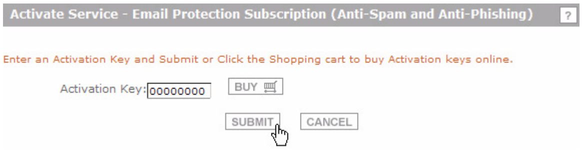
The services that are already activated will display with INSTALLED ✓ and a 27-character license key.


1. Email Security (Appliance) INSTALLED ✓ BAE-000-000-000-000-000-000-000-000

If a service you purchased a license for is not activated, click ACTIVATE next to the service to activate it.

Note: *If your Email Protection Subscription service is not installed, you must activate it in order to use the spam and phishing protection in your SonicWALL Email Security appliance.*

4. Locate your activation codes. They should be sets of 8 alpha-numeric characters in the format XXXXXXXX.
5. Enter the activation code for the service in the **Activation Key field** and click **Submit**.


Activate Service - Email Protection Subscription (Anti-Spam and Anti-Phishing)

Enter an Activation Key and Submit or Click the Shopping cart to buy Activation keys online.

Activation Key: 00000000

6. The Service Name table will list a 27 digit alpha-numeric license key for the service in the format XXX-XXX-XXX-XXX-XXX-XXX-XXX-XXX-XXX. Record this key.
7. Repeat this for each service you want to activate.
8. Copy the license keys in the Service Name table and either paste them into a text file or word processing document, or write them down here. You will need them to activate them locally on your appliance.

License Keys:

____

____

3 Setting Up the SonicWALL Email Security Appliance

In this section, you will:

- “Apply Power to the SonicWALL Email Security Appliance” on page 10
- “Connect Directly to the SonicWALL Email Security Appliance” on page 10
- “Login to the SonicWALL Email Security Appliance” on page 11
- “Change the Default Administrator Password” on page 13
- “Enter the License Keys for Each Service” on page 14

Apply Power to the SonicWALL Email Security Appliance

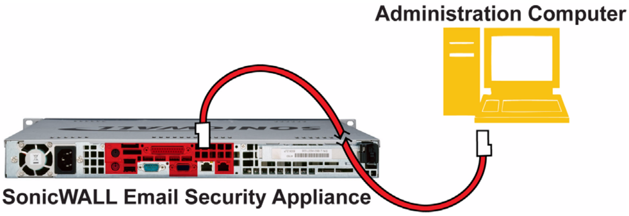
1. Plug the power cord into the back of the SonicWALL Email Security appliance and into an appropriate power outlet.
2. Turn on the power switch on the front, top, right corner of the appliance.

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

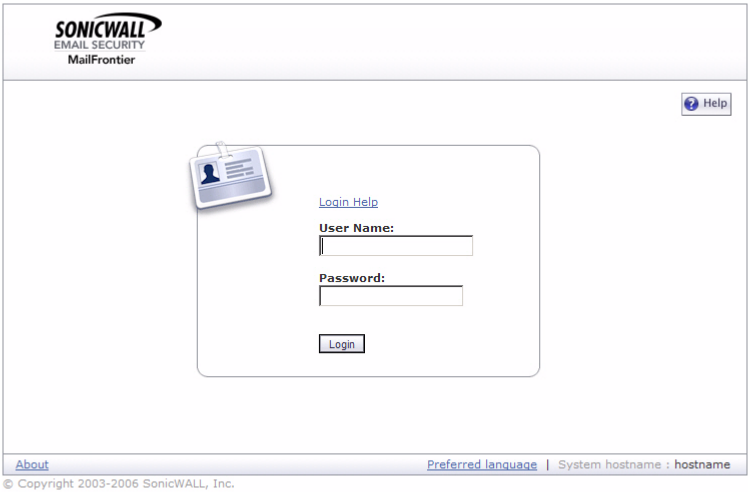
The SonicWALL Email Security appliance comes configured with an IP address of **192.168.168.169**. Before you can connect your management station to it, you must configure your management station to have an address in the same subnet.

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 “Configuring a Static IP Address” on page 30.
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

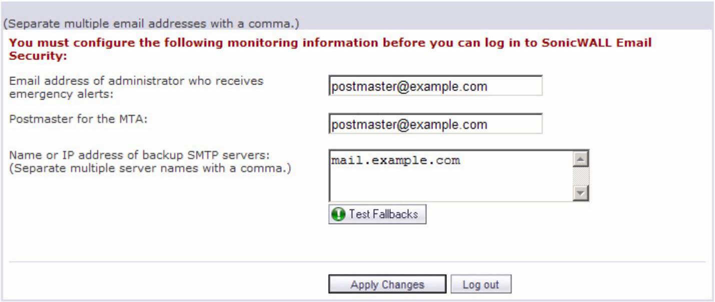
1. Open a Web browser on the computer you are using to administer the SonicWALL Email Security appliance.
2. Enter **http://192.168.168.169** (the default IP address of the SonicWALL Email Security appliance) in the **Location** or **Address** bar. The SonicWALL Email Security Web management login screen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


SONICWALL
EMAIL SECURITY
MailFrontier
Help
Login Help
User Name:
Password:
Login
About
Preferred language | System hostname : hostname
© Copyright 2003-2006 SonicWALL, Inc.

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.

4. The first time you log in to the SonicWALL Email Security appliance, you must configure the monitoring settings before you can use the administrative interface:



(Separate multiple email addresses with a comma.)

You must configure the following monitoring information before you can log in to SonicWALL Email Security:

Email address of administrator who receives emergency alerts: postmaster@example.com

Postmaster for the MTA: postmaster@example.com

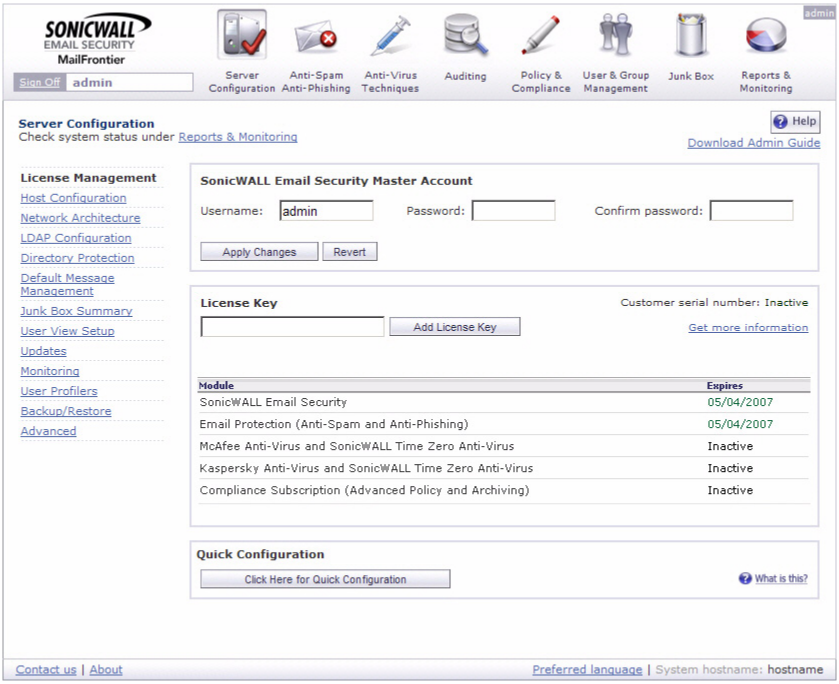
Name or IP address of backup SMTP servers: (Separate multiple server names with a comma.) mail.example.com

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. Enter the complete email address. For example, *user@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*.

5. Click **Apply Changes**. The License Management page should display.

Navigate the SonicWALL Email Security Interface

The SonicWALL Email Security administration interface has eight buttons across the top of the screen. Each button corresponds to a different set of management topics. Each button brings up a set of management pages you can navigate with a menu in the left column. When you select a different button at the top, the left-navigation menu changes. At all times in the management interface, one button is selected and one page in the left-navigation menu is selected.



Server Configuration
Check system status under Reports & Monitoring

SonicWALL Email Security Master Account

Username: admin Password: Confirm password:

License Key

Customer serial number: Inactive

Module	Expires
SonicWALL Email Security	05/04/2007
Email Protection (Anti-Spam and Anti-Phishing)	05/04/2007
McAfee Anti-Virus and SonicWALL Time Zero Anti-Virus	Inactive
Kaspersky Anti-Virus and SonicWALL Time Zero Anti-Virus	Inactive
Compliance Subscription (Advanced Policy and Archiving)	Inactive

Quick Configuration

System hostname: hostname

Change the Default Administrator Password

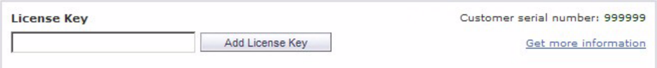
When you first log into the SonicWALL Email Security appliance the **Server Configuration > License Management** page displays.

To change the management password:

1. Enter a new management password into the **Password** field.
2. Enter it again in the **Confirm Password** field.
3. Click **Apply Changes**.

Enter the License Keys for Each Service

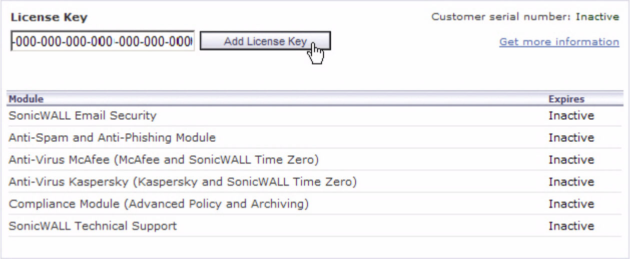
1. Enter each license key for a service in the **License Key** field.
2. Click the **Add License Key** button.



License Key

Customer serial number: 999999

3. Repeat this step for each license key. The **Module** table will display the licensing status of each service you enter a key for.



License Key -000-000-000-000-000-000-000

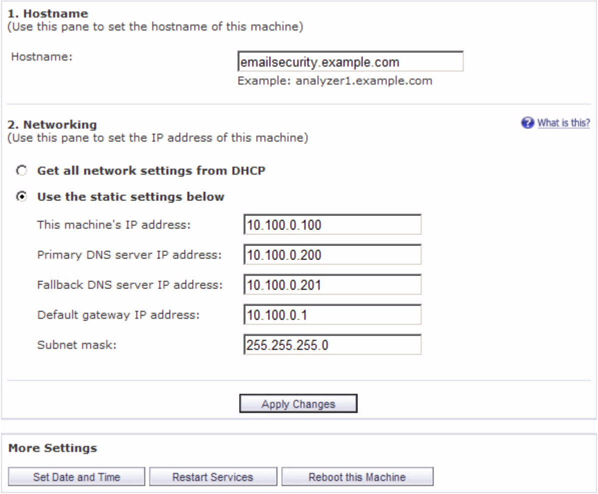
Customer serial number: Inactive

Module	Expires
SonicWALL Email Security	Inactive
Anti-Spam and Anti-Phishing Module	Inactive
Anti-Virus McAfee (McAfee and SonicWALL Time Zero)	Inactive
Anti-Virus Kaspersky (Kaspersky and SonicWALL Time Zero)	Inactive
Compliance Module (Advanced Policy and Archiving)	Inactive
SonicWALL Technical Support	Inactive

4 Setting Up Network Configuration

Before you connect your SonicWALL Email Security appliance to your network, you need to set up the network configuration on the appliance:

1. In the left navigation menu, click on **Host Configuration**. The **Server Configuration > Host Configuration** page displays.



1. Hostname
(Use this pane to set the hostname of this machine)

Hostname: emailsecurity.example.com
Example: analyzer1.example.com

2. Networking
(Use this pane to set the IP address of this machine)

○ **Get all network settings from DHCP**

● **Use the static settings below**

This machine's IP address:	10.100.0.100
Primary DNS server IP address:	10.100.0.200
Fallback DNS server IP address:	10.100.0.201
Default gateway IP address:	10.100.0.1
Subnet mask:	255.255.255.0

More Settings

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

2. Click Apply Changes.

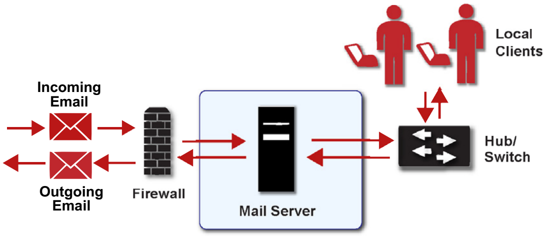
3. Disconnect the crossover cable from the SonicWALL Email Security appliance.
4. Reset your management computer’s IP settings to work with your network. For example, if your network uses DHCP, reset your Local Area Connection to obtain and IP address and DNS settings dynamically from the server.
5. Reconnect your management computer to your network. You will use the network to access the SonicWALL Email Security appliance in the next steps.

5 Connecting the SonicWALL Email Security Appliance to Your Network

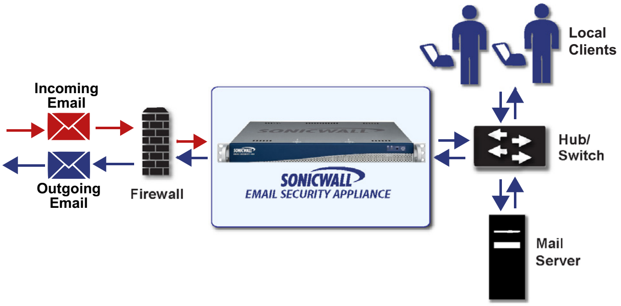
Your SonicWALL Email Security appliance is designed to operate in most network setups with minimal configuration. The following instructions guide you through the process of connecting the SonicWALL Email Security appliance to your network. The diagrams below provide a "before" and "after" view of a 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.

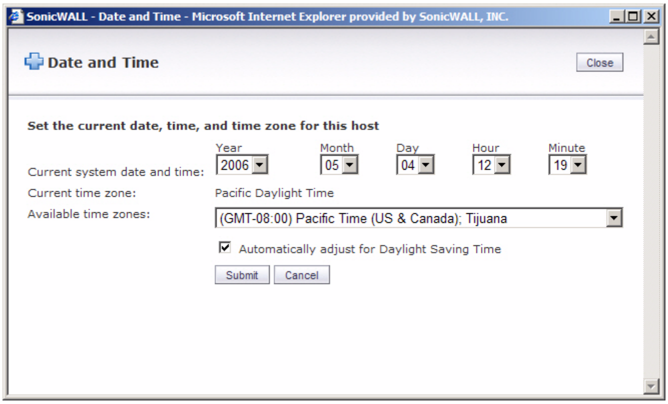
6 Configuring the SonicWALL Email Security Appliance

In this section, you will:

- “Set the Time and Date” on page 18
- “Use Quick Configuration to Set Up Email Management” on page 19

Set the Time and Date

1. Under **Server Configuration** click **Host Configuration** in the left column.
2. At the bottom of the **Server Configuration > Host Configuration** page, under **More Settings**, click Set Date and Time. The Date and Time window displays:



SonicWALL - Date and Time - Microsoft Internet Explorer provided by SonicWALL, INC.

Date and Time

Set the current date, time, and time zone for this host

Current system date and time: Year 2006, Month 05, Day 04, Hour 12, Minute 19

Current time zone: Pacific Daylight Time

Available time zones: (GMT-08:00) Pacific Time (US & Canada); Tijuana

☑ Automatically adjust for Daylight Saving Time

Current system date and time:	Select the current year, month, day, hour, and minute. The minute starts at 0 seconds when you click **Submit**.
Available time zones:	Select the time zone for your area. It is important to communication with the SonicWALL registration server that you select the correct time zone.
Automatically adjust for Daylight Saving Time	Select this if your area observes Daylight Saving Time.

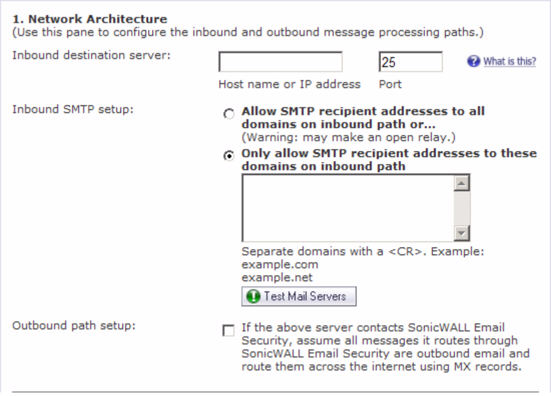
3. Click Submit to apply your settings.

Use 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. More options for these settings are available in the other Server Configuration pages.

Click at the bottom of the **Server Configuration > License Management** page to launch the **Quick Configuration** page.

1. In the **Network Architecture** section, configure the inbound and outbound message processing paths:



1. Network Architecture
(Use this pane to configure the inbound and outbound message processing paths.)

Inbound destination server: [ ] Host name or IP address [25] Port — What is this?

Inbound SMTP setup:
○ **Allow SMTP recipient addresses to all domains on inbound path or...** (Warning: may make an open relay.)
● **Only allow SMTP recipient addresses to these domains on inbound path**
Separate domains with a <CR>. Example:
example.com
example.net

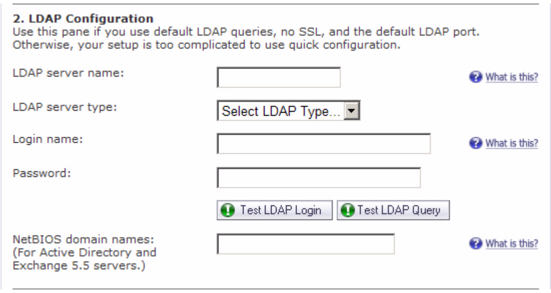
Outbound path setup:
□ If the above server contacts SonicWALL Email Security, assume all messages it routes through SonicWALL Email Security are outbound email and route them across the internet using MX records.

Inbound destination server:	This is the hostname (or IP address) and port number of 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 most common port number is 25.

Inbound SMTP setup:	Select one of the following inbound SMTP setups:
	• **Allow SMTP recipient addresses to all domains on inbound path**
	• **Only allow SMTP recipient addresses to these domains on inbound path**
	Enter the domains you are permitting. Separate domains with a <CR>. Example:
	`example.com`
	`example.net`
	Click Test Mail Servers to test communication with the domains you entered.

Outbound path setup:	If the above server contacts SonicWALL Email Security, assume all messages it routes through SonicWALL Email Security are outbound email and route them across the internet using MX records.

2. In the **LDAP Configuration** section, configure:



2. LDAP Configuration

Use this pane if you use default LDAP queries, no SSL, and the default LDAP port. Otherwise, your setup is too complicated to use quick configuration.

LDAP server name:

LDAP server type: Select LDAP Type...

Login name:

Password:

NetBIOS domain names: (For Active Directory and Exchange 5.5 servers.)

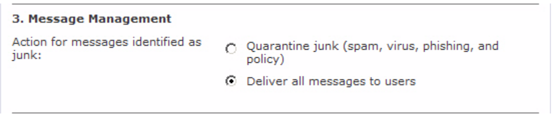
LDAP server name:	This is the hostname or IP address of the LDAP server. In many instances, this is the name of your Exchange server or your email server. Use the Test LDAP Login button to try out various combinations of server name, login name, and password, until you find one that succeeds. **Note:** SonicWALL Email Security uses your existing Active Directory or LDAP server to authenticate end users as they log in to their personal junk boxes. This LDAP configuration page must be correctly filled out to return the complete list of users who are allowed to log in to their junk box. If a user does not appear in this list, their email is filtered, but they cannot log in to their personal junk box.
LDAP server type:	Select one: • **Active Directory** • **Lotus Domino** • **Exchange 5.5** • **Sun ONE iPlanet** • **Other**

Login name:	Many LDAP servers are configured to provide the list of users to anyone who asks. This is called **Anonymous Bind**. The administrator should first select that option, then click on the **Test LDAP Login** button to test it.
	If **Anonymous Bind** does not work, the administrator will need to provide a username and password to get LDAP to return the list of users. Often this can be the login information of an existing, regular user on the network. It probably will not need to be a network administrator.
	Examples of how to fill out this field:
	1) **Active Directory** - In a Microsoft Windows environment running Active Directory or Exchange 2000 or later, the login name will commonly be of the form “domain\username” like:
	`sales\john`
	`<password>`
	2) **Exchange 5.5** - In a Microsoft Windows environment authenticating against Exchange 5.5 or earlier, the login name will commonly be of the form "CN=username" such as:
	`CN=john`
	`<password>`
	3) **Lotus Notes/Domino** - When authenticating against a Lotus LDAP server, the login name will commonly be of the form "username" such as:
	`john`
	`<password>`
	4) **SunOne / iPlanet** - When authenticating against a SunOne or iPlanet LDAP server, the login name can either be the exact string "CN=Directory Manager" or a user's X.400 style login (both examples below):
	`CN=Directory Manager`
	`<password> (for the Directory Manager account)`
	... or ...
	`UID=john,OU=people,O=example.com,O=internet`
	`<password> (for John)`
	Use the **Test LDAP Login** button to try out various combinations until you find one that succeeds.

Password:	Password for the account entered above

NetBIOS domain names:	In a Microsoft Windows environment, users are grouped under **NT Domains** and they are authenticated against the one particular **NT Domain** they are grouped in. Whatever list is specified here is offered as a pull-down menu to users on the Login page. The intent is to provide users who are used to logging in to their Microsoft Windows computers the identical interface they are normally presented with. The effect is that the **NT Domain** string is prepended to their login name when doing authentication. Example: The administrator adds both **sales** and **engr** to the **Domain List**. Then when a user named **JohnS** with email address **JohnS@example.com** logs in, he will be presented with a pull down menu. If he chooses "sales", and types "JohnS" as his login name, the real login name that is passed to Active Directory for authentication is "sales\johns".

3. In the **Message Management** section, configure:

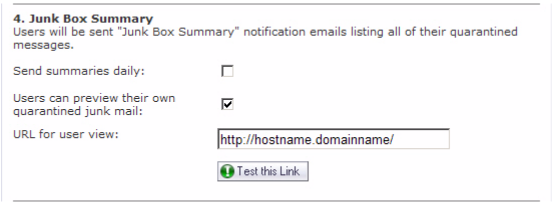


3. Message Management

Action for messages identified as junk: ○ Quarantine junk (spam, virus, phishing, and policy) ● Deliver all messages to users

Action for messages identified as junk:	Select to quarantine all junk mail or deliver all mail to users.

4. In the **Junk Box Summary** section, configure:



4. Junk Box Summary
Users will be sent "Junk Box Summary" notification emails listing all of their quarantined messages.

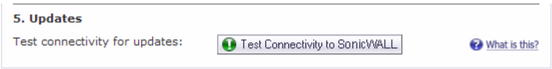
Send summaries daily: □

Users can preview their own quarantined junk mail: ☑

URL for user view: http://hostname.domainname/

Send summaries daily:	If checked, users receive daily summary messages of junk mail caught by the SonicWALL Email Security appliance. If unchecked, summary messages are not sent.
Users can preview their own quarantined junk mail:	If checked, users can preview junk mail messages without unjunking them. If they receive summaries, the summaries will contain a preview link for each junk email.
URL for user view:	The URL users can follow to view their own email junk box.

5. In the **Updates** section, configure:



5. Updates
Test connectivity for updates:

Test connectivity for updates:	Click this to test your connection to mysonicwall.com for automated software updates.

6. Click Apply Changes .

7 Verification and Further Configuration

In this section, you will:

- “Verify Your SonicWALL Email Security Appliance Configuration” on page 25
- “Route Mail to Your SonicWALL Email Security Appliance” on page 26
- “Verify Mail from the Internet Through Your SonicWALL Email Security Appliance” on page 26
- “Configure Outbound Mail Filtering” on page 27

Verify Your SonicWALL Email Security Appliance Configuration

Now that you have completed the configuration of your SonicWALL Email Security appliance, verify that you can send email messages to your mail server.

To test this you need to send a message from the SonicWALL Email Security appliance to a mail account that you have access to on your mail server. In order to send the message from the appliance, you will telnet into the appliance and send a message from the command line.

1. Start a Telnet session to port 25 on your SonicWALL Email Security appliance: In the Windows **Start** menu, select **Run**, and enter:

   ```
   telnet <ip address> 25
   ```

   where <*ip address*> is the address of your SonicWALL Email Security appliance. For example:

   ```
   telnet 10.100.0.100 25
   ```

2. Send an email to your email address. The following is an example of how to send an email over Telnet. The bold text is text that you enter.

   ```
   helo example.com
   250 emailsecurity.example.com
   mail from:<other-name@example.com>
   250 2.1.0 other-name@example.com....Sender OK
   rcpt to:<my-name@example.com>  (your email address on your mail server)
   250 2.0.0 Ok
   data
   354 3.0.0 End Data with <CR><LF>.<CR><LF>
   Subject: EMAIL SECURITY TEST

   This is a test of the email security test

   .
   250 2.6.0 <US0EXF01ZFuwft6aHev000187f5@emailsecurity.example.com> Queued
   mail for delivery quit
   ```

3. If you receive the email, you have successfully configured the SonicWALL Email Security appliance.

Route 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.

Verify 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.

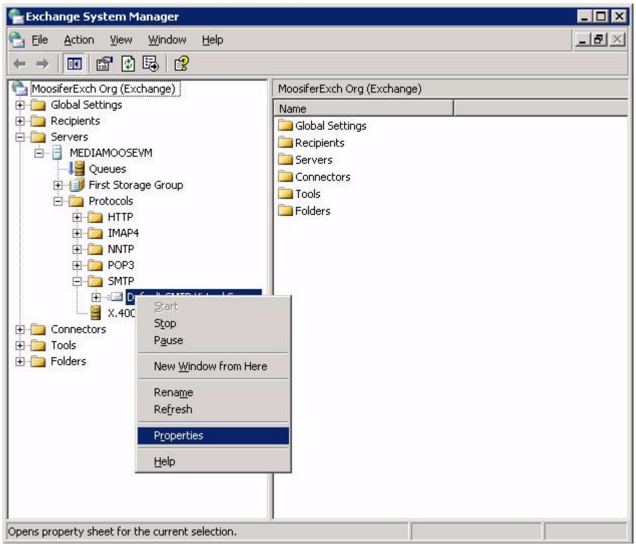
Configure Outbound Mail Filtering

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.

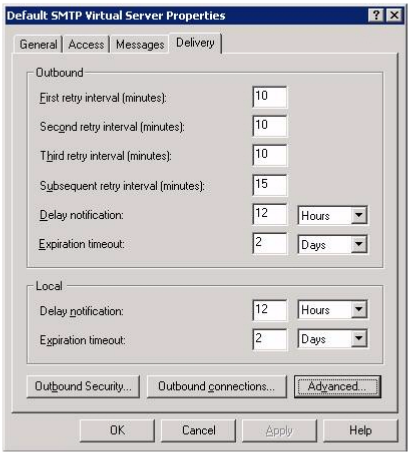
The configuration steps for Exchange Server 2003 are provided here. See the documentation on your mail server for specific instructions.

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



Opens property sheet for the current selection.

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



Default SMTP Virtual Server Properties

Outbound

First retry interval (minutes): 10

Second retry interval (minutes): 10

Third retry interval (minutes): 10

Subsequent retry interval (minutes): 15

Delay notification: 12 Hours

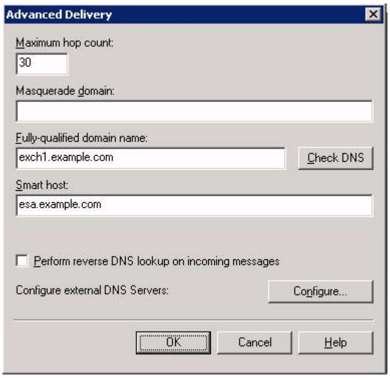
Expiration timeout: 2 Days

Local

Delay notification: 12 Hours

Expiration timeout: 2 Days

3. 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.



Advanced Delivery

Maximum hop count: 30

Masquerade domain:

Fully-qualified domain name: exch1.example.com

Smart host: esa.example.com

☐ Perform reverse DNS lookup on incoming messages

Configure external DNS Servers:

4. 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.

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 our 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.

Congratulations! You have successfully set up and tested your SonicWALL Email Security appliance operation.

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.

Mounting the SonicWALL Email Security 200 / 300 / 400 / 500

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:

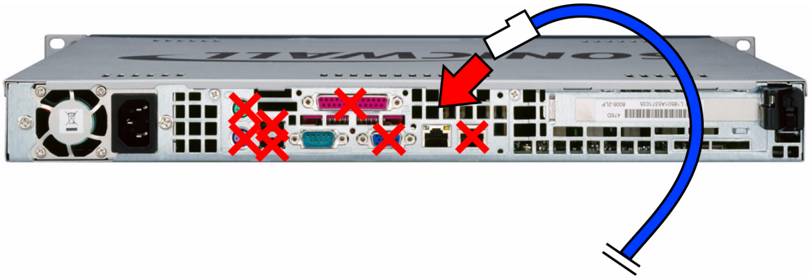
- Vergewissern Sie sich, dass das Rack für die Anwendung geeignet ist, und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an. Montieren Sie das Gerät so, dass sich die Anordnung 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.



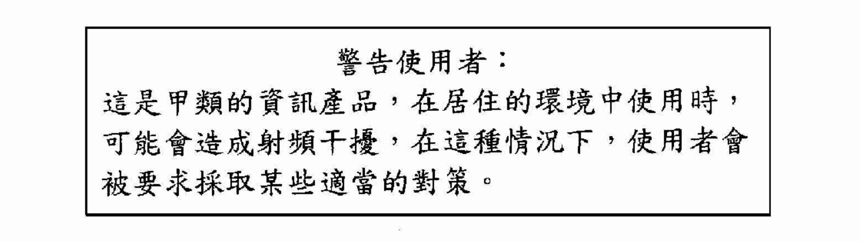
FCC Part 15 Class A Notice

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

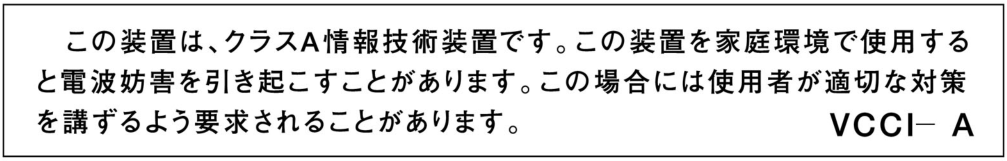
Alert: *Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user's authority to operate this equipment.*

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

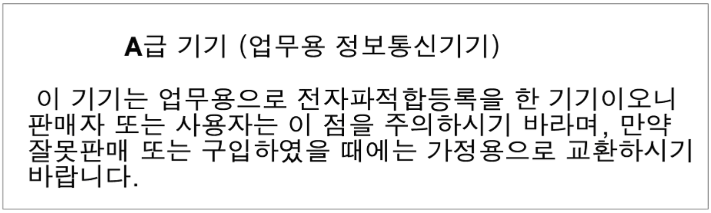
Regulatory Information for Korea

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

Notes

Notes

Notes

SonicWALL, Inc.

1143 Borregas Avenue T: 408.745.9600 www.sonicwall.com
Sunnyvale, CA 94089-1306 F: 408.745.9300

P/N 232-000467-00
Rev B 5/06

SONICWALL