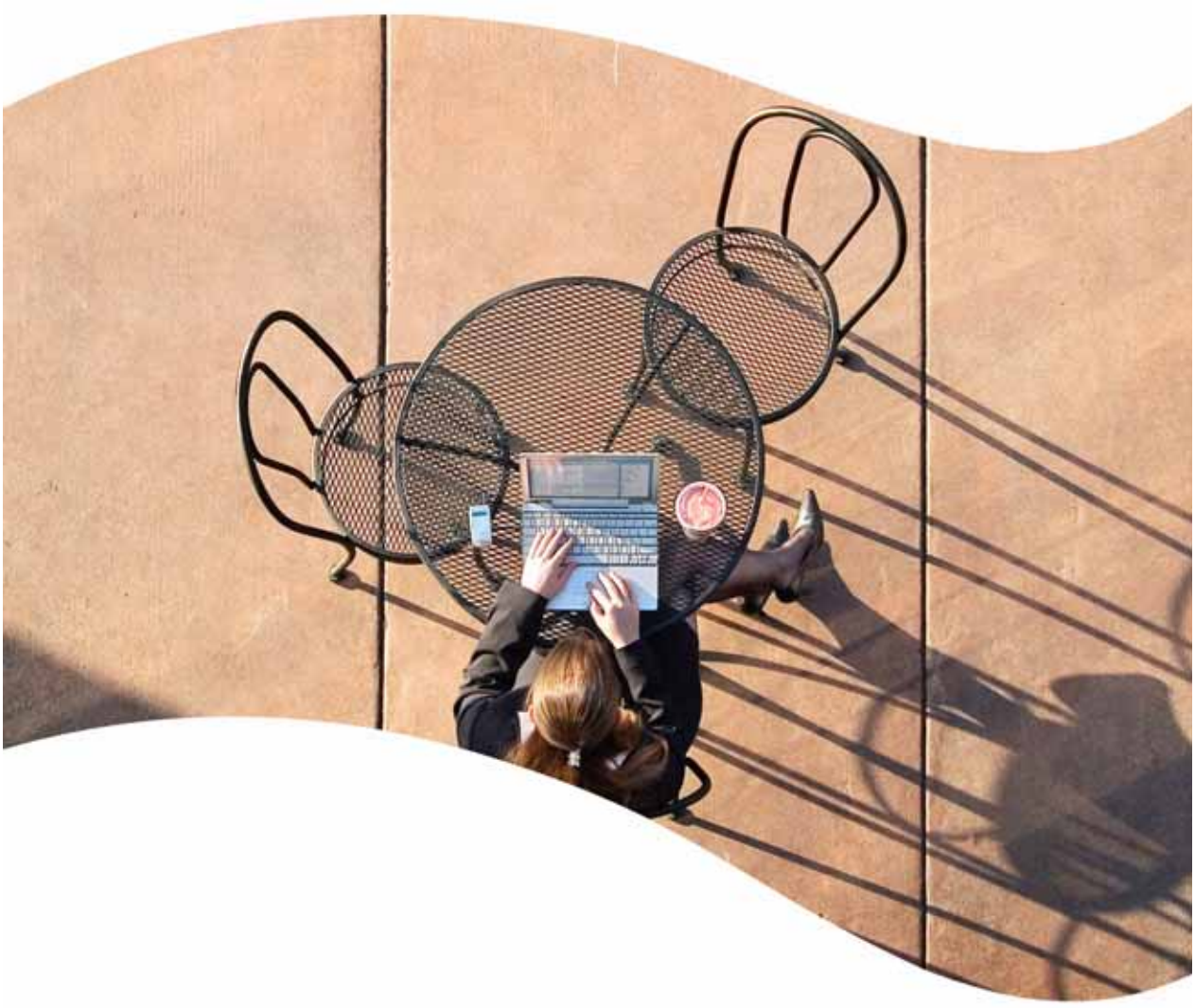
SonicWALL Email Security 4.6 Administrator's Guide

Note: This guide contains out-dated illustrations and references to Mail Frontier. This is currently being updated to the new SonicWALL Email Security product name.

SONICWALL



SonicWALL® Email Security Administrator's Guide

Version **4.6**

SonicWALL, Inc.
1143 Borregas Avenue
Sunnyvale, CA 94089-1306
Phone: +1.408.745.9600
Fax: +1.408.745.9300
E-mail: info@sonicwall.com

Copyright Notice

Trademarks

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

NOTE**:** The SonicWALL Email Security software service is an annual subscription which is subject to the terms and conditions of SonicWALL, Inc.'s applicable subscription agreement and includes:

Product updates, SonicWALL threat signature updates, and standard technical support for one (1) year from the date of purchase.

SonicWALL Email Security Appliances are integrated hardware and software solutions, which include SonicWALL Email Security software. SonicWALL Email Security Appliances are subject to the terms and conditions of SonicWALL, Inc.'s applicable license agreement. Updates to the SonicWALL Email Security software, SonicWALL Spam Signature Updates, and technical support may be purchased on an annual basis. AntiVirus support is optionally available.

Table of Contents

Preface

SonicWALL's email threat protection solution is a dynamic, self-learning, and self-running system, providing IT departments with the protection they need for inbound and outbound email. SonicWALL Email Security Gateway offers redundancy, comprehensive reporting and central administration across multiple data centers. The solution scales for organizations with 10 employees to enterprises with 100,000 or more employees.

About this Guide

This guide describes how to configure SonicWALL Email Security Gateway software for Enterprise and Small Business Editions, and the SonicWALL Email Security Gateway Appliance. Information that is specifically about SonicWALL Email Security Gateway Appliance or SonicWALL Email Security Gateway, Small Business Edition, is indicated by a footnote at the bottom of the page.

Documentation Conventions

Font	Meaning
Bold	Terms you see in a SonicWALL Email Security window
Italic	Variable names
`Courier`	Text on a command line
`Bold Courier`	Text that you type in a command line

Documentation Overview

SonicWALL Email Security provides the following documents to help in the installation, administration, and use of its products to protect email users from phishing, spam, viruses, and to manage the security policies you define for your organization.

Who Should Read this?	Document Name
All Administrators, and Product Evaluators	FAQ Whitepapers
Network and System Administrators	*SonicWALL Email Security Quick Start Guide* *Read Me First for Appliance Administrators* *SonicWALL Email Security's Administrator Guide* SonicWALL Email Security KnowledgeBase: go to http://mailfrontier.com/support
Email Users	*SonicWALL Email Security's User Guide* Two-page Introduction Pamphlet

You can find these documents on http://mailfrontier.com/support_overview.jsp and find product information on http://mailfrontier.com/press_resources.html and http://mailfrontier.com/support_asg_faq.html.

NOTE: To download SonicWALL Email Security's manuals, you must obtain a user ID and password from SonicWALL.

Finding Online Help

Click the **What is this?** button for in-depth online help on a specific area of the SonicWALL Email Security Gateway interface.

Click the **Help** button on any UI web page for information on how to use the UI features on that page.

CHAPTER 1

Planning SonicWALL Email Security Gateway Deployment

You must determine the appropriate architecture for SonicWALL Email Security Gateway before you deploy it in your network. This section discusses the different modules available in SonicWALL Email Security Gateway and network topology planning.

SonicWALL Email Security Gateway and Mail Threats

SonicWALL Email Security Gateway determines that an email fits *only one* of the following threats: Spam, likely Spam, Phishing, likely Phishing, Virus, likely Virus, Policy Violation, or Directory Harvest Attack (DHA). It uses the following precedence order when evaluating threats in email messages:

- DHA
- Virus
- Policy
- Phishing
- Likely Phishing
- Spam
- Likely Spam
- Likely Virus

For example, if a message is both a virus and a spam, the message will be categorized as a virus since virus is higher in precedence than spam.

If SonicWALL Email Security Gateway determines that the message is *not* any of the above threats, it is deemed to be good email and is delivered to the destination server.

Licensing SonicWALL Email Security Modules

SonicWALL Email Security provides multiple modules to protect an organization's email gateway.

When you purchase SonicWALL Email Security Gateway software or an appliance the following modules are licensed.

- Anti-Spam
- Anti-Phishing
- Policy Management
- Outbound (not available for Small Business Edition)
- Split Mode Configuration (not available for Small Business Edition)

In addition, you can optionally license one or more of the following modules for an additional cost:

- SonicWALL Email Security Time Zero Virus protection + Zombie Detection + McAfee™ Anti-Virus Engine
- SonicWALL Email Security Time Zero Virus protection + Zombie Detection + Kaspersky™ Anti-Virus Engine

SonicWALL Email Security recommends that you deploy SonicWALL Email Security Gateway with one or both of the anti-virus modules to provide the best protection and email management capabilities for your organization's inbound and outbound email traffic.

Defining SonicWALL Email Security Gateway Deployment Architecture

SonicWALL Email Security Gateway can be configured in two ways:

- **All in One:** In this configuration, all machines running SonicWALL Email Security Gateway analyze email, quarantine junk mail, and allow for management of administrator and user settings. See Figure 1.1, "All in One Architecture," on page 5 for a typical **All in One** configuration.

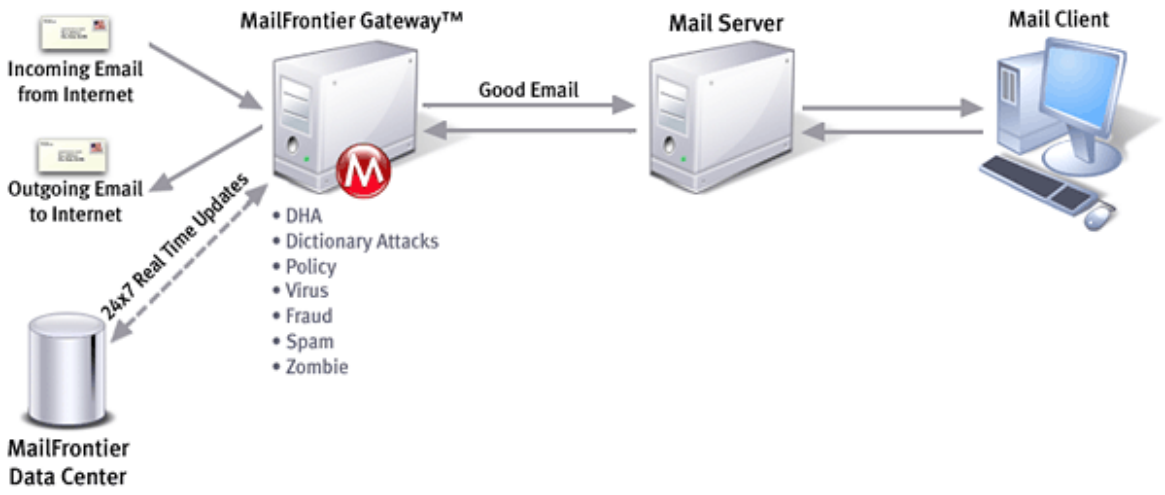


Figure 1.1 All in One Architecture

In an **All in One** configuration, you can also deploy multiple SonicWALL Email Security Gateway servers in a cluster setup wherein all of the gateways share the same configuration and data files. To set up such a cluster, begin by creating a shared directory, on either one of the SonicWALL Email Security Gateway servers or on another dedicated server (preferred) running the same operating system. This shared directory will be used to store data including user settings, quarantine email, etc., from all the SonicWALL Email Security Gateway servers in the cluster.

- **Split:** In a **Split** network configuration, there are two kinds of servers: Control Centers and Remote Analyzers. In this configuration there is typically one Control Center and multiple Remote Analyzers, but the Control Center can be set up in a cluster as well. The Split configuration is designed for organizations with remote physical data centers.

  The Split configuration, shown in Figure 1.2, allows you to manage SonicWALL Email Security Gateway so that email messages are filtered in multiple remote locations through multiple Remote Analyzers. The entire setup is centrally managed from a single location through the Control Center.

  Control Center clusters are not supported by SonicWALL Email Security Gateway Appliance or SonicWALL Email Security Gateway, Small Business Edition.

Figure 1.2 Split Network Architecture

The Control Center, in addition to managing all data files, controls, monitors and communicates with all Remote Analyzers. The data files consist of statistical data such as how much email has been received, network usage, remote hardware space used, and hourly spam statistics. The Control Center stores or *quarantines* email it receives from the Remote Analyzers. It also queries LDAP servers to ensure valid users are logging in to SonicWALL Email Security Gateway. End users can log in to a Control Center to manage their junk mail.

Remote Analyzers analyze incoming email to determine whether it is good or junk. It sends junk email to the Control Center where it is quarantined. It routes good mail to its destination server. Only administrators can log in to a Remote Analyzer.

Note The Replicator is the SonicWALL Email Security Gateway component that automatically sends data updates from the Control Center to the Remote Analyzer, ensuring that these components are always synchronized. Replicator logs are stored in the Control Center's logs directory. You can review replication activity from these logs for troubleshooting purposes.

Inbound vs. Outbound email flow

SonicWALL Email Security Gateway can process both inbound and outbound email on the same machine. Your deployment architecture may be influenced by which machines you configure for inbound email or outbound email or both. In an **All in One** configuration, each SonicWALL Email Security Gateway instance can support both inbound and outbound email. In a **Split** configuration, each Remote Analyzer can support both inbound and outbound email.

Proxy vs. MTA

SonicWALL Email Security Gateway can run either as a SMTP proxy or an MTA (Mail Transfer Agent).

The SMTP proxy operates by connecting to a destination SMTP server before accepting messages from a sending SMTP server. Some benefits of the SMTP proxy are:

- All processing occurs in memory, significantly reducing the latency and providing higher throughput
- There is no queue and SonicWALL Email Security Gateway does not lose any email messages. SonicWALL Email Security Gateway automatically respects your existing fail over strategies if your mail infrastructure experiences a failure.

The MTA service operates by writing messages to disk and allows for routing of a message. Some benefits of the MTA are:

- Can route messages to different domains based on MX records or LDAP mapping.
- Can queue messages by temporarily storing messages on disk and retrying delivery later in case the receiving server is not ready.
- Allows SonicWALL Email Security Gateway to be the last touch mail gateway for outbound traffic

Should You Choose an All in One or a Split Architecture?

SonicWALL Email Security recommends the **All in One** configuration whenever possible because of its simplicity. Choose a **Split** configuration to support multiple physical data centers and if you want to centrally manage this deployment from a single location.

SonicWALL Email Security strongly recommends that after you deploy the chosen architecture, you do not change the setup from a Control Center to a Remote Analyzer or vice versa, as there are no obvious advantages, and some data might be lost. Thus, it is important to make the deployment architecture decision before installing SonicWALL Email Security Gateway.

Typical SonicWALL Email Security Gateway Deployments

SonicWALL Email Security Gateway as the First-Touch / Last-Touch Server in DMZ

Figure 1.3 illustrates a typical network topology when SonicWALL Email Security Gateway is the first-touch and last-touch server in the DMZ.

In this deployment, you need to change your MX records to point to the SonicWALL Email Security Gateway setup. Also, all the inbound and outbound connections (typically port 25) for SonicWALL Email Security Gateway must be properly configured in your firewalls.

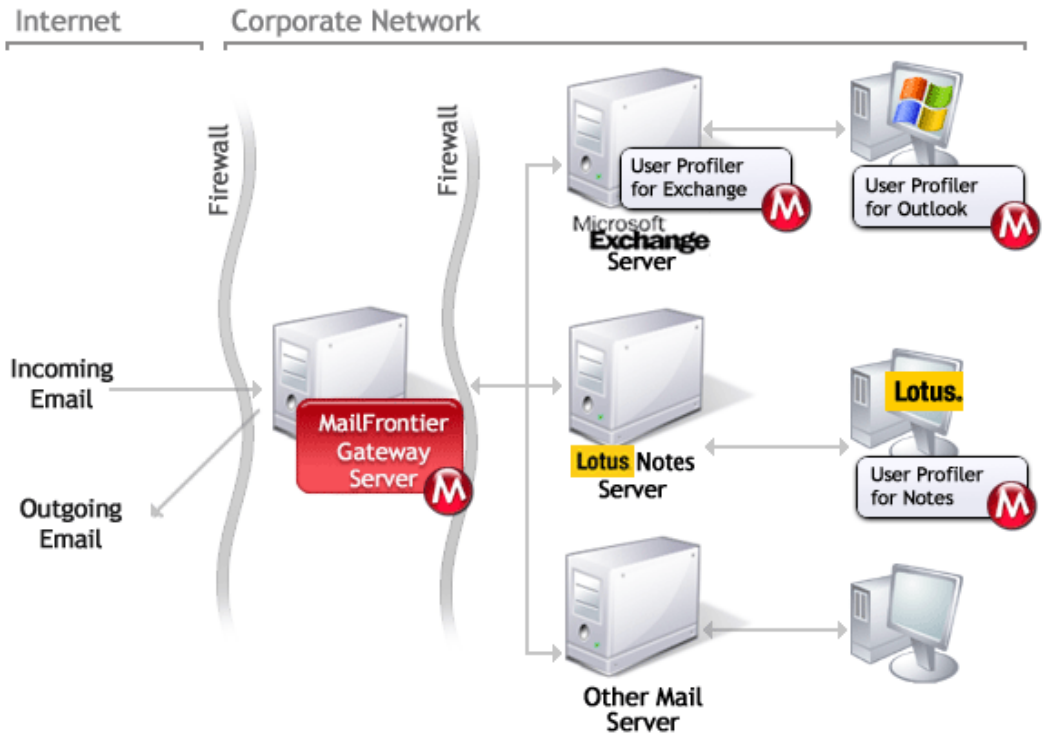


Figure 1.3 SonicWALL Email Security Gateway as the First-Touch and Last-Touch Server in the DMZ

In this configuration, SonicWALL Email Security Gateway can be configured on the inbound path to be either a SMTP Proxy or a MTA. On the outbound path, it must be configured to be a MTA. This setup also can be extended to a cluster with multiple SonicWALL Email Security Gateway servers all using a shared drive for data location.

To configure SonicWALL Email Security Gateway in this configuration, you also need to:

1. Configure SonicWALL Email Security Gateway server with a static IP address on your trusted network.
2. In your firewall, map the server's trusted IP address to an Internet addressable IP address for TCP port 25 (SMTP).
3. In the Internet DNS, create a record for this new server, mapped to the Internet addressable IP address you assigned in step 2.
4. Update your email domain's MX record to point to the new a record. You need to deploy the SonicWALL Email Security Gateway for each MX record.

SonicWALL Email Security Gateway inside Your Trusted Network

Figure 4 illustrates a typical network topology when a non SonicWALL Email Security SMTP MTA is between firewalls. In this topology, SonicWALL Email Security Gateway can be placed on your trusted network and receive email messages from the SMTP MTA in the DMZ.

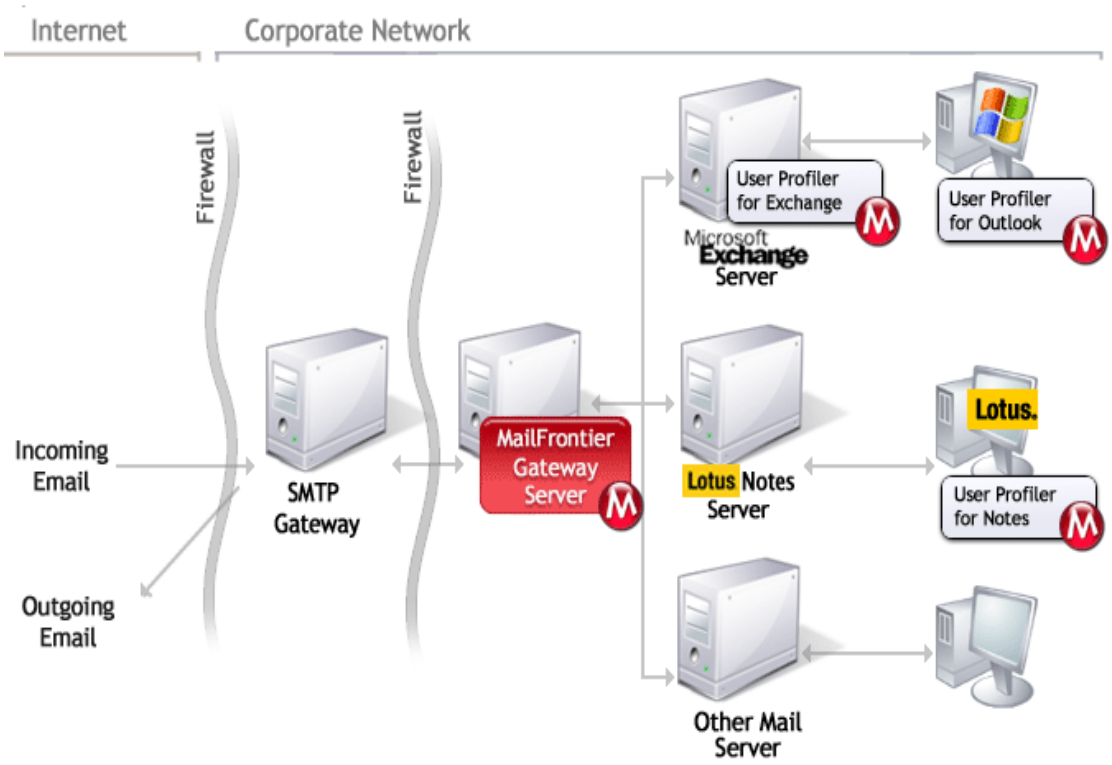


Figure 1.4 Network Topology

In this configuration SonicWALL Email Security Gateway can be configured to be either an MTA or a proxy.

SonicWALL Email Security Gateway on a Mail Server

If your organization has fewer than 500 email users, you can also consider installing SonicWALL Email Security Gateway on your SMTP server. For medium to large-sized organizations, SonicWALL Email Security recommends that you install SonicWALL Email Security Gateway on a separate server.

If you are running Microsoft IIS on the SMTP server, be aware that SonicWALL Email Security Gateway runs as an SMTP service on port 25 and an HTTP service on port 80. Typically, Microsoft IIS also runs on these ports and interferes with the operation of SonicWALL Email Security Gateway. If you require IIS on this server, configure the ports differently for either IIS or SonicWALL Email Security Gateway. If you are not using IIS, disable both the **World Wide Web Publishing Service**" and **Simple Mail Transport Protocol (SMTP)**, or completely uninstall IIS.

Additional Deployment Considerations

Server Preconfiguration Requirements

Before you begin the SonicWALL Email Security Gateway installation, the server on which you install SonicWALL Email Security Gateway must meet the following requirements:

- The server on which SonicWALL Email Security Gateway is installed must have a static IP address.

The server should be listed in DNS.

Supported Mail Servers

SonicWALL Email Security Gateway supports Exchange, SendMail, and Lotus Domino and other mail programs that support SMTP.

SSL (Secure Socket Layer) connection to administrative interface

When users and administrators log into SonicWALL Email Security Gateway, SonicWALL Email Security Gateway exchanges user login and application information with the user's client browser. Using SSL, you can protect login and application data by encrypting communication between the user's browser and SonicWALL Email Security Gateway.

SSL (Secure Socket Layer) connection to LDAP

When users and administrators log into SonicWALL Email Security Gateway, SonicWALL Email Security Gateway verifies via the LDAP protocol that the login information (user ID and password) is valid. Using SSL, you can protect login information by encrypting information sent to the LDAP server. You can also install SSL between a Control Center and a Remote Analyzer to encrypt configuration data transferred between the two servers.

For detailed explanation of SSL and related instructions, see *See "Secure Socket Layer" on page 183.*

Domains and Workgroups

You must configure all servers that deploy SonicWALL Email Security Gateway such that they are in the same Windows domain or workgroup. If your data directory is shared and is in a dedicated server, it must be in the same domain or workgroup as well. If the servers are in a workgroup, you must share the directory so that *everyone* has access to it.

NOTE: Remote Analyzers do not need to be in the same Windows domain or workgroup. The above applies to **All in One** configuration and **Control Centers** in Split Configuration.

How to change the SMTP Port on Exchange

Changing SMTP Port on Exchange 2000

To change the SMTP port on Microsoft Exchange 2000, go to the Exchange System Manager.

1. Select **Servers>** *Your Server***> Protocols.**

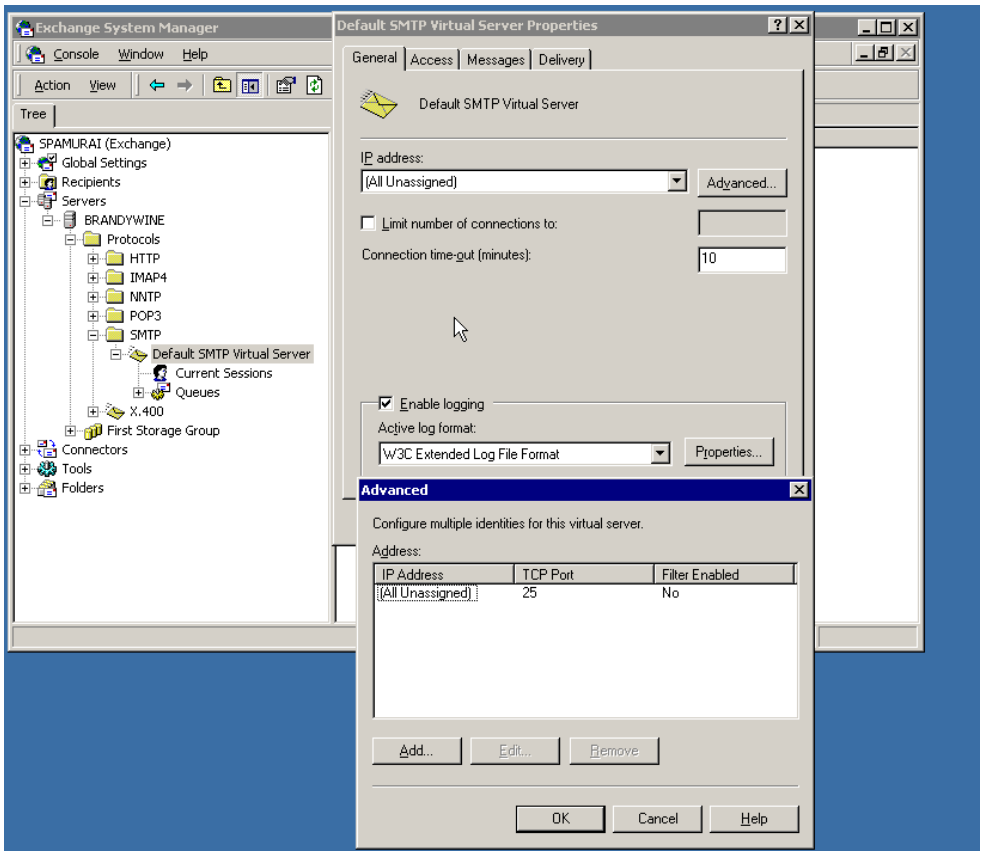


Figure 1.5 Exchange 2000

2. Select **Default SMTP Server** and choose **Properties > General > Advanced**.
3. Change the port number to the port desired.

Changing SMTP Port Exchange 5.5

To change the SMTP port on Microsoft Exchange 5.5, you can follow the instructions in Microsoft Support Q173903: Edit the `Services` file, `Winnt\System32\Drivers\Etc\Services`, to specify the port used for SMTP.

The following example, an excerpt from the `Services` file, shows removing SMTP from port 25 and enabling SMTP on port 17. Port 17 is normally used for `qotd` (quote of the day) service.

- smtp 17/tcp mail
- #qotd 17/tcp quote
- #qotd 17/udp quote
- chargen 19/tcp ttytst source
- chargen 19/udp ttytst source

- ftp-data 20/tcp
- ftp 21/tcp
- telnet 23/tcp
- #smtp 25/tcp mail
- time 37/tcp timeserver

Use `telnet ip_address` or `server_name 17` to verify that the Internet Mail Service is indeed listening on tcp port 17. For information on how to configure other types of mail servers to listen on another port, refer to your mail server documentation.

How to create a Shared Data Directory

On Windows

To share a directory via Windows file sharing:

1. Right-click the folder and select **Sharing...**
2. Select **Share this folder**.
3. Click **Permissions** to choose who has access to this shared folder.
4. Click **Add** and add the computers on which you are installing SonicWALL Email Security Gateway.

SonicWALL Email Security Gateway runs as a Windows Service, which does not use the same user account as the account you use for interactive login. SonicWALL Email Security Gateway does not have access to the shared directory unless you enable access to the computer itself.

NOTE: Control Centers and All in One servers must be in the same Windows domain or workgroup, and must be in the same domain or workgroup as the computer that shares the directory. If the computers are in a workgroup, you must share the directory so that everyone has access to it. Remote Analyzers do not need to be in the same Windows domain or workgroup, but it is not recommended they be set up to share directories.

On Unix NFS

On Unix, files are shared via a directory exported over NFS, which can be from any server that can act as an NFS server, for example, a Solaris server, a Linux server, or a Network Attached Storage (NAS) device. The procedures for exporting the directory for sharing over NFS might vary. These are the basic rules:

- You must export the directory to all of the SonicWALL Email Security Gateway servers that use it.
- You must give the same access permissions to each SonicWALL Email Security Gateway server.
- Each SonicWALL Email Security Gateway server must mount the directory as an NFS client.

Example of Exporting NFS

This is an example of exporting an NFS directory from a Solaris server. For other servers providing NFS service, consult the manuals for those servers.

1. On the Solaris server exporting the directory, add an entry to the `/etc/dfs/dfstab` file to specify the directory to share. For example: if the directory is `/disk1,` enter:

   ```
   share -F nfs -o rw /disk1
   ```

2. Type the command:

```
share /disk1
```

If you are running an instance of SonicWALL Email Security Gateway on the same server as the exported directory, then this instance of the gateway accesses the directory locally as the root user, and therefore all other instances of SonicWALL Email Security Gateway that share this directory via NFS also need root access. To accomplish this, the entry in `/etc/dfs/dfstab` should read:

```
share -F nfs -o rw,root=hostname1,hostname2,... /disk1
```

where *hostname1*, *hostname2* and so forth are the DNS fully qualified names of the remote SonicWALL Email Security Gateway instances. If you did not export any directories prior to this, reboot your server to start the NFS server.

On SonicWALL Email Security Gateway instances that share via NFS, you must have a path that accesses the shared directory. If you are running the automounter, the path is provided automatically. That is, if host *turoa* is sharing `/disk1`, you can access the directory remotely as

```
/net/turoa/disk1
```

If you are not running the automounter, or want to mount the remote directory, this provides an alternative path. That is, for the exported directory example given above, issue the command

```
mount -F nfs turoa:/disk1 /mnt
```

The remote directory is accessed as

```
/mnt/disk1
```

Make an entry in the `/etc/vfstab` file so that this directory is mounted every time the Solaris server boots.

When you install SonicWALL Email Security Gateway and are prompted for the data directory, specify the path to the NFS shared directory.

For more information about sharing, type:

```
man share
```

```
man dfstab
```

Note Regardless of platform, if two computers share a directory, access to the shared drive must be fast. As a general rule, there should be at least a 100 Megabit connection to the data drive and less than 10 millisecond latency to the data drive. Latency can be tested with ping.

Deploying SonicWALL Email Security Gateway's Web-based Administrative User Interface

From a security standpoint, SonicWALL Email Security Gateway's Web-based administrative user interface that is served by the Tomcat Web server is currently not qualified to be exposed on the Internet. SonicWALL Email Security strongly recommends that you install Tomcat Web server inside the corporate network.

Deploying SonicWALL Email Security Gateway to talk to Multiple Destination Mail Servers

A single SonicWALL Email Security Gateway server can filter mail for multiple destination mail servers. To do so, the SonicWALL Email Security Gateway server must be configured to have multiple IP addresses.

Set up the SonicWALL Email Security Gateway server with multiple IP addresses, one for each destination mail server (for example, mail1.mycorp.com and mail2.mycorp.com), as follows:

Configure your mail topology so that email messages intended for each domain are routed to the appropriate IP address (for example, email messages to `mail1.mycorp.com` are routed to 10.1.1.1 and email messages to `mail2.mycorp.com` are routed to 10.1.1.2).

Configure SonicWALL Email Security Gateway so that good email messages addressed to each IP get passed on to the correct mail address.

User Profilers

SonicWALL Email Security Gateway has a built-in profiler that can watch your organization's outbound traffic to reduce false positives and create per user Allowed Lists automatically. This option is disabled by default and can be enabled in the anti-spam techniques section of the administrative user interface.

If your organization's outbound email traffic is not passing through SonicWALL Email Security Gateway, you may want to consider deploying various User Profilers to work with your email servers. <Xref_Color>Figure 1.6 illustrates typical places on a network where the various User Profilers can be deployed.

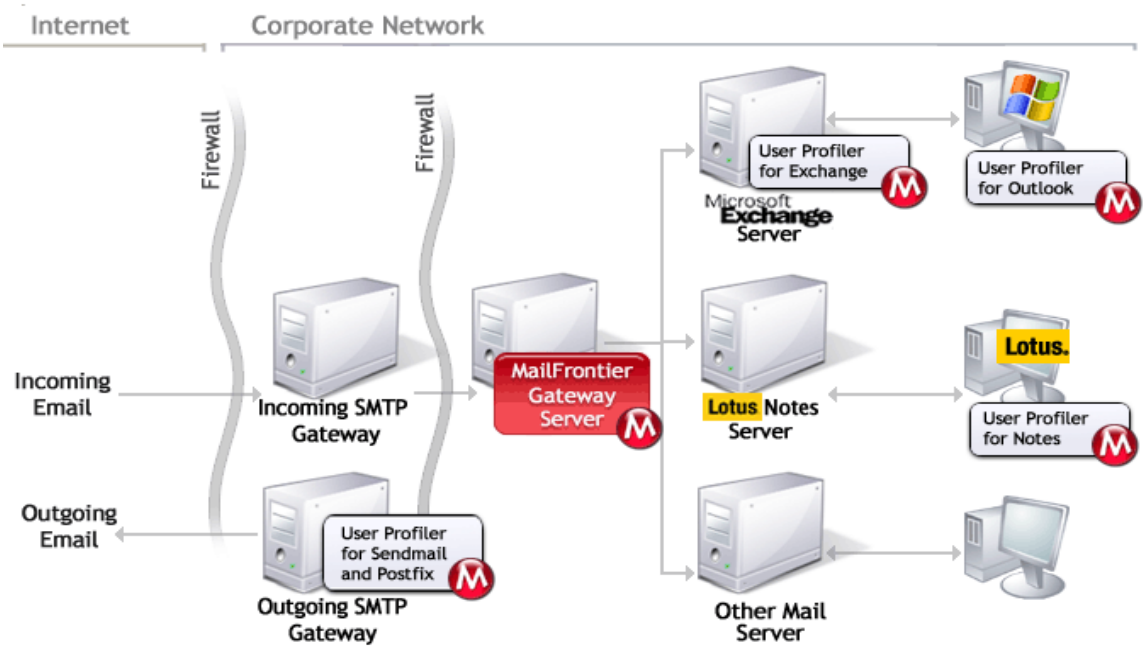


Figure 1.6 User Profilers Network Deployment

Caution

Your enterprise must use an LDAP server in order for User Profilers to work.

Where the User Profilers Run

As shown in <Xref_Color>Figure 1.6 on page 14, the Microsoft Outlook and Lotus Notes User Profilers run on employees' desktop computers. The Microsoft Exchange, Solaris Sendmail, and Solaris Postfix User Profilers are server-based; that is, they can be used on the SonicWALL Email Security Gateway server, or any other mail server in the company.

How the User Profilers Create Allowed Lists

All User Profilers help prevent false positives by automatically creating Allowed List email addresses for users. When a user sends an email message through the Mail Server, the recipient email address is placed on an allowed list for the sender. This per-user allowed list creation ensures that the recipient's response will not be accidentally quarantined.

Microsoft Outlook and Lotus Notes

The Microsoft Outlook and Lotus Notes User Profilers create Allowed Lists from employees' personal address books and their outgoing email messages. The first time the Outlook User Profiler runs, it obtains the past 30 days of sent email addresses and populates SonicWALL Email Security Gateway from the first day it is turned on. The Lotus Notes User Profiler posts sent email information to SonicWALL Email Security Gateway in real time.

Microsoft Exchange and Solaris

The Microsoft Exchange and Solaris User Profilers watch the outbound log files. When an employee sends an email, the recipient of that email is placed on an allowed list for that employee. These User Profilers do not have access to employee's personal address books, so if a system administrator deploys only that User Profiler, the allowed lists are initially smaller.

The Exchange User Profiler posts sent email information to the SonicWALL Email Security Gateway five minutes after the email is sent.

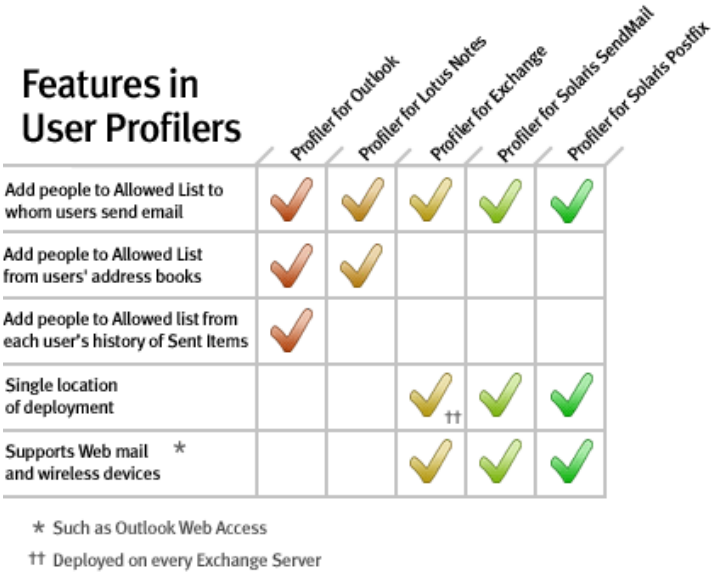


Figure 1.7 Features in User Profilers

Advantages and Disadvantages of the Various User Profilers

It would be unusual to deploy all of the profilers in a single organization. All User Profilers operate strictly in the background and require nothing from the user. However, each User Profiler has distinct advantages and disadvantages and you must weigh these and decide which to deploy. For example, the User Profiler for Solaris Sendmail does not have access to individual user's address books so Allowed lists are built by adding recipients as users send email. However, the Solaris Sendmail User Profiler has the advantage of working with all email clients on your corporate network and only needs to be installed in one place.

Client-specific User Profilers such as Microsoft Outlook and Lotus Notes have more power in terms of outgoing mail data, but only support a single client and so need to be installed on every user's desktop.

CHAPTER 2

Installing SonicWALL Email Security Gateway on Solaris

This chapter covers Solaris-specific details of installation and configuration of SonicWALL Email Security Gateway. See “Installing SonicWALL Email Security Gateway on Windows” on page 31 for instructions for installing on Microsoft Windows operating systems.

System Requirements

To install SonicWALL Email Security Gateway on Solaris, SonicWALL Email Security recommends the following minimum software and hardware configurations.

Operating System:

- Solaris 8 or 9 operating system
- `gzip/gunzip` utilities for decompressing the installation file

Note It is strongly recommended that you install SonicWALL Email Security Gateway in a separate partition and not in the root partition.

Hardware:

- Processor: UltraSparc II or better
- Processor Speed: minimum 1.2 GHz
- Memory: 1 Gbyte
- Hard Disk: 40 GB minimum, with a caching RAID controller for the data directory
- Available swap space: minimum 3 Gbytes.
  The installer issues an alert message and prompts you to either force or cancel the installation if your server does not have this much available swap space on your system.

SonicWALL Email Security recommends installing SonicWALL Email Security Gateway on a dedicated server.

SonicWALL Email Security Gateway Installer

The components bundled in SonicWALL Email Security Gateway Installer include the following:

- Sun Microsystems Java Runtime Environment
- Apache Tomcat
- Firebird Database Engine
- Jaybird JDBC driver
- SonicWALL Email Security Gateway
- SonicWALL Email Security Gateway User Profilers
- Port25 PowerMTA

The installer installs all these components in the appropriate location.

Note

If the Firebird database engine is already running on the server on which you install SonicWALL Email Security Gateway, Firebird will not get installed. Also, the host must be configured properly with a system name so that Firebird installation will be successful. If the name returned by the `uname -n` command does not match the name in `/etc/nodename`, the hostname is not accurate. In this case, you will see the following alert while installing SonicWALL Email Security Gateway:

```
The host name in the /etc/nodename file did not match the hostname
returned by uname -n. The Firebird Database might not start. Please
fix the hostname issue and restart the installation.

Type “force” to ignore this warning.
```

You must resolve the hostname before installing. Otherwise, certain reports will not be available.

Caution

If you have anti-virus programs running on the machines where you install SonicWALL Email Security Gateway, please make sure that those programs do not scan SonicWALL Email Security Gateway installation or data directories. If virus scanning for these directories is not disabled, SonicWALL Email Security Gateway data directory can get corrupted and quarantined messages may not be retrievable for all users.

SonicWALL Email Security Gateway Installation Checklist

Use the table below to record installation values.

Table 1 Installation Checklist

IDs	Parameters	Needed During	Value (write your values)
A	The directory path where SonicWALL Email Security Gateway will install	Installation	Default path: `/usr/local/MailFrontierEG`
B	Administrative Web Server Port	Installation	Default web server port: 80
C	The server's trusted network IP address	Login Page	Example: 192.168.31.15
D	The server's trusted fully qualified DNS name	Login Page	Example: EnterpriseGateway.mycorp.com
E	SonicWALL Email Security Licenses	Licensing	
F	Admin Username	Setup Admin	Default: admin
G	Admin Password	Setup Admin	Default: master
H	Admin email address	Setup Admin	Example: postmaster@mycorp.com
I	SonicWALL Email Security Gateway SMTP Listening Port	Add Mail Server	Default: 25
J	Destination SMTP server DNS name or IP address	Add Mail Server	Example: `mail-relay.mycorp.com`
K	Destination SMTP server's port number	Add Mail Server	Default: 25
L	Email domain names for which your organization accepts mail	Add Mail Server	Example: `mycorp.com, mycorp.net, mydivision.com`
M	LDAP Server Name	LDAP Config	Example: mail-relay.mycorp.com
N	LDAP Port Number	LDAP Config	Default: 389
O	LDAP Login Name	LDAP Config	varies by mail server, check Appendix A, "LDAP".
P	LDAP Password	LDAP Config	
Q	LDAP Directory Tree Node to Search	LDAP Config	varies by mail server, check Appendix A, "LDAP".
R	Microsoft NT NETBIOS Domain Name (only required if using Active Directory or Exchange 5.5)	LDAP Config	Example: `MYCORP`, check Appendix A, "LDAP".

Upgrading SonicWALL Email Security Gateway

If you are upgrading from SonicWALL Email Security Gateway version 2.x, please contact SonicWALL Email Security Support to get upgrade instructions. If you are upgrading from version 3.0 or later, you must uninstall the previous version before you install the new version.

Uninstalling a previous version

To uninstall a previous version,

1. Type the following command:

   > pkgrm MLFeg

2. Respond **y** to subsequent questions about whether you want to remove the `MLFeg` package, and whether you want to continue with the removal of the package. At the end of the upgrade process, SonicWALL Email Security Gateway displays:

   ```
   The pkgrm script lists and removes the files and concludes with:
   ## Updating system information.
   Removal of MLFeg was successful.
   ```

You have now uninstalled Enterprise Gateway. Your existing user data and configuration files remain on the server. To upgrade to a newer version of SonicWALL Email Security Gateway and preserve your existing user data and configuration, leave the data and configuration files untouched and install the new version as described in “Installing SonicWALL Email Security Gateway ” on page 20. When prompted for pathnames for the SonicWALL Email Security Gateway installation directory and the Gateway data files installation directory, specify the directories that were used when you performed the previous installation. When the new installation is complete, SonicWALL Email Security Gateway starts up configured identically to the previous installation, with all user data and configuration preserved.

Installing SonicWALL Email Security Gateway

You must be logged in as `root` to install SonicWALL Email Security Gateway.

1. Decompress (unzip) the compressed installation file. Type:

   > **gunzip *filename*.gz**

2. Run `pkgadd` on the decompressed installation file. Type:

   > pkgadd -d *filename*

3. Press **Enter** to select the default when `pkgadd` lists the available packages and prompts for the package to install.

4. SonicWALL Email Security installer detects whether you have sufficient available swap space on your system. If you do not, an alert message will appear displaying size of the available and required swap space.

- If you get this message, and you want to continue the installation and fix this problem later, type:

  force

- To stop the installation and add the swap space as requested, press **Enter**. After increasing swap space, to start the installation again, type:

  > **pkgadd -d *filename***

5. At the following prompt, respond with the desired installation directory, or press **Enter** for the default:

   ```
   Please enter an installation directory for the
   SonicWALL Email Security Gateway default:

   /usr/local/[MailFrontierEG]:
   ```

   This is the directory where the executable files are stored.

6. At the following prompt, respond with the desired location for the data files, or press **Enter** for the default.

```
Please enter an installation directory for the
SonicWALL Email Security Gateway data files default: /usr/local/
MailFrontierEG/datadir]:
```

This is the directory where user and administrative data and configuration information is stored, which includes junk mail files, Allowed Lists, Blocked Lists, and junk-blocking preferences.

Note If you are deploying multiple SonicWALL Email Security Gateways specify the shared folder here for your data.

Note For performance reasons, read/write access to the data directory should be fast. If the data directory is on the same disk drive as the install directory, it is almost certainly fast enough. If the data directory is shared between two or more computers, or is on a different device than the install directory, administrators need to make sure that performance requirements are met. As a general rule, there should be at least a 100 Megabit connection to the data drive and less than 10 millisecond latency to the data drive. Latency can be tested with `ping` command.

7. Specify the web server port number. Choose the default unless you are running another web server on port 80, in which case, you must specify an alternate port when the installer displays the following prompt:

   ```
   Please specify a port number on which to run the
   SonicWALL Email Security Gateway web server default: [80]:

   NOTE: You can change the port number and also configure HTTPS
   access through the UI in Server Configuration > User View Setup
   page.
   ```

8. If your site uses an HTTP proxy server, specify the hostname (or IP address) and port number of the proxy server as requested. The installer prompts:

   ```
   If you use a proxy server, and SonicWALL Email Security Gateway is
   required to go through the proxy to access the Internet, please
   enter its address here in the form hostname:port. Otherwise, press
   Enter.
   ```

   SonicWALL Email Security Gateway communicates regularly with the SonicWALL Email Security datacenter to obtain updates of collaborative spam thumbprints, spam-blocking rules, Blocked Lists, and other information to help keep its spam-blocking capabilities up to date. This communication takes place via HTTP. If your organization restricts HTTP access via a proxy server, SonicWALL Email Security Gateway can use this proxy to communicate with the SonicWALL Email Security Data Center. To do this, you must inform SonicWALL Email Security Gateway about the proxy. If SonicWALL Email Security Gateway does not have access to the data center, collaborative rules, and allowed and blocked lists are not updated.

   Note If your HTTP proxy server requires basic username and password authentication, you can set this in the **Server Configuration > Updates** page of the administration UI after you finish the installation.

   If your site does not use an HTTP proxy server, press **Enter** and SonicWALL Email Security Gateway's external Internet access is not proxied.

9. If you previously installed an earlier version of SonicWALL Email Security Gateway on this server, the following prompt is displayed:

```
The following files are already installed on the system and are
being
used by another package:
* /export/home/asg2/firebird <attribute change only>
* /export/home/asg2/jakarta-tomcat-4.1.29-LE-jdk14/wrap-ups/ROOT
<attribute change only>
* /export/home/asg2/jakarta-tomcat-4.1.29-LE-jdk14/wrap-ups/ROOT/
WEB-INF <attribute change only>

* - conflict with a file which does not belong to any package.

Do you want to install these conflicting files [y,n,?,q]
```

10. Type **y** to install these files.
11. The following prompt is displayed:

```
This package contains scripts which will be executed with super-
user

permission during the process of installing this package.

Do you want to continue with the installation of <MLFeg> [y,n,?] ^C
```

12. Press **Enter** to continue.

Note SonicWALL Email Security Gateway creates new links under `MailFrontier`: `/opt/firebird` and `/usr/local/firebird`; and copies new files in `/usr/lib`.

13. When the installation is complete, the SonicWALL Email Security Gateway is started. The installer displays the location of the licensing agreement in the installation directory.
14. Read the agreement and press **Enter** to accept its terms.

    Installation is now complete.

Testing SonicWALL Email Security Gateway Installation

To test that SonicWALL Email Security is properly installed:

1. Verify that SonicWALL Email Security Gateway is running. Look in the process table for the following items:

- `MlfAsgSm`—the Gateway mail server
- `MlfThumb`—an auxiliary administrative update program
- `MlfMonit`—a monitor that checks the health of SonicWALL Email Security Gateway and notifies you via e-mail of irrecoverable problems
- `Java`, the Gateway web interface, which runs as an Apache Tomcat web server application

15. Check all of the running processes. Type:

    > ps -ae

    The response should be similar to the following text:

```
PID TTY      TIME CMD
9849 ?        0:00 fbguard
29750 ?        0:00 MlfRepli
9850 ?        0:00 fbserver
29747 ?        0:01 MlfThumb
29321 ?        0:02 sshd
29763 pts/6    0:23 java
29711 pts/6    0:00 fbguard
```

Note `fbserver` and `fbguard` refer to Firebird database processes.

Starting and Stopping the SonicWALL Email Security Gateway

SonicWALL Email Security provides the script `/etc/init.d/asg` to start and stop SonicWALL Email Security Gateway during start up and shut down.

1. To start and stop SonicWALL Email Security Gateway manually, invoke this script either from `/etc/init.d` or the SonicWALL Email Security installation directory. Type:

   > asg <start|stop>

CHAPTER 3

Installing SonicWALL Email Security Gateway on Linux

This chapter covers Linux-specific details of installation and configuration of SonicWALL Email Security Gateway. See “Installing SonicWALL Email Security Gateway on Windows” on page 31 for instructions for installing on the Microsoft Windows OS.

System Requirements

To install SonicWALL Email Security Gateway on Linux, SonicWALL Email Security recommends the following minimum software and hardware configurations.

Operating System:

RedHat Enterprise Linux AS 3.0, update 4. To verify the version, type the following command:

```
> uname -a
```

The version printed should match **Linux 2.4.21-27.ELsmp**.

Note No other version of Linux and no other update for RedHat Linux is supported at this time.

Caution It is strongly recommended that you install SonicWALL Email Security Gateway in a separate partition and not in the root partition.

Hardware:

- Processor: Pentium 4 or Xeon or equivalent
- Memory: 1 Gbyte
- Hard Disk: 40GB minimum, with a caching RAID controller for the data directory
- Available swap space: minimum 3 Gbytes.

SonicWALL Email Security recommends installing SonicWALL Email Security Gateway on a dedicated server.

SonicWALL Email Security Gateway Installer

The components bundled in SonicWALL Email Security Gateway Installer include the following:

- Sun Microsystems Java Runtime Environment
- Apache Tomcat
- Firebird Database Engine
- Jaybird JDBC driver
- SonicWALL Email Security Gateway
- SonicWALL Email Security Gateway User Profilers
- Port25 PowerMTA

The installer installs all these components in the appropriate location.

Note

If the Firebird database engine is already running on the server on which you install SonicWALL Email Security Gateway, Firebird will not get installed.

Caution

If you have anti-virus programs running on the machines where you install SonicWALL Email Security Gateway, please make sure that those programs do not scan SonicWALL Email Security Gateway installation or data directories. If virus scanning for these directories is not disabled, SonicWALL Email Security Gateway data directory can get corrupted and quarantined messages may not be retrievable for all users.

SonicWALL Email Security Gateway Installation Checklist

Use the table below to record installation values.

Table 1 Installation Checklist

IDs	Parameters	Needed During	Value (write your values)
A	The directory path where SonicWALL Email Security Gateway will install	Installation	Default path: `/usr/local/MailFrontierEG`
B	Administrative Web Server Port	Installation	Default web server port: 80
C	The server's trusted network IP address	Login Page	Example: 192.168.31.15
D	The server's trusted fully qualified DNS name	Login Page	Example: EnterpriseGateway.mycorp.com
E	SonicWALL Email Security Licenses	Licensing	
F	Admin Username	Setup Admin	Default: admin
G	Admin Password	Setup Admin	Default: master
H	Admin email address	Setup Admin	Example: postmaster@mycorp.com
I	SonicWALL Email Security Gateway SMTP Listening Port	Add Mail Server	Default: 25
J	Destination SMTP server DNS name or IP address	Add Mail Server	Example: `mail-relay.mycorp.com`
K	Destination SMTP server's port number	Add Mail Server	Default: 25
L	Email domain names your organization accepts mail for	Add Mail Server	Example: `mycorp.com, mycorp.net, mydivision.com`
M	LDAP Server Name	LDAP Config	Example: mail-relay.mycorp.com
N	LDAP Port Number	LDAP Config	Default: 389
O	LDAP Login Name	LDAP Config	varies by mail server, check Appendix A, "LDAP".
P	LDAP Password	LDAP Config	
Q	LDAP Directory Tree Node to Search	LDAP Config	varies by mail server, check Appendix A, "LDAP".
R	Microsoft NT NETBIOS Domain Name (only required if using Active Directory or Exchange 5.5)	LDAP Config	Example: `MYCORP`, check Appendix A, "LDAP".

Installing SonicWALL Email Security Gateway

You must be logged in as `root` to install SonicWALL Email Security Gateway.

1. To install, type:

   `> eg-4.1.2.5855-linux-x86.sh`

2. Confirm that you have the root privileges.

3. SonicWALL Email Security installer detects whether you have sufficient available swap space on your system. If you do not, an alert message will appear displaying size of the available and required swap space.

   - If you get this message, and you want to continue the installation and fix this problem later, type:

     `force`

   - To stop the installation and add the swap space as requested, press **Enter**. After increasing swap space, to start the installation again, type:

     > **`eg-4.1.2.5855-linux-x86.sh`**

4. At the following prompt, respond with the desired installation directory, or press **Enter** for the default:

   ```
   Enter the installation directory for the
   SonicWALL Email Security Gateway [default: /usr/local/MailFron-
   tierEG]:
   ```
   This is the directory where the executable files are stored.

5. At the following prompt, respond with the desired location for the data files, or press **Enter** for the default.

   ```
   Enter the installation directory for the
   SonicWALL Email Security Gateway data files [default: /usr/local/
   MailFrontierEG/data]:
   ```
   This is the directory where user and administrative data and configuration information is stored, which includes junk mail files, Allowed Lists, Blocked Lists, and junk-blocking preferences.

Note If you are deploying multiple SonicWALL Email Security Gateways specify the shared folder here for your data.

Note For performance reasons, read/write access to the data directory should be fast. If the data directory is on the same disk drive as the install directory, it is almost certainly fast enough. If the data directory is shared between two or more computers, or is on a different device than the install directory, administrators need to make sure that performance requirements are met. As a general rule, there should be at least a 100 Megabit connection to the data drive and less than 10 millisecond latency to the data drive. Latency can be tested with ping command.

6. Specify the web server port number. Choose the default unless you are running another web server on port 80:

   ```
   Please specify a port number for the SonicWALL Email Security
   Gateway
   Web server [default: 80]:
   ```

   ```
   NOTE: You can change the port number and also configure HTTPS
   access through the UI in Server Configuration > User View Setup
   page.
   ```

7. The installer now will extract and copy over the necessary files and modify the system files for necessary configuration.

8. When the installation is complete, the SonicWALL Email Security Gateway is started. The installer displays the location of the licensing agreement in the installation directory.

9. Read the agreement and press **Enter** to accept its terms.

Installation is now complete.

Starting and Stopping the SonicWALL Email Security Gateway

SonicWALL Email Security provides the script `/etc/init.d/asg` to start and stop SonicWALL Email Security Gateway during start up and shut down.

1. To start and stop SonicWALL Email Security Gateway manually, invoke this script either from `/etc/init.d` or the SonicWALL Email Security installation directory. Type:

   `> asg <start|stop>`

CHAPTER 4

Installing SonicWALL Email Security Gateway on Windows

This chapter describes installation of SonicWALL Email Security Gateway on Windows operating systems. See “Installing SonicWALL Email Security Gateway on Solaris” on page 17 and “Installing SonicWALL Email Security Gateway on Linux” on page 25 for instructions for installing on Solaris operating systems.

System Requirements

To install SonicWALL Email Security Gateway on Windows, SonicWALL Email Security recommends the following minimum software and hardware configurations.

Operating System

- Microsoft Windows Server 2000 and 2003 with Service Pack 2 or later.

Note SonicWALL Email Security periodically sends upgraded versions of SonicWALL Email Security Gateway software. To enable your server to upgrade to the latest downloaded SonicWALL Email Security Gateway, download and install Sun’s Java Runtime Environment (JRE) 1.4.2_06 or later from http://java.sun.com/j2se/1.4.2/download.html on the computer where you administer SonicWALL Email Security Gateway using your browser.

Hardware

SonicWALL Email Security recommends the following hardware for SonicWALL Email Security Gateway:

- Processor: Pentium 4 or Xeon or equivalent
- Memory: 1 Gbyte
- Hard Disk: 40GB minimum, with a caching RAID controller for the data directory

SonicWALL Email Security recommends installing SonicWALL Email Security Gateway on a dedicated server.

SonicWALL Email Security Gateway Installer

SonicWALL Email Security Gateway installer includes the following components:

- Sun Microsystems Java Runtime Environment
- Apache Tomcat
- Firebird Database Engine
- Jaybird JDBC driver
- SonicWALL Email Security Gateway
- SonicWALL Email Security Gateway User Profiler Installers
- Port25 PowerMTA

The installer installs all these components in the appropriate location.

Note If the Firebird database engine is already running on the server on which you install SonicWALL Email Security Gateway, Firebird will not get installed.

Note Ensure that you have write access to the data directory in which you want to install SonicWALL Email Security Gateway.

Caution If you have anti-virus programs running on the machines where you install SonicWALL Email Security Gateway, please make sure that those programs do not scan SonicWALL Email Security Gateway installation or data directories. If virus scanning for these directories is not disabled, the SonicWALL Email Security Gateway data directory can get corrupted and quarantined messages may not be retrievable for all users.

SonicWALL Email Security Gateway Installation Checklist

Use Table 1 to record installation values.

Table 1 Installation Checklist

IDs	Parameters	Needed During	Value (write in your values)
A	The directory path where SonicWALL Email Security Gateway will install	Installation	Default path: C:\Program Files\MailFrontierEG
B	Administrative Web Server Port	Installation	Default web server port: 80
C	The server's trusted network IP address	Login Page	Example: 192.168.31.15
D	The server's trusted fully qualified DNS name	Login Page	Example: SonicWALL Gateway.mycorp.com
E	SonicWALL Email Security License	Licensing	
F	Admin Username	Setup Admin	Default: admin

G	Admin Password	Setup Admin	Default: master
H	Admin email address	Setup Admin	Example: postmaster@mycorp.com
I	SonicWALL Email Security Gateway SMTP Listening Port	Add Mail Server	Default: 25
J	Destination SMTP server DNS name or IP address	Add Mail Server	Example: mail-relay.mycorp.com
K	Destination SMTP server's port number	Add Mail Server	Default: 25
L	Email domain names your organization accepts mail for	Add Mail Server	Example: mycorp.com, mycorp.net, mydivision.com
M	LDAP Server Name	LDAP Config	Example: mail-relay.mycorp.com
N	LDAP Port Number	LDAP Config	Default: 389
O	LDAP Login Name	LDAP Config	Example: varies by mail server, check Appendix A, "LDAP".
P	LDAP Password	LDAP Config	
Q	LDAP Directory Tree Node to Search	LDAP Config	Example: varies by mail server, check Appendix A, "LDAP".
R	Microsoft NT NETBIOS Domain Name (only required if using Active Directory or Exchange 5.5)	LDAP Config	Example: MYCORP check Appendix A, "LDAP".

Installing SonicWALL Email Security Gateway

You must be logged in as `administrator` to install SonicWALL Email Security Gateway. SonicWALL Email Security Gateway's installer alerts you if your system does not have the required physical memory. SonicWALL Email Security strongly encourages you to upgrade the memory of your server to a minimum of 1 Gbyte for optimal effectiveness and performance.

1. Run the installer. You get the welcome screen. Click **Next.**
2. Read the License Agreement and click **Next** to agree to the terms presented.

3. SonicWALL Email Security provides an alert if the server where you are installing SonicWALL Email Security Gateway does not have Asian language packs installed.

Figure 4.1 Asian Language Packs are not installed

NOTE: Even though this step is optional, SonicWALL Email Security Gateway's spam prevention capabilities may be diminished if the East Asian language pack is not installed. Also, to view messages in Asian languages, you will need to install this language pack. This language pack can be installed separately after the SonicWALL Email Security Gateway installation is completed.

To install the East Asian Language Pack support on Windows 2003, go to the **Regional and Language Options** in the Control Panel and select the **Languages** tab. Select the **Install files for East Asian Languages** check box.

To install the East Asian Language Pack support on Windows 2000, go the **Regional and Language Options** in the Control Panel and select the **General** tab. Select all Asian languages from the **Languages settings for the system**.

4. Click **Next** to accept the default location, or **Browse** to select an alternate location (install checklist parameter A), and click **Next**.

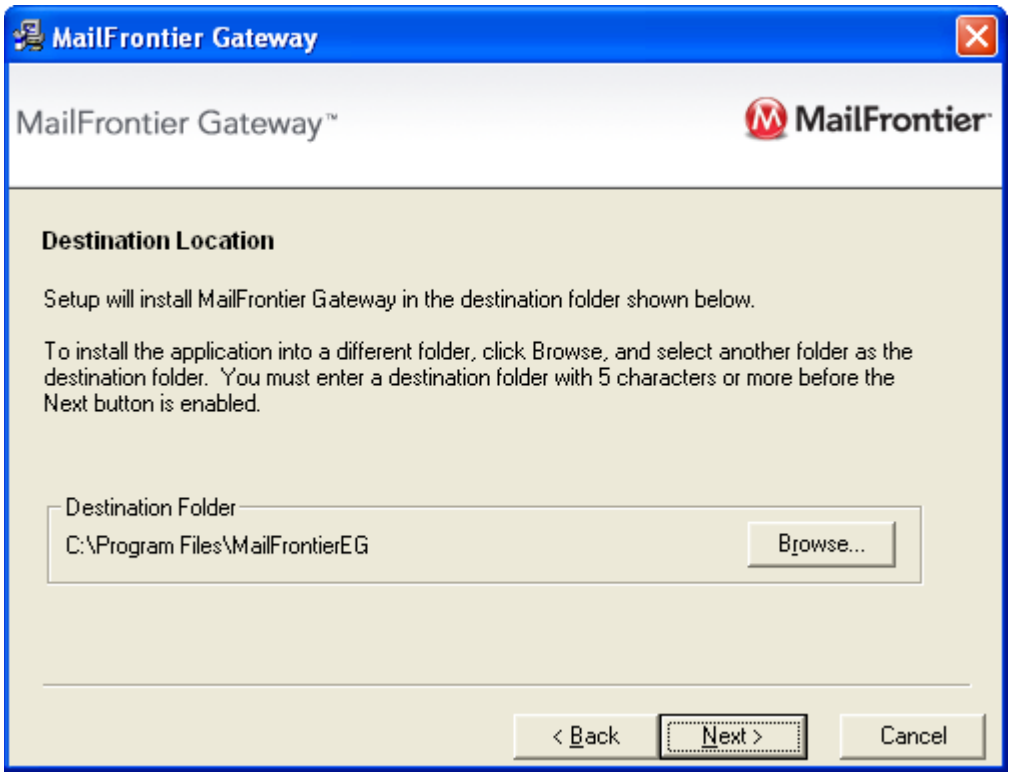


Figure 4.2 Destination Location for SonicWALL Email Security Gateway

Caution It is important that this folder is not scanned by an anti-virus engine.

5. Choose the directory to install your data, as shown in <Xref_Color>Figure 4.3 on page 36.

   The default destination location for SonicWALL Email Security Gateway files is suitable for most servers.

Note If you are deploying multiple SonicWALL Email Security Gateway servers that share a folder, specify that shared folder for your data.

Note For performance reasons, read/write access to the data directory must be fast. If the data directory is on the same disk drive as the install directory, it is almost certainly fast enough. If the data directory is shared between two or more computers, or is on a different device than the install directory, administrators need to make sure that performance requirements are met. As a general rule, there should be at least a 100 Megabit connection to the data drive and less than 10 millisecond latency to the data drive. Latency can be tested with the ping command.

Caution It is important that this folder is not scanned by an anti-virus engine.

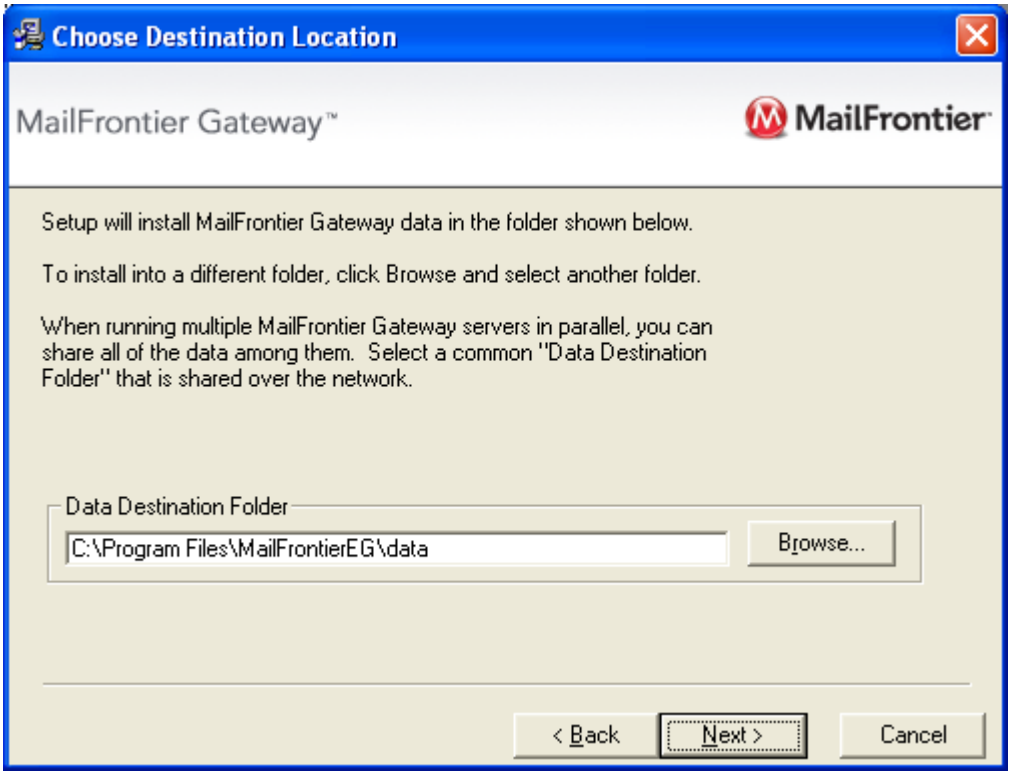


Figure 4.3 Choose Destination Location for SonicWALL Email Security Gateway Data

Click **Next** to accept the default data destination folder or click **Browse** to specify another folder.

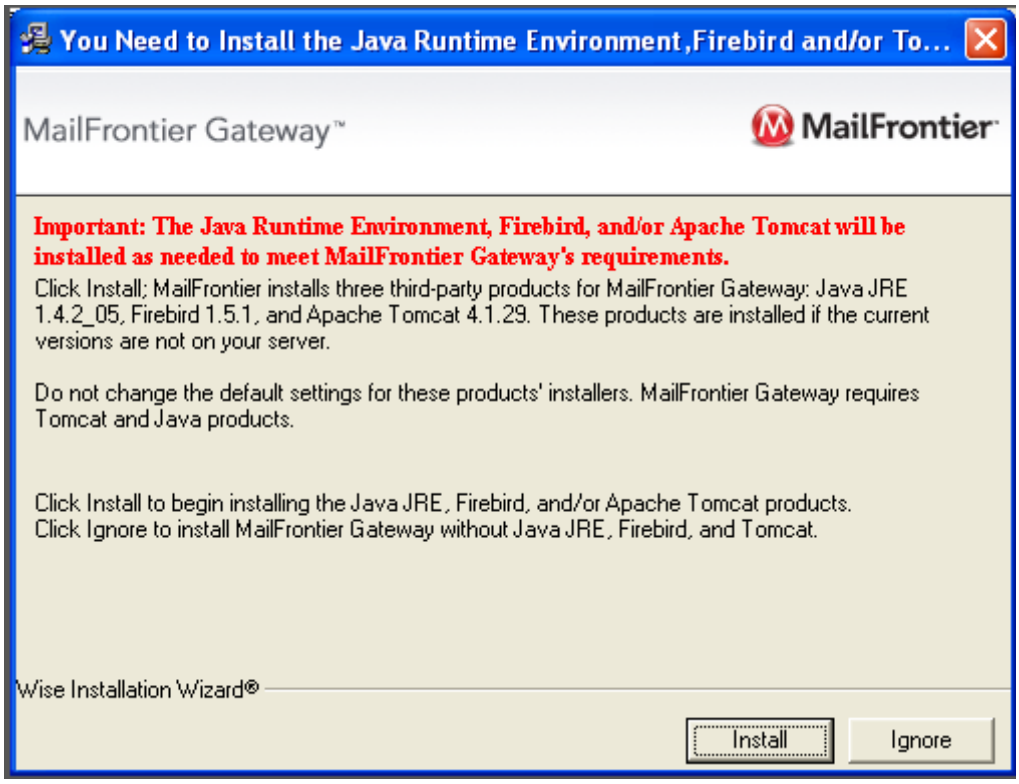


Figure 4.4 Installing Third-Party Products

6. Click **Install** to install these third-party products.
   If the required versions of Tomcat, Firebird, and the Java Runtime Environment (JRE) are not installed, they will be installed now.

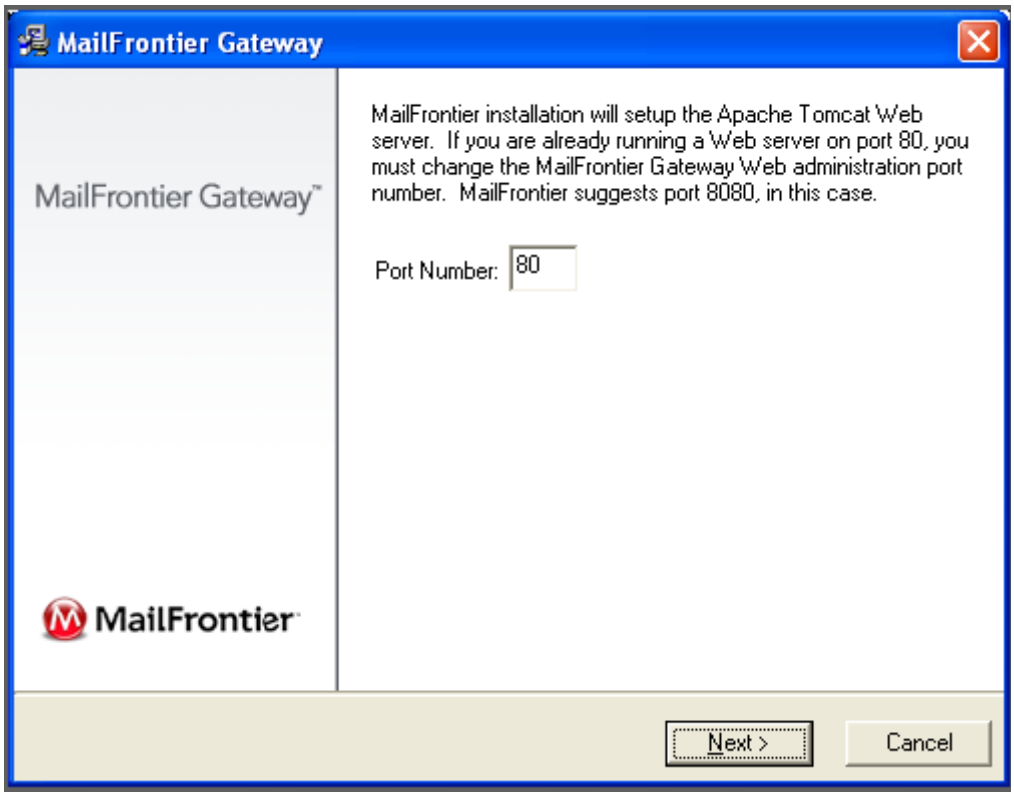


Figure 4.5 Choosing the port number for the Apache Tomcat Server

7. If you are already running a Web server on port 80, you can change the port setting (install checklist parameter B). SonicWALL Email Security recommends port 8080 for Apache Tomcat if port 80 is already used. Click **Next** to continue.

NOTE: You can change the port number and also configure HTTPS access through the UI on the **Server Configuration > User View Setup** page.

Figure 4.6 Installation Completed

8. A window appears to say that installation is complete. Click the **Finish** button. SonicWALL Email Security displays a browser window in which you can click links to view the documentation.

Confirm Windows Services Are Running

1. Test your SonicWALL Email Security Gateway installation to confirm that SonicWALL Email Security Gateway services are running and you can navigate to the **Login** page.
2. Select **Start > Programs > Administrative Tools > Services** and confirm that the following services have started:

- Apache Tomcat
- MlfAsg Gateway
- MlfAsg Monitor
- MlfAsg Replicator
- MlfAsg Updater
- Firebird Guardian
- Firebird Server
- MlfMTA

Configuring Proxy Services for SonicWALL Email Security Gateway for Windows

SonicWALL Email Security Gateway communicates regularly with the SonicWALL Email Security data center to obtain updates of collaborative spam thumbprints, spam-blocking rules, Blocked Lists, and other information to help keep its spam-blocking capabilities up to date. This communication takes place via HTTP. If your organization restricts HTTP access via a proxy server, SonicWALL Email Security Gateway can use this proxy to communicate with the SonicWALL Email Security Data Center. To do this, you must configure SonicWALL Email Security Gateway to use the proxy. If SonicWALL Email Security Gateway does not have access to the SonicWALL Email Security data center, collaborative rules and allowed and blocked lists are not updated.

Configure the Proxy Server settings within Internet Explorer. By default, those settings are not visible to Windows Services, including SonicWALL Email Security Gateway. To make the settings visible, edit the Windows Registry with `regedit`, and add the following Windows Registry entry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVers
ion\Internet Settings\ProxySettingsPerUser with a DWORD value of
0.
```

Then, reconfigure the proxy server settings in Internet Explorer.

Note

If your HTTP proxy server requires basic username and password authentication, you can set these parameters in the **Server Configuration > Updates** page of the administration UI after you finish installation.

Uninstalling SonicWALL Email Security Gateway

Except in very rare cases, new versions of SonicWALL Email Security Gateway can be installed without uninstalling the older version. If you are required to uninstall, SonicWALL Email Security recommends that you use the Control Panel to uninstall SonicWALL Email Security Gateway and its components. To remove SonicWALL Email Security Gateway for Windows and other installed components:

1. Select **Start > Settings > Control Panel > Add/Remove Programs**.
2. Click SonicWALL Email Security **Gateway** and select **Change/Remove**.
3. Click **Apache Tomcat** *version number* and select **Change/Remove**.
4. Click **Java 2 Runtime Environment SE** and select **Change/Remove**.
5. Click **Java Web Start** and select **Change/Remove**.
6. Click **Firebird** *version number* and select **Change/Remove.**

IF you uninstall SonicWALL Email Security Gateway and its components, do not delete SonicWALL Email Security Gateway data from the SonicWALL Email Security installation or data directories unless directed to by SonicWALL Email Security Technical Support. This information will be needed when you reinstall the product.

CHAPTER 5

Getting Started

Introduction

This guide describes how to configure SonicWALL Email Security Gateway to match your environment and user needs.

Note Disable your browser's pop-up blockers before configuring SonicWALL Email Security Gateway, because many of the configuration windows are pop-up windows.

Note For security purposes, SonicWALL Email Security terminates your session if there is no activity for 10 minutes. You must log in again if this occurs.

Initial Configuration

SonicWALL Email Security Gateway Master Account

Each SonicWALL Email Security Gateway setup has a Master Account which is a master administrative account. You use this account to initially configure the server, configure for LDAP synchronization and assign administrative privileges to other accounts. The Master Account's user name is **admin** and the password is **master**.

Logging In

Log in to your SonicWALL Email Security Gateway as a user with administrator privileges.

Example:
`http://mailfrontiergateway.mycorp.com`

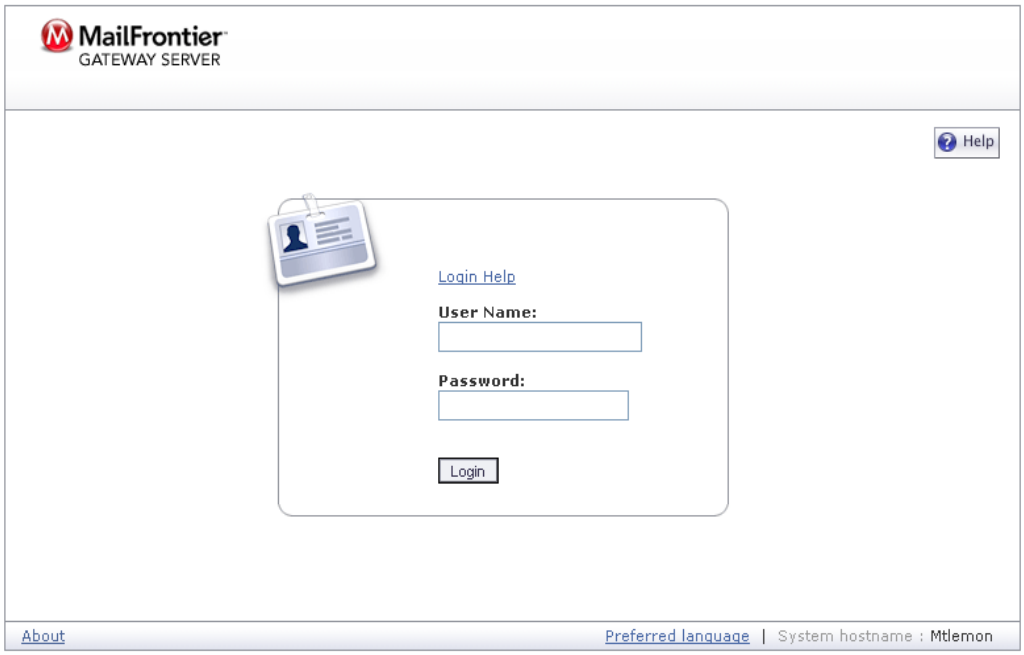


Figure 5.1 Login window

To log in with the Master Account, type:

- User Name: **`admin`**
- Password: **`master`**

The first time you log in to the SonicWALL Email Security Gateway system, you are directly taken to the license settings screen, see Figure 5.2, “License Management Window,” on page 43, where you can do the following:

- Change Master Account password
- Enter license keys
- Perform Quick Configuration of the system

Change Master Account Password

After you login using the Master Account, you can change the password. SonicWALL Email Security strongly recommends that you change the Master Account password.

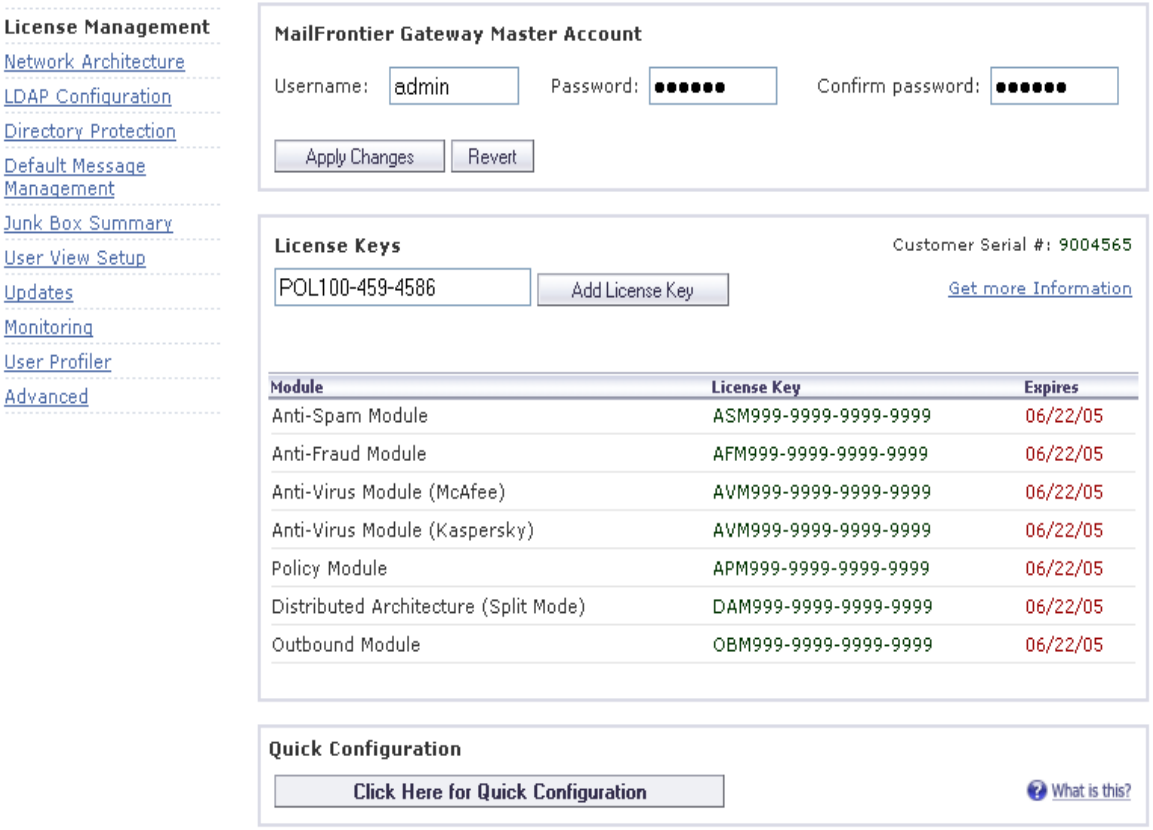


Figure 5.2 License Management Window

To change password:

1. Type **admin** for the username.
2. Type a new password in the **Password** text box.
3. Type the same password in the **Confirm password** text box.

Licensing SonicWALL Email Security Gateway Modules

Enter a license key for each SonicWALL Email Security module that you purchased and want to run. You can add additional modules at any time by entering the appropriate license keys. To purchase additional modules, contact your sales representative or email mailto:sales@mailfrontier.com.

To enter your license keys:

1. Cut and paste license key string from the email you received for the module you want to run in to the **License Keys** field.

2. Click **Add License Key**.
   After you add the license key, it appears adjacent to the module along with its license key and expiration date.
3. Repeat steps 1 and 2 for any additional modules you purchased that you want to run.

Note

After you have licensed SonicWALL Email Security Gateway, you will be taken to the **Report Dashboard** window directly on subsequent login.

Quick Configuration

If you plan to install SonicWALL Email Security Gateway in an All in One Configuration for inbound and outbound message processing with only one downstream server, no SSL, and routine LDAP options, click the **Quick Configuration** link from the **License Management** window. Quick Configuration allows you to set up SonicWALL Email Security Gateway in a default configuration.

Quick Configuration also allows you to choose whether to quarantine junk messages in the Junk Box or to pass messages through to users. However, Quick Configuration requires that you configure all modules similarly; that is, if you store spam messages in the Junk Box, you must also store messages with viruses in the Junk Box.

NOTE: If you have previously configured your SonicWALL Email Security Gateway with more complex settings than are supported by Quick Configuration, the following alert will appear:

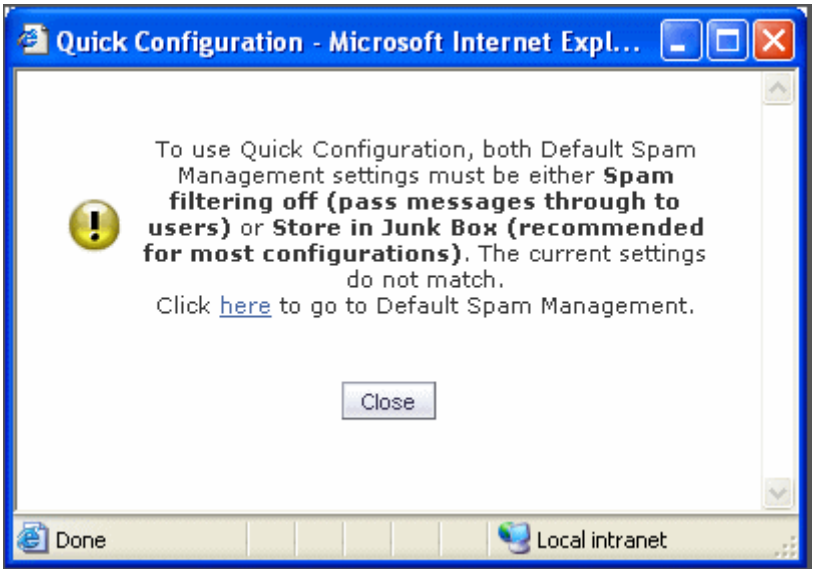


Figure 5.3 Quick Configuration Alert

If this alert window or a similar alert window appears, you must either configure all of the modules to pass through email without filtering or to store it in the Junk Box. Otherwise, follow the directions in “Server Configuration” on page 53.

<Xref_Color>Figure 5.4 on page 45 displays the Quick Configuration window. To configure SonicWALL Email Security Gateway using the Quick Configuration window, select the radio buttons and enter values for the following configuration variables:

1. Network Architecture:

- Enter the **Inbound Destination server** name or IP address and port number.

- Select the **Inbound SMTP setup**:
  - Allow SMTP recipient addresses to all domains
  - Only allow SMTP recipients addresses to these domains and enter the domains
- Click **Test Mail Servers** to determine that the flow of email from the SonicWALL Email Security server to downstream mail server is able to process email.
- Select the **Outbound Path setup** checkbox if the specified **Inbound Destination Server** will be the only server passing outbound messages to SonicWALL Email Security Gateway.

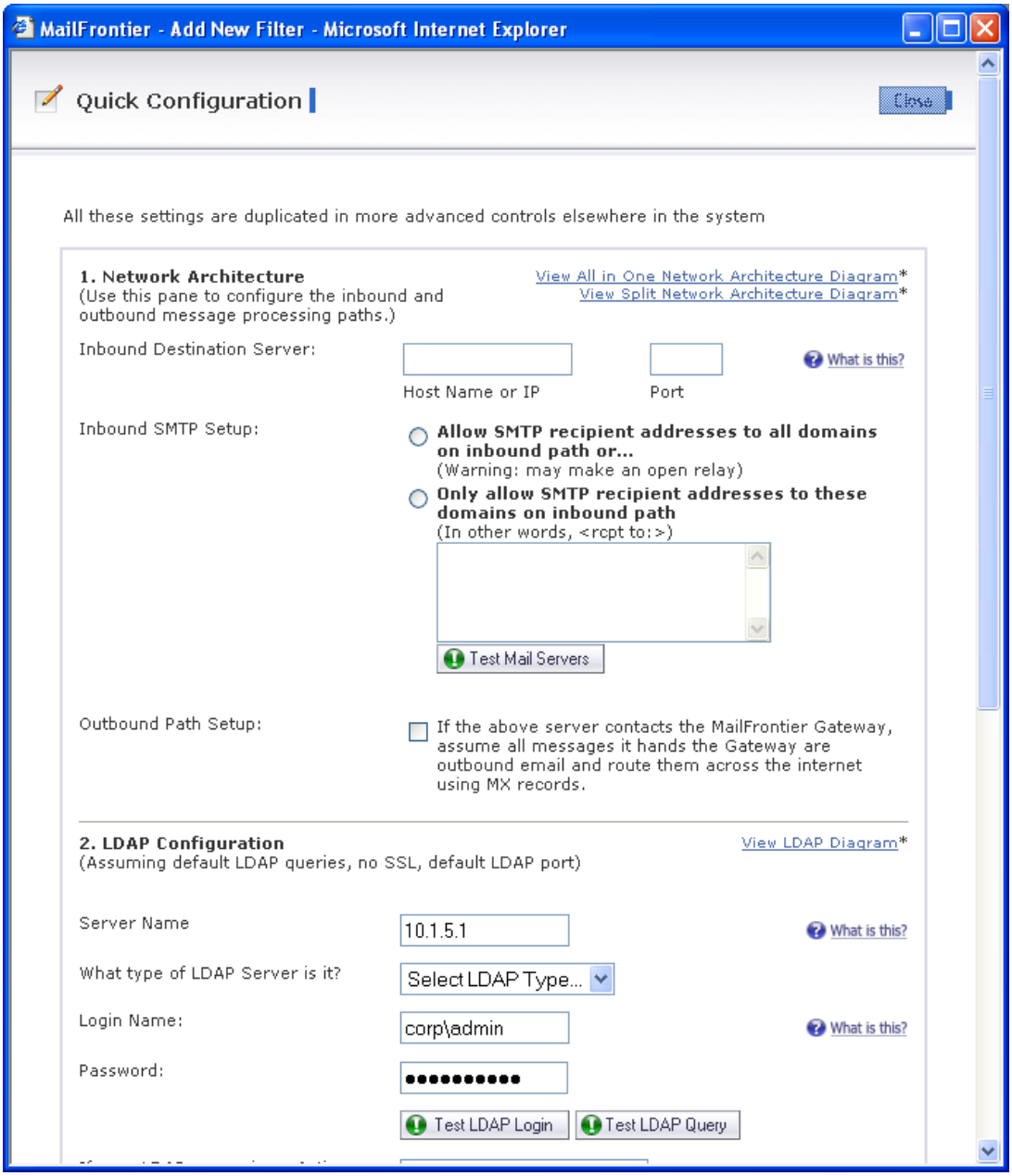


Figure 5.4 Quick Configuration Window

2. LDAP Configuration

- Add your **LDAP Server name or IP address**.
  This is the hostname or IP address of the LDAP server. Frequently, this is the name of your Exchange server or your email server.
- Select the **LDAP Server type** from the drop-down list.
- Enter your **Login name** in the format indicated by the type of LDAP server.

  Active Directory - The login name is commonly of the form *domain\username*; for example:

  ```
  sales\john
  ```

  Exchange 5.5 - The login name is commonly of the form *CN=username*, for example:

  ```
  CN=john
  ```

  Note: To use NTLM authentication, add the LDAP domains on the LDAP configuration page.

  Lotus Notes/Domino - The login name is commonly of the form *username*, for example:

  ```
  john
  ```

  SunOne/iPlanet - The login name can either be the exact string `"CN=Directory Manager"` or a user's X.400-style login. Consider both examples below:

  ```
  CN=Directory Manager
  UID=john,OU=people,O=xyz.com,O=internet
  ```

  For **Other LDAP Servers**, see the documentation that shipped with that product.
- Enter your **password**.
- Click the **Test LDAP Login** button to ensure that LDAP you can log in to your LDAP server.
- Click the **Test LDAP Query** button to ensure that LDAP you can query your LDAP server.
- Enter the Windows NT/NetBIOS domain name if you have an Active Directory or an Exchange 5.5 server.

3. Message Management:

- Select the action SonicWALL Email Security Gateway should take for messages identified as junk:
  - Click Quarantine junk to cause SonicWALL Email Security Gateway to store all messages in the Junk Box.
  - Click **Deliver all messages to users** to allow all messages to pass through to users without filtering for email threats.

4. Junk Box Summary:

- Check the **Send summaries daily** check box to send users daily summaries of their quarantined email, if you selected **Quarantine junk** in step 3.
- Check the **Users can preview their own quarantined junk mail** check box to allow users to preview their junked messages.
- Enter the **URL for the user view**. This text box is filled in automatically based on your server configuration and is included in the Junk Box Summary email.
- Click **Test this Link** to ensure that you have configured a link for users to connect to SonicWALL Email Security Gateway.

5. Updates

- Click the **Test Connectivity to** SonicWALL Email Security button to ensure that you can connect to the SonicWALL Email Security data center.

Click **Apply Changes** to save your Quick Configuration settings. Your server is now ready to process email messages and stop email threats.

Understanding the SonicWALL Email Security Gateway User Interface

This section describes how to navigate the SonicWALL Email Security Gateway user interface. Figure 5.5 displays the basic SonicWALL Email Security window.

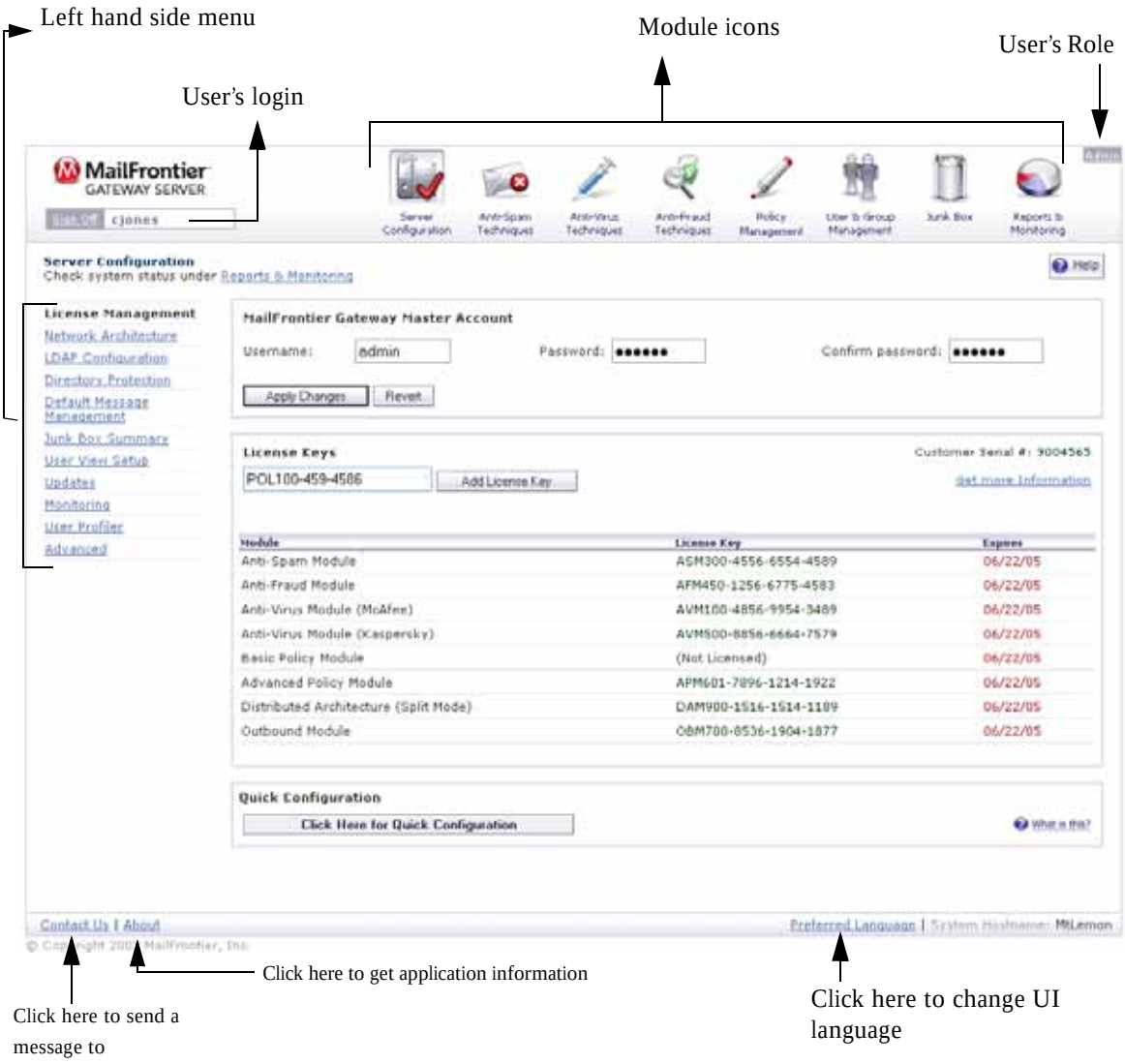


Figure 5.5 SonicWALL Email Security Gateway User Interface Overview

The upper left corner displays the current login name. The upper right hand corner displays the role of the user logged in: Admin, Manager, Help Desk, Group Admin or User. See “SonicWALL Email Security Gateway Roles” on page 147 for more information about roles.

Click the icons on the top of the window to select the different modules, such as spam management or server configuration. Each button brings up a unique menu on the left hand side.

Click the links on the lower margin of the window for the following information:

- **Contact us:** Click this link for a Contact Technical Support form and other support information.
- **About:** Click this link to display a window that contains information about the SonicWALL Email Security Gateway software.
- **Sign in as any user:** Click this link if you are signed in as the administrator and would like to login as a user.
- **System host name:** SonicWALL Email Security Gateway can run on more than one server. The lower right corner of your window displays the host name for the server to which you are currently logged in.
- **Preferred Language:** Click this drop-down box to change SonicWALL Email Security Gateway’s user interface in any of the languages shown in Figure 5.6. By default, SonicWALL Email Security Gateway automatically senses the language that you have configured your Web browser.

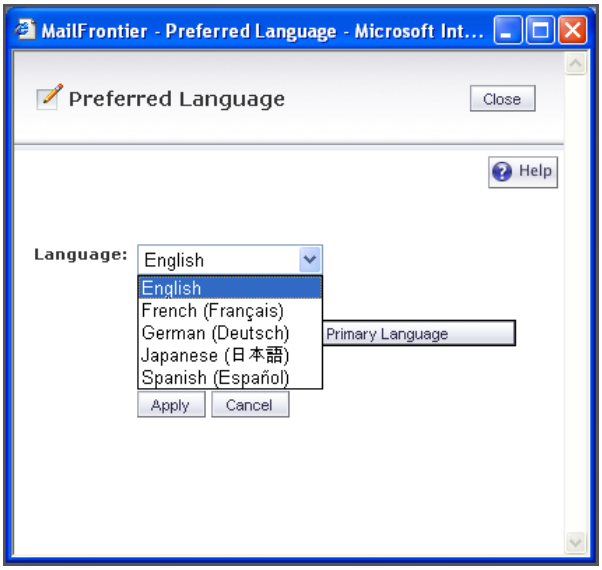


Figure 5.6 Preferred Language

Automatically Download Software for SonicWALL Email Security Gateway

To provide the best protection against latest threats, SonicWALL Email Security periodically releases updates to its Gateway software. SonicWALL Email Security recommends that you keep your software version up-to-date to ensure that you get the best protection available. The updates are classified as minor updates and major updates.

Minor Updates

Windows OS

For Windows based installations, when a minor software update is available, SonicWALL Email Security Gateway automatically downloads the newer version and alerts the administrator that a newer version is available and can be installed. The administrator will see the following pop-up window after logging in to the system.

Configuring Automatic Software Downloads

To configure automatic software downloads for MailFrontier Gateway servers that run All in One configuration on Windows:

1. Click **Server Configuration>Updates**.

   MailFrontier Gateway displays the Updates window, as shown in Figure 5.7.

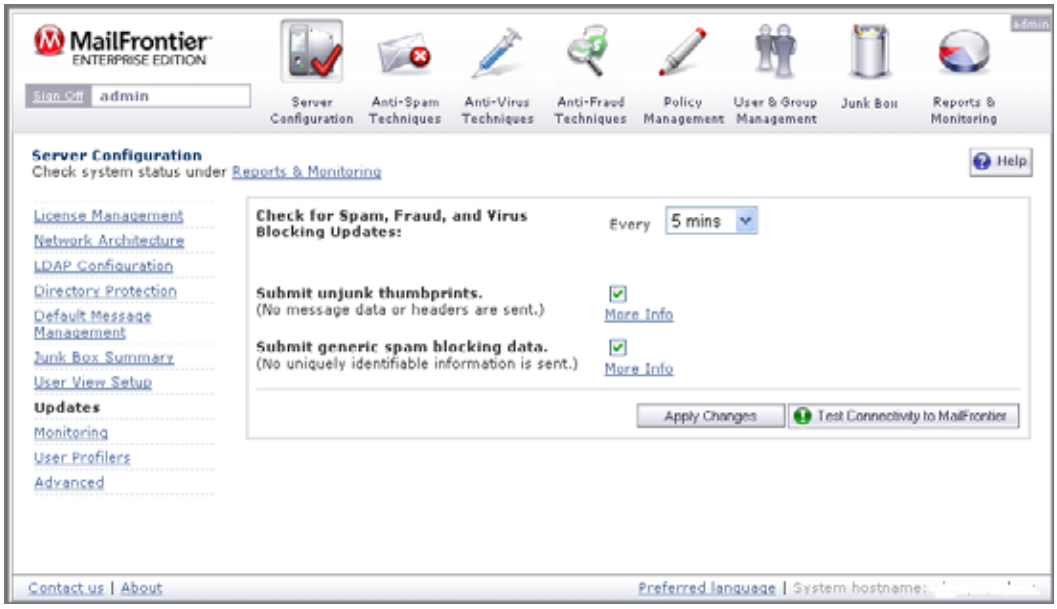


Figure 5.7 Configuring Updates to MailFrontier Gateway

2. Select the time interval from the **Check for Spam, Fraud, and Virus Blocking Updates** drop-down list to configure how often to receive junk-blocking updates.
3. Check the **Submit unjunk thumbprints** check box to send unjunked thumbprints to MailFrontier's Collaborative Laboratory.

   NOTE: When users unjunk a message, a thumbprint of that message can be sent to MailFrontier Gateway. These unjunked email messages are used to improve the collaborative settings for all users, which tracks new trends in spam and other junk email, and helps prevent unwanted email. The thumbprints sent optionally from MailFrontier Gateway contain absolutely no readable information.
4. Check the **Submit generic spam blocking data** check box to send spam-blocking data to MailFrontier's Collaborative Laboratory.

   Generic spam blocking data is sent to MailFrontier to assist in customer support and to help improve spam blocking. No messages, email content, header information or any other uniquely identifiable information is ever sent. Sample information that is sent includes the following data:

- Volume of messages processed and junked
- Success of various junking methods

Number of users protected

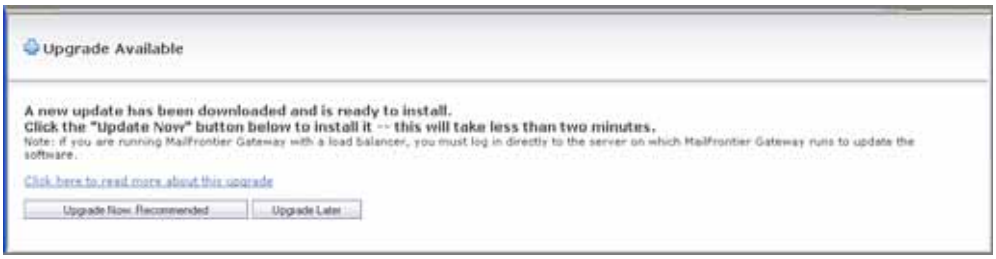


Figure 5.8 Windows: Update Available Alert

Note If you want to use the Upgrade Now button to upgrade the software and you are administering the system from a remote machine, you must install Java Runtime Environment (JRE) 1.4.2_05 or later from http://java.sun.com/j2se/1.4.2/download.html on the remote machine first.

Note If you are running SonicWALL Email Security Gateway with a load balancer, you must log in directly to the server on which SonicWALL Email Security Gateway runs to update the software

Solaris

For Solaris based installations, when a minor software update is available, SonicWALL Email Security Gateway only alerts the administrator that a newer version is available. The administrator will see the following pop-up window after logging in to the system. The administrator will have click **Download for Solaris** button to download and install the software.

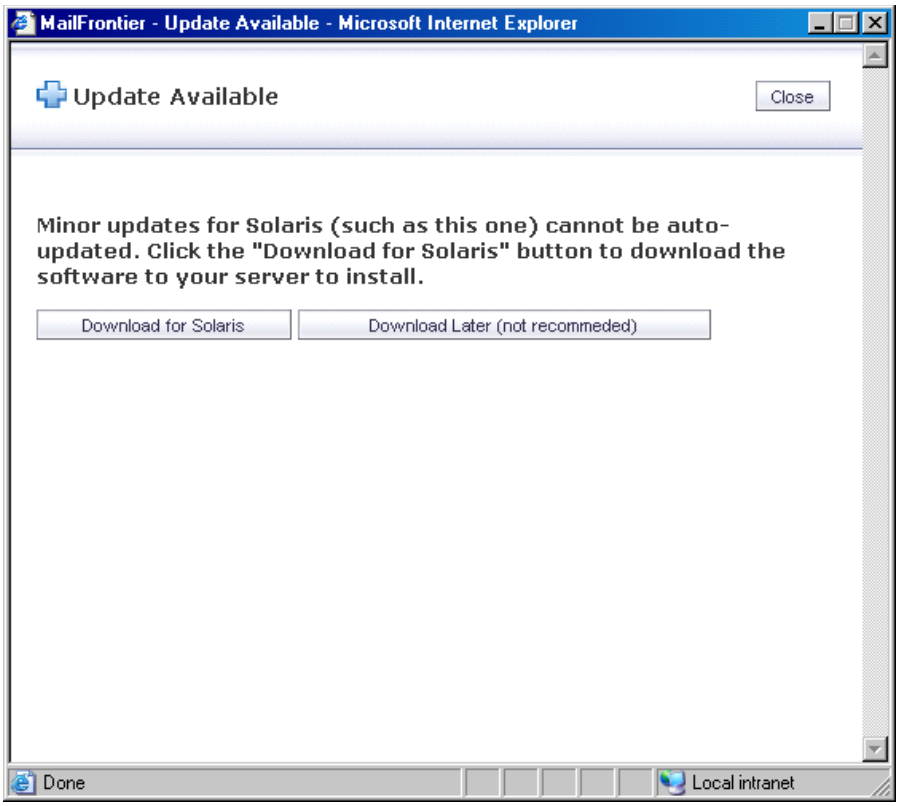


Figure 5.9 Solaris: Update Available Alert

Major Updates

When a major update is available, in both Windows and Solaris, SonicWALL Email Security gateway will alert the administrator that a major update is available and prompt for downloading update for the platform in use. SonicWALL Email Security recommends that you download and install major updates as soon as possible.

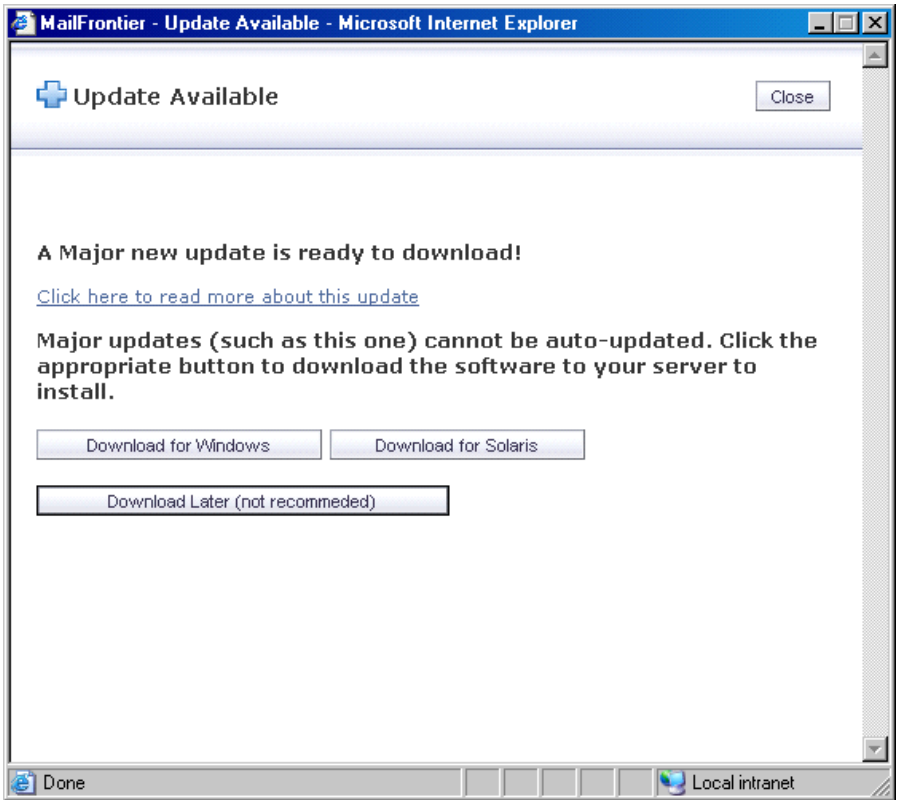


Figure 5.10 Major Update Alert

CHAPTER 6
Server Configuration

Introduction

In this chapter, you will learn how to configure the system more extensively and learn more about additional system administration capabilities.

Host Configuration

You can use this page to make changes to the server on which SonicWALL Email Security Gateway is installed.

Changing the Hostname

If you want to change the hostname of this server, enter the new fully-qualified hostname in the **Hostname** field and click the **Apply Changes** button. Changing the hostname will cause a number of changes to be made to SonicWALL Email Security Gateway settings, configuration files, and will rename some of the directories in the SonicWALL Email Security installation and data directories.

If you are running SonicWALL Email Security Gateway in split mode, you must also make changes to the hostname on the other servers. If you rename a Remote Analyzer, you must log in to the Control Center and click the **Server Configuration > Network Architecture** page. Then remove the old Remote Analyzer hostname from any of the Control Centers with which it is associated, and add the new Remote Analyzer hostname. If you rename a Control Center, you must login to the Remote Analyzers and click the **Server Configuration > Network Architecture** page. Then remove the old Control Center hostname and add the new one.

Networking

To configure network settings, such as the IP address, use the **Networking** panel. If DHCP (Dynamic Host Configuration Protocol) is chosen, all the necessary settings will be automatically found from the network DHCP server. If static IP settings are chosen, additional information must be entered in the remaining fields.

The **More Settings** panel allows you to change the date and time of the host machine, restart all the SonicWALL Email Security Gateway services, or reboot the host machine.

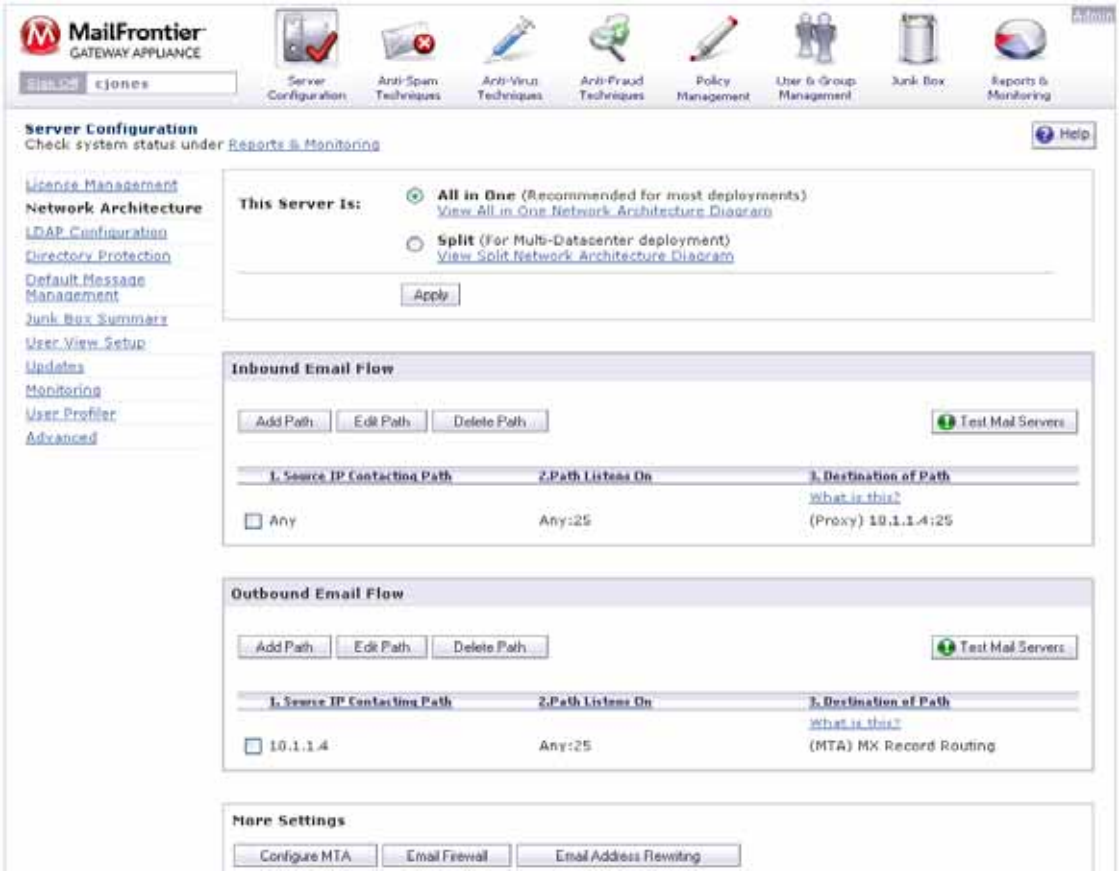
Setting Your Network Architecture

There are different ways to configure and deploy SonicWALL Email Security Gateway, and the first decision to make is the choice of network architecture. See “Planning SonicWALL Email Security Gateway Deployment” on page 3 for more information on what network architecture is appropriate for your need. You must decide whether you are setting up a Split or All in One architecture, as that choice impacts other configuration options. You can change the architecture later, but if you do so, you will need to add your mail servers and reset configuration options again.

To configure SonicWALL Email Security Gateway as your desired network architecture, click **Server Configuration > Network Architecture**. A screen similar to Figure 6.1, “Network Architecture,” on page 54 appears.

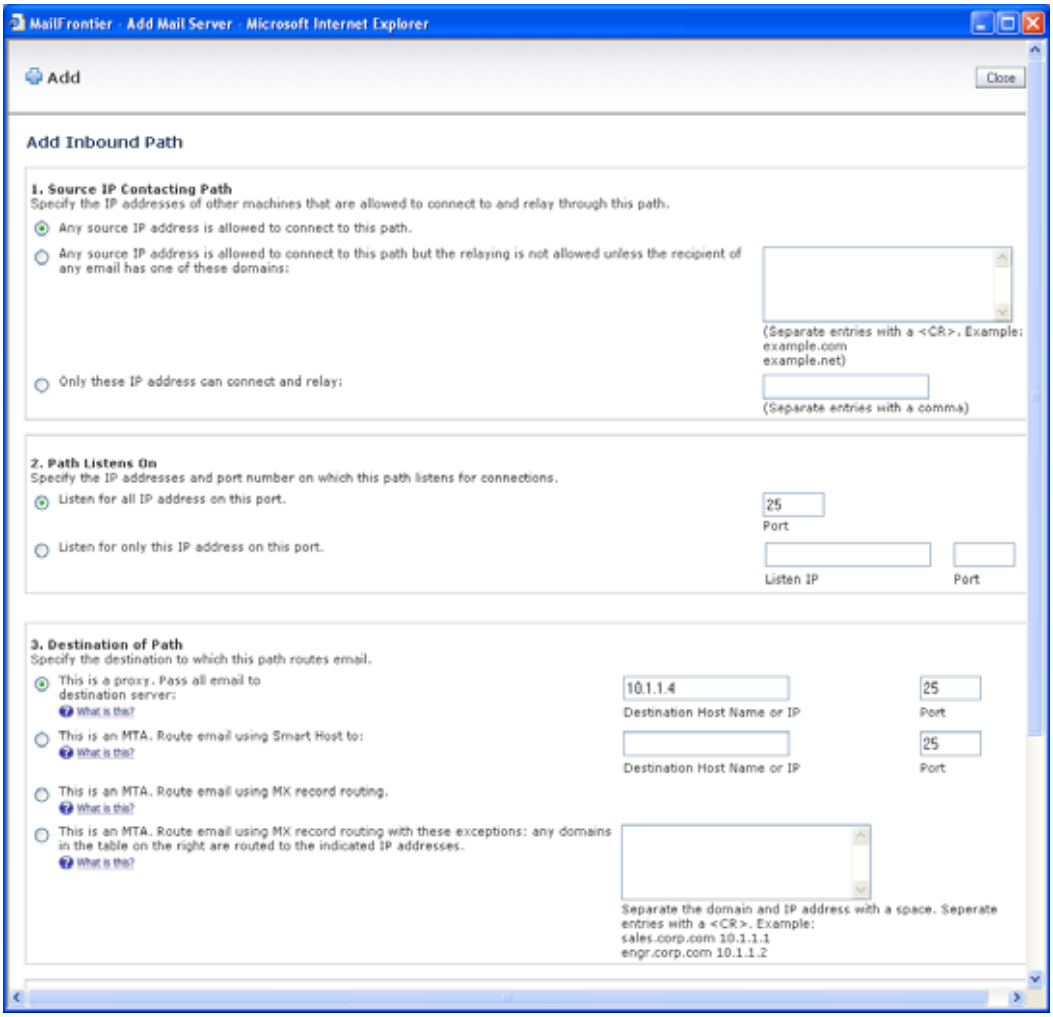
Adding an Inbound Mail Server for All in One Architecture

Figure 6.1 Network Architecture



Set this server to All in One configuration by choosing the radio button next to **All in One**. Click the **Add Path** button in the **Inbound Email Flow** section. The **Add Inbound Path** window appears, as shown in Figure 6.2.

Figure 6.2 Adding Inbound Path Window



1. **Source IP Contacting Path**. In this section you can configure where you accept email from. You can choose to
   - Accept connections for all senders. Use of this setting can make the product an open relay.

Caution SonicWALL Email Security strongly recommends *against* an open relay. Open relays can reduce the security of your email network and allow malicious users to spoof your email domain.

   - Accept connections for all senders sending to the specified domains.
   - Accept connections from the specified senders
2. **Path Listens On**. In this section, you can specific which IP addresses and port number the service is listening on for incoming email.

- **Listen for all IP address on this port** - This is the typical setting for most environment as the service listens on the specified port using the machine's default IP address. The usual port number for incoming email traffic is 25.
- **Listen only on this IP address and port** - If you have multiple IP addresses configured in this machine, you can specify which IP address and port number to listen on.

3. **Destination of Path**. In this section, you can specify the destination server for incoming email traffic in this path.
   - **This is a proxy. Pass all email to destination server** - This setting configures this path to act as a proxy and relay messages to a downstream email server. If the downstream server is unavailable, incoming messages will not be accepted.
   - **This is an MTA. Route email using SmartHost to** - This setting is the same as the above Proxy option, except that incoming messages will be accepted and queued if the downstream server is unavailable. In this instance, this path acts as a SMTP smarthost.
   - **This is an MTA. Route email using SmartHost with load balancing to the following multiple destination servers** - When a path is configured with this choice, messages received will be routed to multiple downstream servers as follows.
   - If **Round robin** is specified, email will be load-balanced by sending a portion of the email flow through each of the servers specified in the text box in round-robin order. All of the servers will process email all the time.
   - If **Fail over** is specified, the first server listed will handle all email processing under normal operation. If the first server cannot be reached, email will be routed through the second server. If the second server cannot be reached, email will be routed through the third server, and so on.
   - **MTA with MX record routing** - This setting configures this path to route messages by standard MX (Mail Exchange) records. To use this option, your DNS server must be configured to specify the MX records of your internal mail servers that need to receive the email.
   - **MTA with MX record routing (with exceptions)** - This setting configures this path to route messages by standard MX (Mail Exchange) records, except for the specified domains. For the specified domains, route messages directly to the listed IP address.

Note You can specify email addresses in addition to domains in this routing table. Also, hostnames can be specified instead of IP addresses. For example, if you want to route customer service emails to one downstream server and the rest of the traffic to a different downstream server, you can specify some thing like

```
service@mycompany.com   10.1.1.1

mycompany.com   internal_mailserver.mycompany.com
```

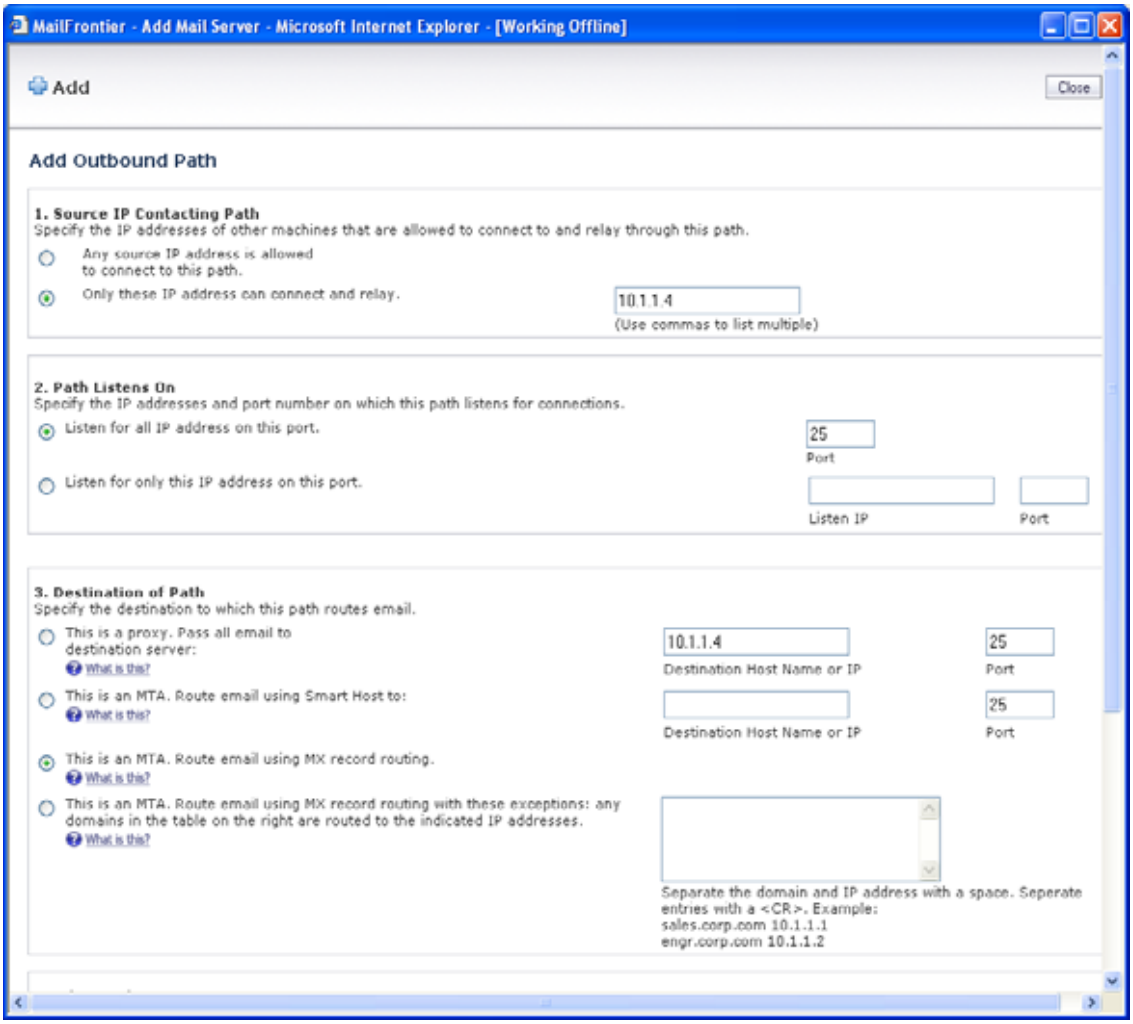
4. Advanced Settings
   - **Use this text instead of a host name in the SMTP banner** - Use this text to customize the HELO banner. By default, the fully qualified domain name will be used
   - Set the action you want to take for messages for email recipients who are not listed in your LDAP server. Typically, it is a good practice to set this path to adhere to corporate settings.
   - **Enable StartTLS on this path** - Check this check box if you want a secure internet connection for email. If the check box is checked, SonicWALL Email Security Gateway uses Transport Layer Security (TLS) to provide the secure internet connection. When StartTLS is enabled, email can be sent and received over a secure socket. The source and destination email addresses and the entire message contents are all encrypted during transfer.

Click **Add** to add an inbound path for this All in One server.

Adding an Outbound Mail Server for All in One Architecture

Click the **Add** button in the **Outbound Email Flow** section. The **Add Outbound Path** window appears, as shown in Figure 6.3.

Figure 6.3 Adding an Outbound Path



1. **Source IP Contacting Path**. In this section, you can specify which servers within your organization can connect to this path to relay outgoing email.
   - **Any source IP address is allowed to connect to this path** - This setting configures this path to receive outgoing email from any server. Using this option could make your server an open relay.
   - **Only these IP addresses can connect and relay** - This setting configures this path to accept email only from the specified IP addresses.
     NOTE: You need to use this setting if you configure your SonicWALL Email Security Gateway installation to listen for both inbound and outbound email traffic on the same IP address on port 25.
2. **Path Listens On**. In this section, you can specify the IP addresses and port number on which this path listens for connections.
   - **Listen for all IP address on this port** - This is the typical setting for most environment as the service listens on the specified port using the machine's default IP address.

- **Listen only on this IP address and port** - If you have multiple IP addresses configured in this machine, you can specify which IP address and port number to listen to.

3. **Destination of Path.** In this section, you can specify the destination server for outgoing email traffic in this path.
   - **This is a Proxy. Pass all email to destination server** - Use this setting if you want this path to act as a proxy and relay messages to an upstream MTA. Enter the host name or IP address of the upstream MTA and the port on which it should be contacted. If the upstream MTA is unavailable, outgoing messages will not be accepted.
   - **This is an MTA. Route email using SmartHost to** - This setting is same as the Proxy option above except that outgoing messages will be accepted and queued if the upstream MTA is unavailable.
   - **This is an MTA. Route email using SmartHost with load balancing to the following multiple destination servers** - When a path is configured with this choice, outbound messages will be routed to multiple upstream MTAs as follows.
   - If Round robin is specified, email will be load-balanced by sending a portion of the email flow through each of the MTAs specified in the text box in round-robin order. All of the MTAs will process email all the time.
   - If Fail over is specified, the first MTA listed will handle all email processing under normal operation. If the first MTA cannot be reached, email will be routed through the second MTA. If the second MTA cannot be reached, email will be routed through the third MTA, and so on.
   - **This is an MTA. Route email using MX record routing** - Use this setting to configure this path to route outbound email messages by standard MX (Mail Exchange) records.
   - **This is an MTA. Route email using MX record routing with these exceptions** - Use this setting to configure this path to route outbound email messages by standard MX (Mail Exchange) records except for the specified domains. For the specified domains, route messages directly to the listed IP address.
4. **Advanced Settings**.
   - **Use this string instead of a host name in the SMTP banner** - Use this string to customize the HELO banner. By default, the fully qualified domain name will be used.

Adding a Server for Split Architecture

If you chose Split Architecture, you must define whether the server is the Control Center or Remote Analyzer, and then let each know about the other.

1. Go to **Server Configuration > Network Architecture**.

2. Choose **Split**.

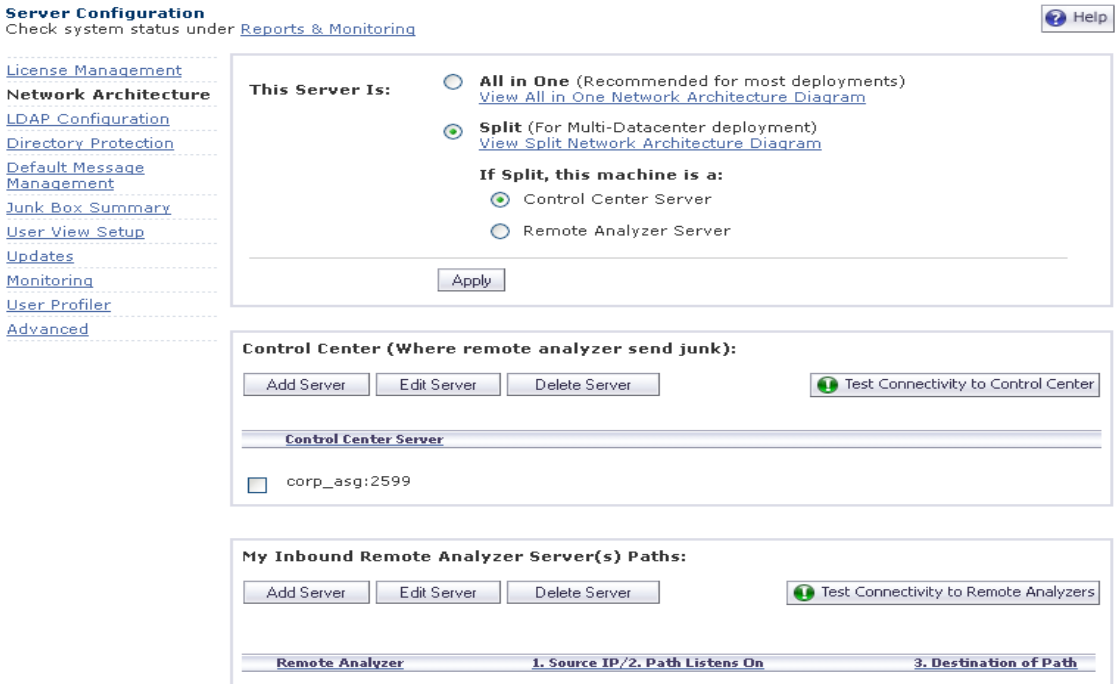


Figure 6.4 Split Configuration Network Architecture

3. Click **Control Center** to configure the server as a Control Center or click **Remote Analyzer** to configure the server as a Remote Analyzer.
4. Click **Apply**.

Adding a Control Center

To add a Control Center:

1. Click **Add Server** in the Control Center section of the Network Architecture window.

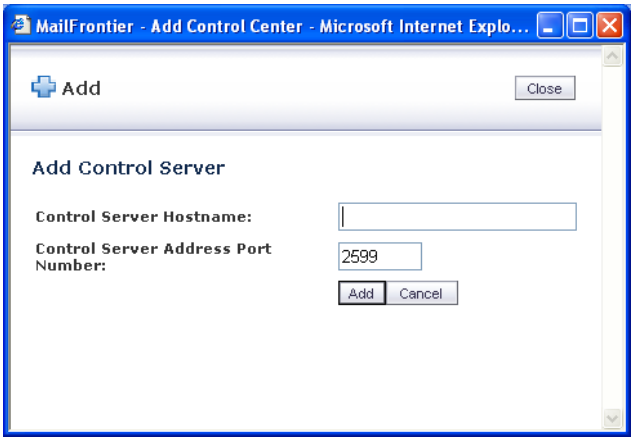


Figure 6.5 Adding a Control Center

2. Enter the **Control Center hostname**.

3. If feasible, use the default port number. If not, enter a new **Control Center Server Address Port Number**.
4. Click **Add**.

Adding a Remote Analyzer

You must add one or more Remote Analyzers to a Split Configuration. Remote Analyzers can process inbound messages or outbound messages or both.

1. Click the **Add Server** button in the Inbound Remote Analyzer or Outbound Remote Analyzer section based on your need.

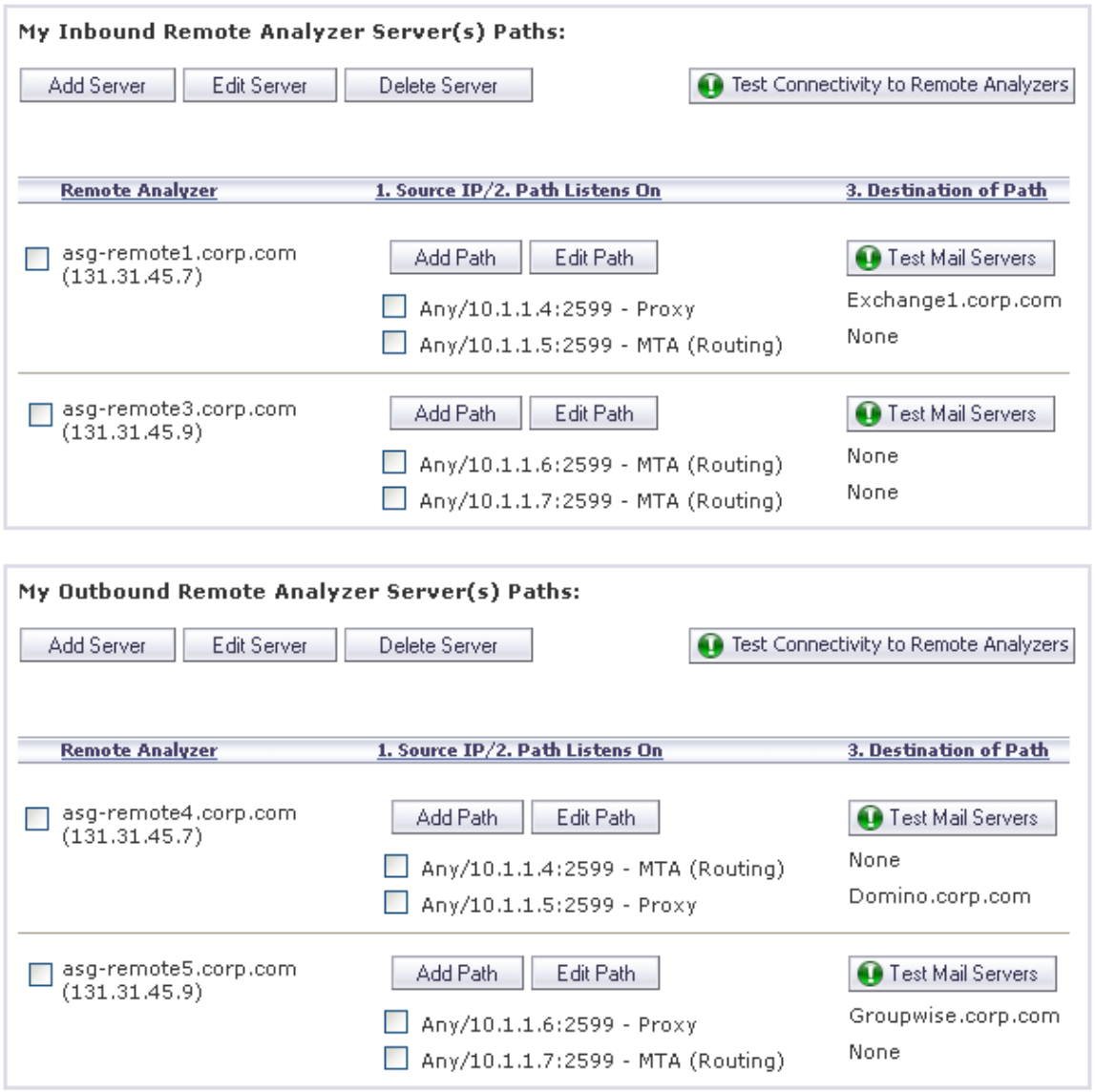


Figure 6.6 Adding a Remote Analyzer

2. Figure 6.7, “Adding Remote Analyzer Server,” on page 61 appears. Enter the Remote Analyzer’s hostname or IP address.

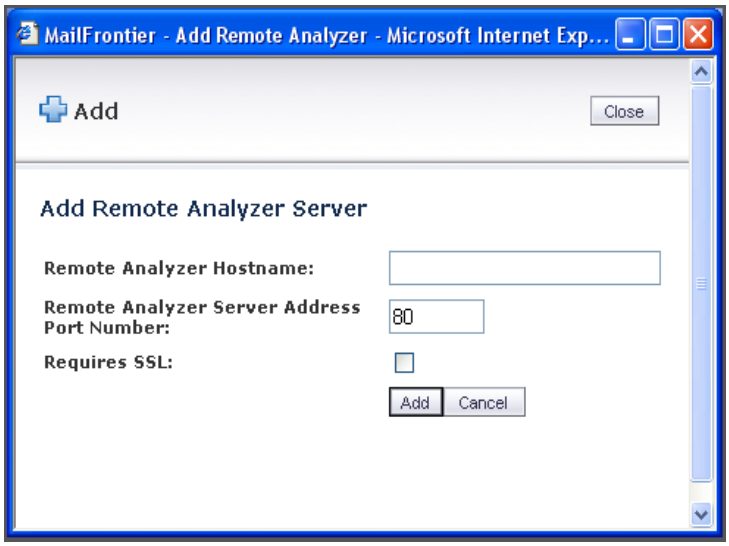


Figure 6.7 Adding Remote Analyzer Server

3. Enter the **Remote Analyzer Server Address Port number**.
4. If your network requires SSL, check the **Requires SSL** check box.
5. Click the **Add** button.

NOTE: If there is a high volume of network traffic, it might take some time before the new Remote Analyzer is displayed in the **Server Configuration>Network Architecture** window.

Any changes you make at the Control Center are propagated to the Remote Analyzers you just added. You can monitor their status on the Reports page as well.

Configuring Inbound Email Flow for a Remote Analyzer

While logged into the Control Center, Click the **Add Path** button next to the Inbound Remote Analyzer. An **Add Inbound Path** window appears. Follow the instructions in “Adding an Inbound Mail Server for All in One Architecture” on page 54.

Configuring Outbound Email Flow for a Remote Analyzer

While logged into the Control Center, Click the **Add Path** button next to the Outbound Remote Analyzer. An **Add Outbound Path** window appears. Follow the instructions in “Adding an Outbound Mail Server for All in One Architecture” on page 57. Make sure that the Control Center can connect and relay email messages through this path - step 1 in the Add Outbound Path dialog.

Configuring Remote Analyzers to Communicate with Control Centers

After you have set up the Control Center, configure each Remote Analyzer so that it can communicate with its Control Center.

1. Log in to each server set up as a Remote Analyzer and go to **Network Architecture**.

2. Click the **Add** button to identify from which Control Center this Remote Analyzer will accept instructions.

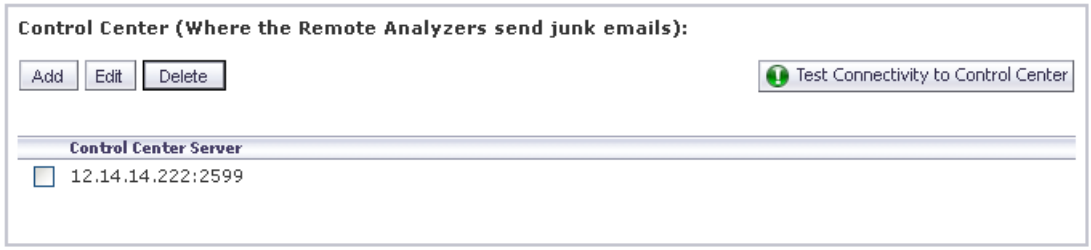


Figure 6.8 Adding the Control Server to a Remote Analyzer

3. An Add Control Center screen appears. Enter the hostname of your **Control Center**.
   If your Control Center is a cluster, you must add each individual hostname as a valid Control Center.

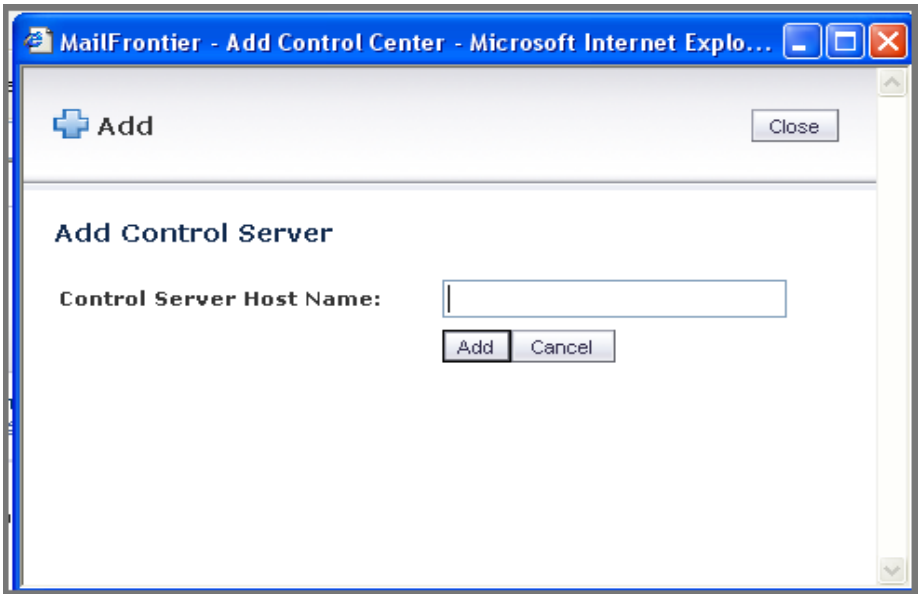


Figure 6.9 Adding Control Center to a Remote Analyzer

NOTE: If your Control Center is a cluster, add each individual hostname as a valid Control Center by repeating steps 2-3.

All other configuration options for the Remote Analyzer are managed by the Control Center.

Deleting a Remote Analyzer from a Split Configuration

Before deleting a Remote Analyzer, ensure there are no messages in the queue for quarantine as follows:

4. Stop SMTP traffic to the Remote Analyzer by turning off the SonicWALL Email Security Gateway Service. Click **Control Panel>Administrative Tools>Services>MlfAGS Gateway> Stop**.
5. After a few minutes, view the last entry in the `mfe` log on the Remote Analyzer log.
6. View the `mfe` log in the Control Center logs directory to ensure the last entry in the `mfe` log for the Remote Analyzer is there: this can take a few moments. For more information on log files, see “SonicWALL Email Security Log Files” on page 197.

Turn off the ability of the associated email server to send mail to this Remote Analyzer, and/or point the associated email server to another installed and configured Remote Analyzer

Testing the Mail Servers

Click the **Test Mail Servers** button. SonicWALL Email Security Gateway displays a window that indicates either a successful test or an unsuccessful test.

NOTE: It takes 15 seconds for SonicWALL Email Security Gateway to refresh its settings. If the first test fails, try the test again.

Figure 6.10 Test Mail Servers Results

Changing from an All in One Configuration to a Split Configuration

There are only two situations that warrant changing your configuration:

- You are a current SonicWALL Email Security customer running All in One architecture and want to upgrade to a Split Network configuration.
- You are a new customer and have incorrectly configured for All in One architecture and you want to configure for Split Network, or vice versa.

CAUTION: Call SonicWALL Email Security Technical Support and work with them to go through these settings.

Configure MTA

Click the Configure MTA button to specify several parameters for the MTA. You can limit the number of inbound and outbound connections that SonicWALL Email Security Gateway will accept. You can also restrict email messages based on message characteristics such as message size and number of recipients.

You can also specify how the MTA will handle the case where it is unable to deliver a message right away. It will retry delivery on the interval specified in the Retry interval drop-down menu, and it will stop trying and bounce the message after the length of time specified in the Bounce after drop-down menu.

Email Address Rewriting

Use this dialog to rewrite email addresses for inbound or outbound emails. These operations affect only the email envelope (the RFC 2821 fields): the email headers are not affected in any way. For inbound email, the “To” field (the RCPT TO field) is rewritten. For outbound email, the” From” field (the MAIL FROM field) is rewritten.

7.

LDAP Configuration

SonicWALL Email Security Gateway uses Lightweight Directory Access Protocol (LDAP) to integrate with your organization's email environment. LDAP is an Internet protocol that email programs use to look up users' contact information from a server. As users and email distribution lists are defined in your mail server, this information is automatically reflected in SonicWALL Email Security Gateway in real time.

Many enterprise network use directory servers like Active Directory or Lotus Domino to manage user information. These directory servers support LDAP and SonicWALL Email Security Gateway can automatically get user information from these directories using the LDAP. You can run SonicWALL Email Security Gateway without access to an LDAP server as well. If your organization does not use a directory server, users cannot access their Junk Boxes, and all inbound email is managed by the message-management settings defined by the administrator.

SonicWALL Email Security Gateway uses the following data from your mail environment.

- Login Name and Password: When a user attempts to log into the SonicWALL Email Security Gateway server, their login name and password are verified against the mail server via LDAP authentication. Therefore, changes made to the user names and passwords are automatically uploaded to SonicWALL Email Security Gateway in real time.
- If your organization allows users to have multiple email aliases, SonicWALL Email Security Gateway ensures any individual settings defined for the user extends to all the user's email aliases. This means that junk sent to those aliases aggregates into the same folder.
- Email groups or distribution lists in your organization are imported into SonicWALL Email Security Gateway. You can manage the settings for the distribution list in the same way as a user's settings.

LDAP groups allow you to assign roles to user groups and set spam-blocking options for user groups.

Configuring LDAP

Use the LDAP Configuration screen to configure SonicWALL Email Security Gateway for username and password authentication for all employees in the enterprise.

NOTE: You must complete the LDAP configuration screen to get the complete list of users who are allowed to login to their Junk Box. If a user does not appear in the User list in the User & Group screen, their email is filtered, but they cannot view their personal Junk Box or change default message management settings.

Enter the server information and login information so that connection to the LDAP server can be tested.

1. Check the **Configure LDAP** check box to enable per-user access and management check box to enable users to log into their Junk Box and change various settings. These settings are limited according to the preferences you set in the User Management pane. See the SonicWALL Email Security *Administration Guide* for details.
2. Enter the following information about your LDAP server:

- **Server Name:** The IP address or DNS name of your LDAP server. (Configuration checklist parameter M)
- **Port**: The TCP port running the LDAP service. The default LDAP port is 389. (Configuration checklist parameter N)
- **SSL Connection**: Check this box if your server requires a secured connection.
- **Type of LDAP Server:** Choose the appropriate type of LDAP server from the list.

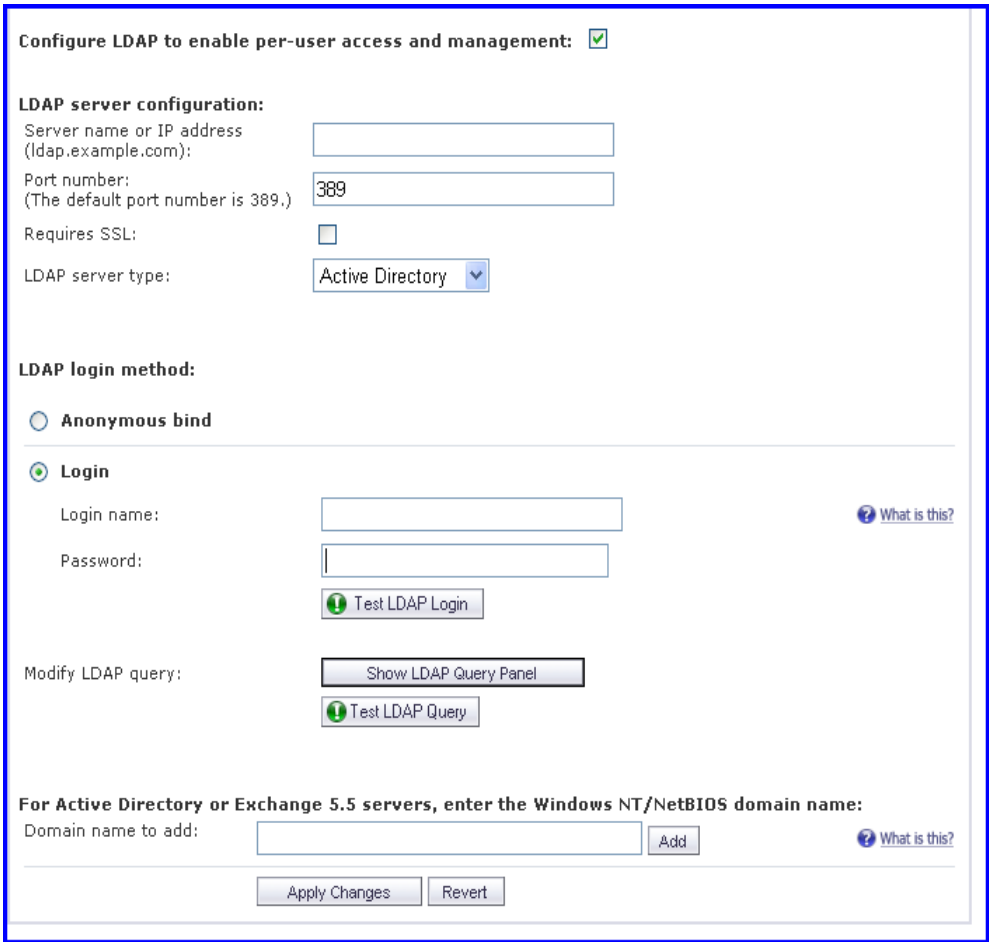


Figure 6.11 LDAP Configuration

3. Determine the **Login** options for your LDAP server:
4. **Anonymous Bind Login Name and Password**: Enter a username and password for a regular user on the network. This typically does not have to be a network administrator.

Note Some LDAP servers allow anybody to get a list of valid email addresses out of them. This state of allowing full access to anybody who asks is called Anonymous Bind. In contrast to Anonymous Bind, most LDAP servers such as Microsoft's Active Directory require a valid username/password in order to get the list of valid email addresses. (Configuration checklist parameter O and P)

5. Click the **Test LDAP query** button.

   A successful test indicates a simple connection was made to the LDAP server. If you are using anonymous bind access, be aware that even if the connection is successful, anonymous bind privileges might not be high enough to retrieve the data required by SonicWALL Email Security Gateway.
6. (Optional) Click the **Show LDAP Query Panel** button to configure advanced LDAP settings. See “Advanced LDAP Settings” on page 66.
7. Click **Apply Changes**.

Note After you configure LDAP, you can give other users within your organization administrative rights. These users will also be emailed if SonicWALL Email Security Gateway experiences problems.

Advanced LDAP Settings

To access the **Advanced LDAP** settings window, click the **Show LDAP Query Panel** button in the LDAP Configuration window.

NOTE: SonicWALL Email Security does not require you to configure advanced LDAP settings for most installations.

CAUTION: Use this feature only if you need to modify your LDAP configuration. Clicking the **AutoFill** button usually produces valid entries. SonicWALL Email Security recommends that you call Technical Support before changing these settings.

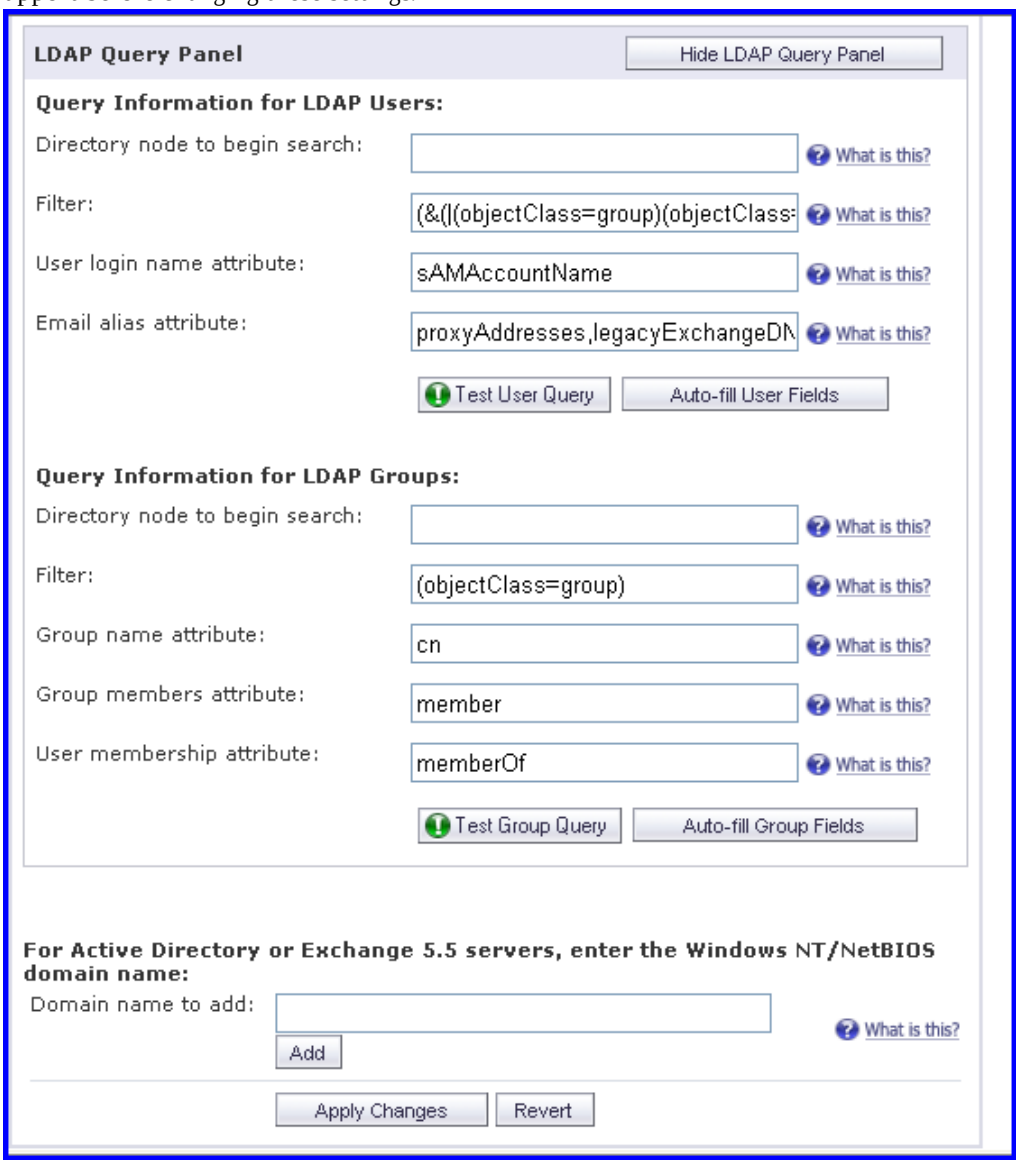


Figure 6.12 Advanced LDAP settings

To configure advanced LDAP settings for users:

1. Enter values for the following fields:
   - **Directory node to begin search:** The node of the LDAP directory to start a search for users. (Configuration checklist parameter Q).
   - **Filter:** The LDAP filter used to retrieve users from the directory.
   - **User login name attribute:** the LDAP attribute that corresponds to the user ID.
   - **Email alias attribute:** The LDAP attribute that corresponds to email aliases.
2. Click the **Test Group Query** button to verify that the configuration is correct.
3. Click the **Auto-fill User Fields** button to have SonicWALL Email Security Gateway automatically complete the remainder of this form.
4. To configure **LDAP Settings for Groups**, enter values for the following fields:
   - **Directory node to begin search:** The node of the LDAP directory to start a search for users. (Configuration checklist parameter Q). For information on how to discover your organization's primary directory node, see Appendix A, "LDAP".
   - **Filter**: the LDAP filter used to retrieve groups from the directory.
   - **Group name attribute**: the LDAP attribute that corresponds to group names.
   - **Group members attribute:** the LDAP attribute that corresponds to group members.
   - **User member attribute:** the LDAP attribute that specifies attribute inside each user's entry in LDAP that lists the groups or mailing lists that this user is a member of.
5. Click the **Apply Changes** button.

Note Be aware that if you have a lot of user mailboxes, applying these changes could take a several minutes.

Directory Protection

Spammers not only threaten your network with junk mail; they stage Directory Harvest Attacks (DHA) to get a list of all users in an organization's directory. DHA makes unprotected organizations vulnerable to increased attacks on their email and other data systems.

How DHA Threatens Your Network

DHA can threaten your network in the following ways:

- Expose the users in your directory to spammers

  The people at your organization need their privacy in order to be effective. To expose them to malicious hackers puts them and the organization at significant risk from a variety of sources.

  Users whose email addresses have been harvested are at risk. Once a malicious hacker knows their email, users are at risk for being spoofed: someone can try to impersonate their email identity. In addition, exposed users can be vulnerable to spoofing by others. IT departments routinely receive email from people pretending to be providing upstream services, such as DNS services.

- Expose users to phishing

  Exposed users can be targeted to receive fraudulent email. Some receive legitimate-appearing email from banks or credit cards asking for personal or financial information.

Some exposed users have been blackmailed; Reuters reported cases where users were told if they did not pay up, their computers would be infected with viruses or pornographic material.

- Expose your organization to Denial of Service Attacks

  DHA can lead to denial of service attacks because malicious hackers can send lots of information to valid email addresses in an effort to overwhelm the capacity of your mail server.

- Expose your organization to viruses

  DHA provides a highly effective means of delivering virus-infected email to users.

- Personalized email masquerades as good email

  Directory Harvest Attacks can perpetuate fraudulent email messages by giving malicious hackers the ability to target your users individually and by name.

Protecting your Directory

To protect your directory and users:

1. Go to **Server Configuration->Directory Protection**.
   The window in <Xref_Color>Figure 6.13 appears.

Figure 6.13 Directory Harvest Attacks

2. Choose one of the following options to deal with DHA, as shown in Table 1 on page 68.

Table 1 DHA Options

Options	Consequences
1. Process all messages the same (whether or not email address is in LDAP) **No action is taken on messages to invalid recipients.**	**No directory protection.**
2. Permanently Delete **All email addressed to users not in the organization's directory is permanently deleted.**	**The sender does not receive notification about the email they have sent. This option can lead to permanently deleting legitimate mail with a typographical error in the address.**

Table 1 DHA Options (continued)

Options (continued)	Consequences
3. Reject invalid address (550) **Email to valid addresses are delivered. Email to invalid addresses are sent back to the sender with a message indicating that the addressee is not available.**	**Caution: This provides some information about the users in your directory to outside people. However, your upstream email server might also notify the sender that the address was invalid.**
4. Always store in Junk Box (regardless of spam rating). **Email that is sent to an invalid address is stored in the Junk Box. SonicWALL Email Security does not process the email to determine if it is spam or another form of unwanted email.**	**SonicWALL Email Security recommends this option to protect the confidentiality of your directory population.**

Enable Tarpitting Protection

Click the **Enable Tarpitting Protection** checkbox to discourage DHA. Tarpitting discourages spamming without permanently blocking an offending IP address. SonicWALL Email Security Gateway maintains a record of the percentage of good and invalid email messages that come from each IP address. IP addresses that send a large number of invalid addresses are tarpitted; that is, email from these addresses is delayed for some time period to slow down the rate that they can attack an organization's mail system.

NOTE: You can enable tarpitting regardless of the option you chose above for email that does not match the LDAP listings.

Default Message Management Settings

The Default Message Settings window enables the administrator to set default settings for users' messages, as shown in Figure 6.14.

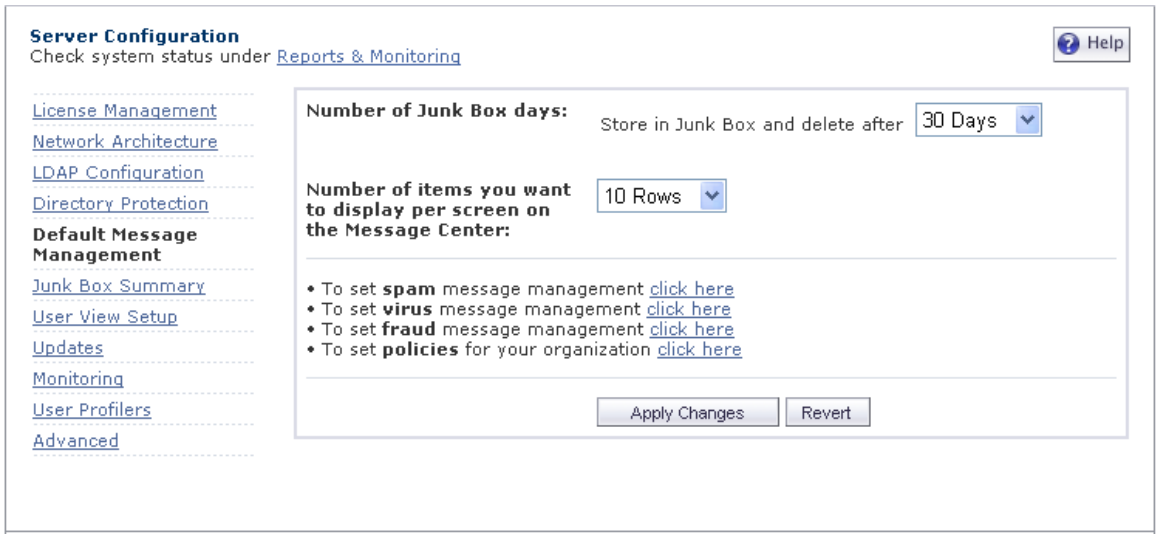


Figure 6.14 Default Message Management Settings

The Default Message Settings window allows you to choose default settings for messages that contain spam, phishing, virus, and policy management issues.

1. Choose the number of **Junk Box days** from the drop-down list.

   Set the enterprise-wide policy for the number of days email messages will remain in the Junk Box before being automatically deleted. The maximum number of days is 180. This can be adjusted for an individual user by an administrator or the user, if you allow it (See Configuring the User View Setup on page 68.)

2. Choose the **number of items to display in the Message Center** from the drop-down list.

3. What do you want to do with messages marked as Junk or Likely Junk?

   Configure the enterprise-wide default policy for handling of junk mail or likely junk mail. This setting can be overridden for an individual user by an administrator or optionally by the user themselves. Choose one of the following options:

Table 2 ***Junk and Likely Junk Email Handling Options***

Options	Definition
Nothing (Do not process)	All incoming email is scanned for spam, but delivered to the recipients. (Nothing goes into the Junk Box.) SonicWALL Email Security Gateway will still gather statistics about spam deliveries even though no processing takes place.
Permanently Delete	Junk email is removed. Use this option with care. Deleted email cannot be retrieved.
Bounce Back to Sender	Returns the junk email message to the sender without accepting it. Upon reading the bounce, the sender will believe the recipient does not exist.
Store in Junk Box	Junk email is quarantined in the Junk Box for review by IT or the user. The number of days email is stored before deletion is set above, Number of Junk Box Days.
Send to (email address)	Junk email is directed to a specific email address.
Tag with ...	The junk email subject line is tagged with text such as “[Maybe Junk]” and sent to the recipient.

4. Click the **go here** links to manage spam, virus, phishing, and policy.

5. Click **Apply Changes**.

Junk Box Summary

SonicWALL Email Security Gateway sends an email message to users listing all the messages that have been placed in their Junk Box. Users can unjunk items listed in the Junk Box Summary email by clicking links in the email.

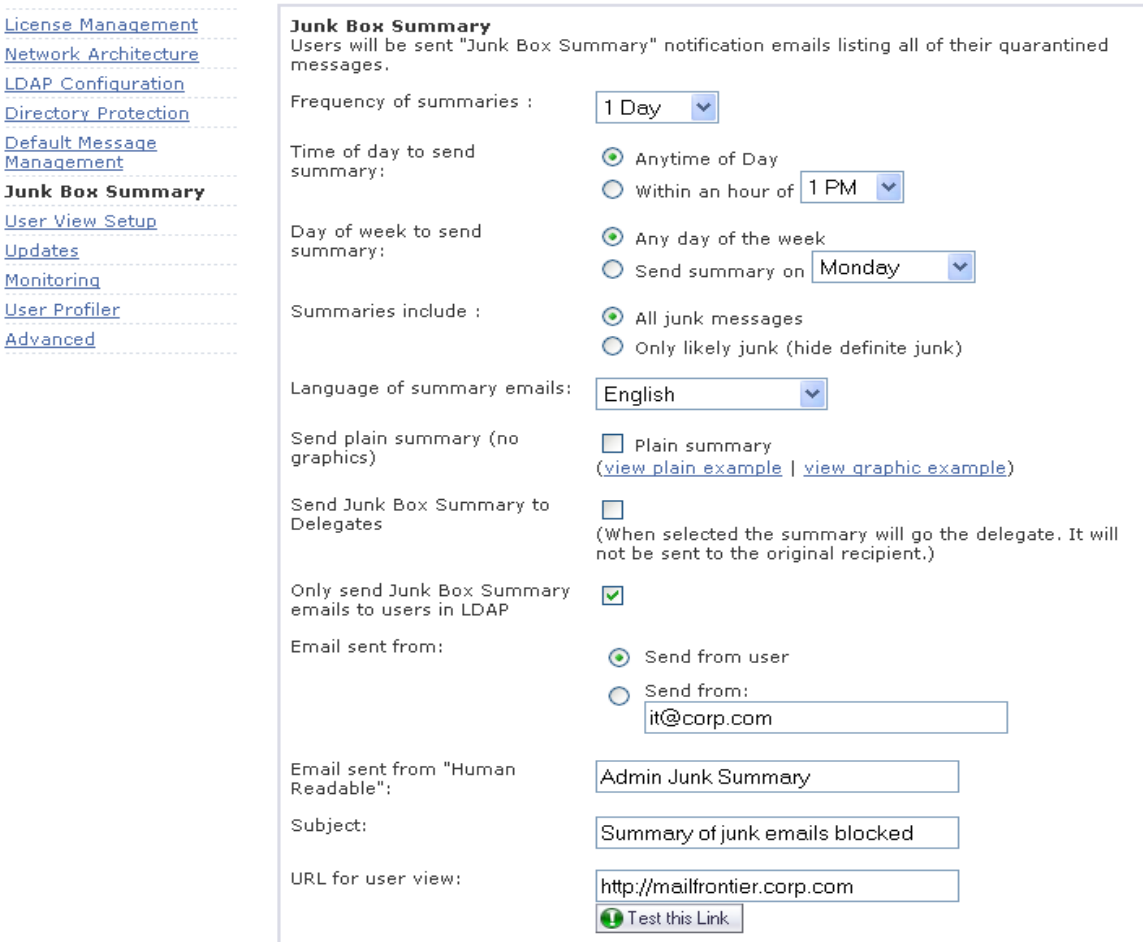


Figure 6.15 Junk Box Summary

To manage the Junk Box summary:

1. Choose **Default Mail Frequency** from the drop-down box.
2. Choose the **dates and times to receive email notification.** Individual users can override these settings.
3. Check the check box to **Send Junk Notifications Only send to LDAP Users**.
4. Choose whether to include in message summary **All Junk Messages** or **Likely Junk Only** (hide definite junk).
5. Choose **Language to send Summary** from the drop-down list.
6. Choose a plain or graphics rich summary.
7. If a delegate has been assigned to manage an user's Junk Box, select the summary for that user to be sent to the assigned delegate.
8. Select to send summary only to users in LDAP.
9. Email Sent From

   The message summary can come from the individual user or another email address which you enter here. Be aware that if summaries are sent because the address doesn't exist, the message summary message will bounce as well.
10. Select the name to be displayed in end user's email client for the summary emails.

11. Subject

    Enter the subject line for the Junk Box Summary email.

12. URL for User View

    This text box is filled in automatically based on your server configuration and is included in the Junk Box Summary email. Clicking on the email link will allow users to unjunk messages. Test the link if you make any changes to ensure connectivity. If you are using multiple SonicWALL Email Security Gateways, enter the virtual hostname here.

- Test this Link

  Users unjunk items in the Junk Box summary email by clicking links in the email. To test the URL, click Test this Link. If the test fails, check that the URL is correct. (Installation checklist parameters B, C, D)

13. Click the **Apply Changes** button.

User View Setup

Using these screens, the administrator can configure whether and how the end users of the SonicWALL Email Security Gateway server access the system and what capabilities of the system are exposed to the end users.

The following options are available in this screen:

1. You can configure the **HTTP settings**. For example, you can change the port number to be used by SonicWALL Email Security Gateway's user interface for HTTP access. You can also configure HTTPS access by selecting the **Enable https access on port** checkbox. By default, a generic self-signed certificate is created. If you need a certificate specific to the machine's host name or a 3rd party certificate from a well known certificate authority, click the **Settings** button.

   Also, you can click the **Redirect access from http to https** checkbox if you always want the users to connect through HTTPS.

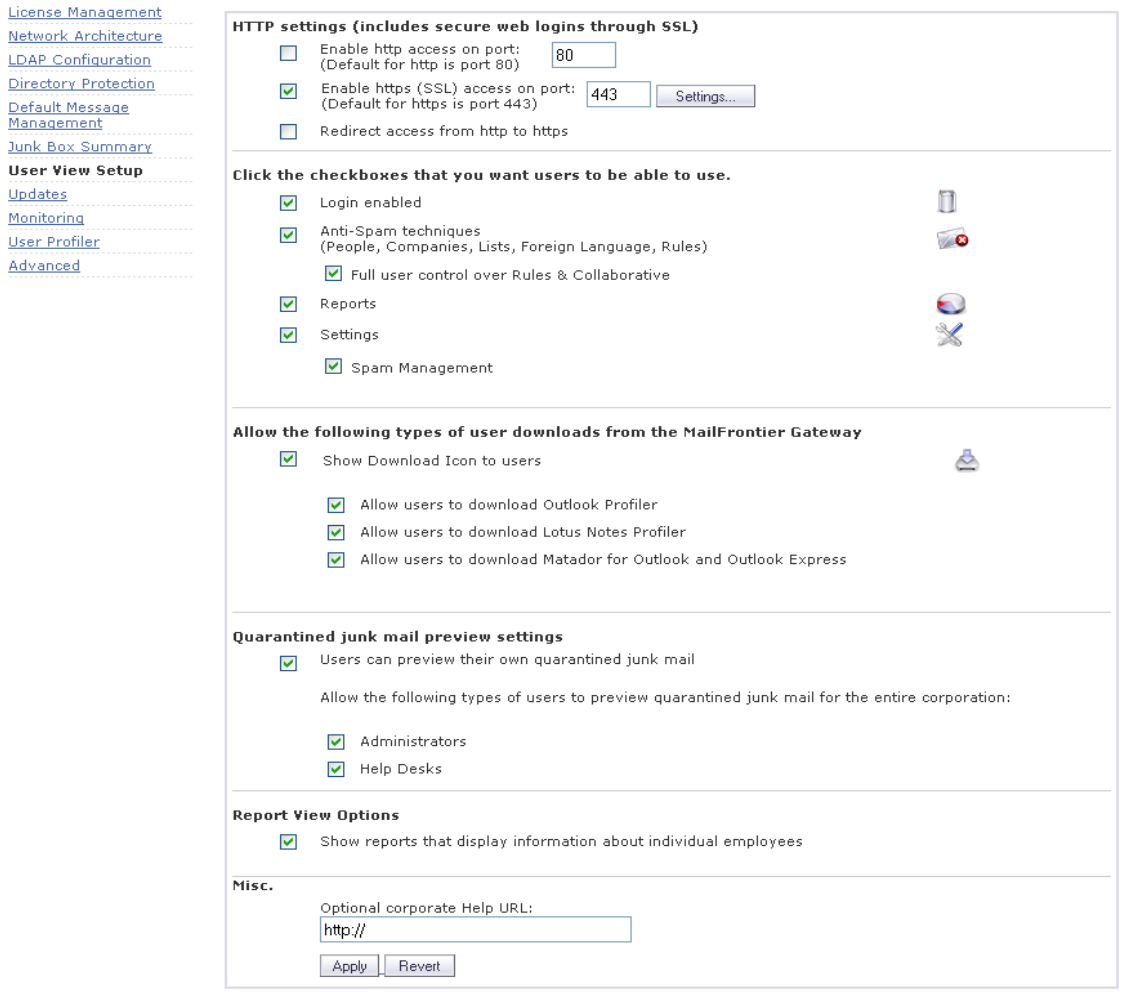


Figure 6.16 User View Setup Page

2. Check the **Login enabled** check box to allow users to access their junk boxes.

   This allows users to log into SonicWALL Email Security Gateway and have access to their per-user Junk Box. If you disable this, mail will still be analyzed and quarantined, but users will not have access to their Junk Box. It makes SonicWALL Email Security Gateway operate in a manner that is not visible to the user.

3. Click **Full Control over Rules and Collaboration** to force users to adhere to the aggressiveness settings configured by the administrator in Rules and Collaboration.

   They can set their individual settings more aggressively, but cannot change settings to any less aggressive than the one that the administrator has set for the organization.

4. Check the **Reports** check box to allow users to view SonicWALL Email Security Gateway reports.

   Enabling reports allows users to view the Inbound Messages Processed Report, the Outbound Messages Processed Report, and the Junk Breakdown Report. Users cannot configure any reports.

5. Click the **Settings** check box to enable users to view their spam aggressiveness settings.

6. Click the **Junk mail management** check box to enable users to customize the actions SonicWALL Email Security Gateway takes on their junk email. (Not all settings can be customized.)

7. Determine user download settings.

- Check the **Show download icon to users** to allow users to download Profilers and SonicWALL Email Security Desktop.
- Check the **Allow Outlook Profiler download** checkbox to allow users to download the Outlook Profiler.
- Check the **Allow Lotus Notes download** checkbox to allow users to download the Outlook Profiler.
- Check the **Allow** SonicWALL Email Security **Desktop for Outlook and Outlook Express download** check box to allow users to download SonicWALL Email Security Desktop.

8. Determine who can preview quarantined mail.
   - Check the **Users can preview their own quarantined junk mail** check box to enable users to view their individual mail that is junked.
9. Check the following check boxes to enable the types of users who can preview quarantined junk mail for the entire organization.
   - Administrators
   - Help Desks
10. Enter an **Optional login help URL.**

    An administrator can specify a URL for any customized help web page for users to view on the Login screen. If no URL is entered, SonicWALL Email Security Gateway provides a default login help screen. If a URL is entered, that page is launched when the user clicks the **Login Help** link.
11. Click **Apply Changes**.

Updates

SonicWALL Email Security uses collaborative techniques as one of many tools in blocking junk messages. The collaborative database incorporates thumbprints of junked email from SonicWALL Email Security Desktop and SonicWALL Email Security Gateway users. Your SonicWALL Email Security Gateway communicates with a data center hosted by SonicWALL Email Security (using the HTTP protocol) to download data used to block spam, phishing, virus and other evolving threats. This page is shown below in

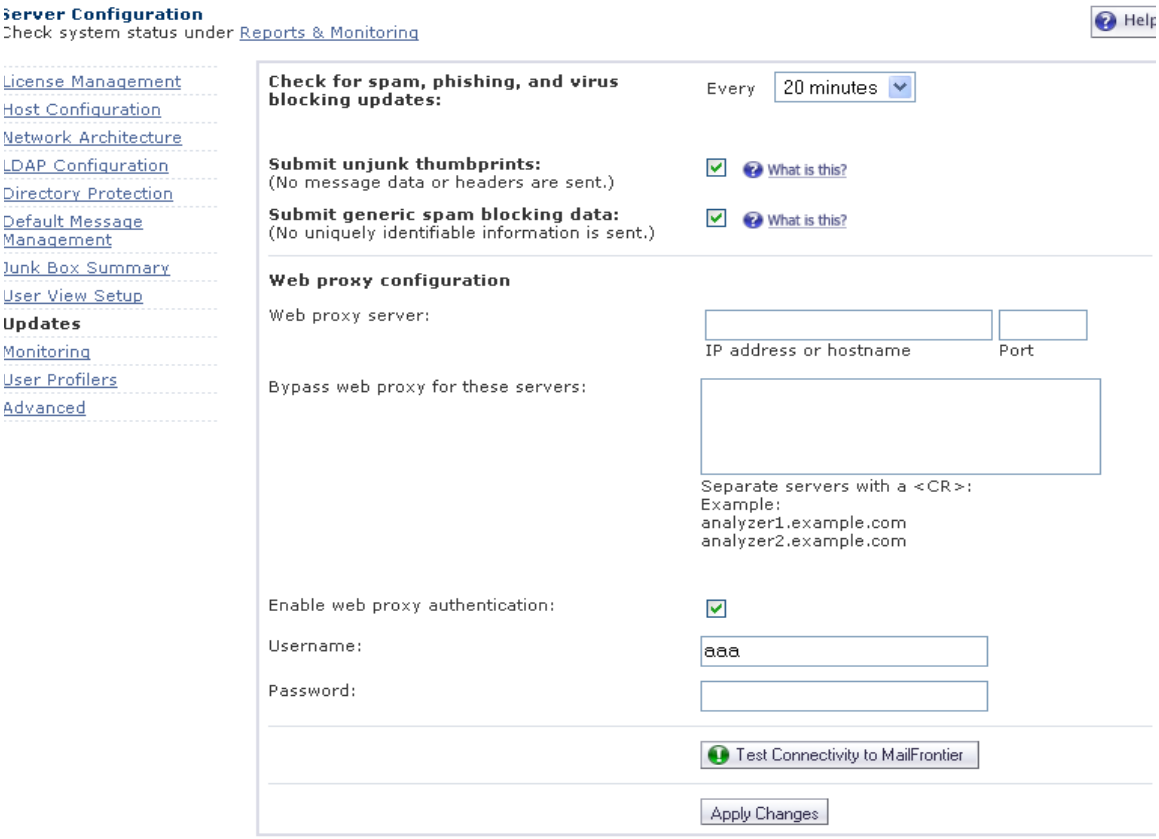


Figure 6.17 Updates Window

SonicWALL Email Security recommends that you check for spam, phishing, and virus blocking updates at least every twenty minutes.

Check the **Submit unjunk thumbprints** check box to submit thumbprints to the SonicWALL Email Security data center when users unjunk a message. Thumbprints sent from SonicWALL Email Security Gateway contribute to the collaborative community by improving junk-blocking accuracy. They contain absolutely no readable information.

Check the **Submit generic spam blocking data** check box to send generic spam-blocking data to the SonicWALL Email Security data center to assist in customer support and to help improve spam blocking. No emails, email content, header information or any other uniquely identifiable information is ever sent.

Web proxy configuration

When your SonicWALL Email Security Gateway contacts the SonicWALL Email Security hosted data center to download data, it uses the HTTP protocol. If your organization routes HTTP traffic through a proxy, you can specify the proxy server here. You can also allow HTTP traffic from certain servers to bypass the proxy server. You may want to do this for data transferred between SonicWALL Email Security Gateway servers within your organization.

If your organization routes HTTP traffic through a proxy which requires basic authentication, you can enter the username and password to configure SonicWALL Email Security Gateway to authenticate with the HTTP proxy server.

Test Connectivity to SonicWALL Email Security

Test that communication through the web proxy is working. Click the **Test Connectivity to** SonicWALL Email Security button to ensure that SonicWALL Email Security Gateway has access to the SonicWALL Email Security hosted data center.

Figure 6.18 illustrates the successful test response.

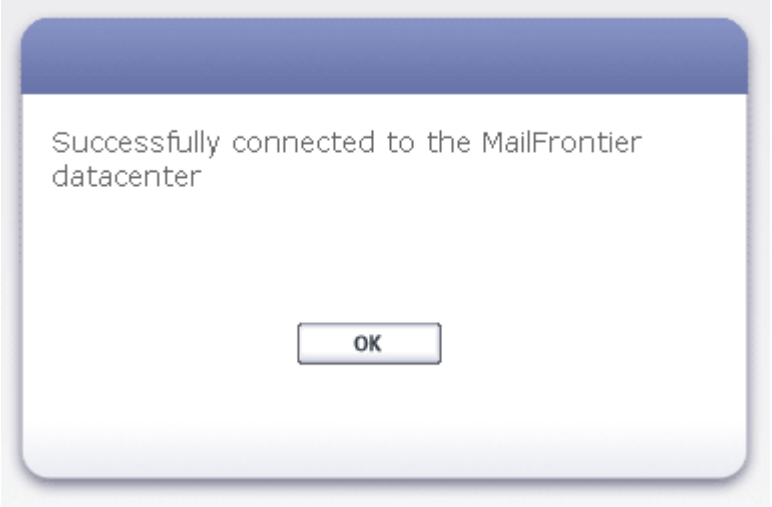


Figure 6.18 Successful Connectivity Test

Monitoring

Use the Monitoring page to enter the email addresses of administrators who receive emergency alerts, outbound quarantine notifications, and the postmaster for the MTA.

You can also enter the names or IP addresses of backup SMTP servers. If you are running SonicWALL Email Security Gateway in split mode, and you route outbound email through SonicWALL Email Security Gateway, you must enter the IP addresses or fully-qualified domain names of any Remote Analyzers through which outbound email is routed in this text box on the Control Center.

User Profilers

A User Profiler is an optional software module that you can run either on your users desktops or on your SMTP server to collect a profile of their email communication and use that profile in SonicWALL Email Security Gateway to increase the effectiveness of the server in dealing with constantly evolving threats. It allows for automatic, per user customization in the form of allowed list, based on the individual users email profile. This data is then posted through HTTP(S) to the SonicWALL Email Security Gateway where it is mapped to the user's id to update the user's allowed lists.

User Profilers need to be installed separately and can be installed any time after SonicWALL Email Security Gateway is installed. There are different User Profilers and directions for installing each User Profiler are given below and are also contained in a `readme.txt` file in the folder where you installed SonicWALL Email Security Gateway, for example:

```
c:\Program Files\MailFrontierEG\Profilers\LotusNotes
```

Installing the User Profiler for Microsoft Exchange

Exchange User Profiler runs as a windows service and can be installed either directly on the Exchange Server or on the server running the SonicWALL Email Security Gateway. In both cases, the Exchange User Profiler creates allowed lists approximately every five minutes by looking at the outbound SMTP logs.

If it is installed on a server other than the Exchange Server, Windows file sharing is used to read the Exchange log files remotely. These logs files are shared by default (Exchange 5.5 users, see the note below regarding turning the trace log on) and are typically accessed as follows:

On Exchange 2000:

```
Share:   \\EXCHANGE_MACHINE_NAME\EXCHANGE_MACHINE_NAME.log
Locally: C:\Program Files\exchsrvr\EXCHANE_MACHINE_NAME.log
```

On Exchange 5.5:

```
Share:   \\EXCHANGE_MACHINE_NAME\tracking.log
Locally: C:\exchsrvr\tracking.log
```

To run the Exchange User Profiler installer:

1. Run the Installer available under the directory `Profilers\MicrosoftExchange` in SonicWALL Email Security Gateway installation directory.
2. This step is for Exchange 5.5 only. Enable the Exchange 5.5 tracking log by accessing **Microsoft Exchange Administrator > Configuration > Connections.** Browse to the **Internet Mail Service**. Open the **Properties** page and check the box at the bottom of the Internet Mail tab.

   NOTE: Make sure you do not access the extended logging files. These files have file names that look like `ex`*`date`*`.log`.
3. Set READ permission.

   In order to run the User Profiler for Microsoft Exchange via file sharing, the shares mentioned above need to allow read-only access for the `Mlfasg Profiler` service wherever it is installed. The easiest way to do this is to add READ access for the entire server that this service is installed on.

Setting up READ permission to the Exchange Log Folder

If the `Mlfasg` Exchange Profiler Service is running to log on using the Local System Account (install default), add the SonicWALL Email Security Gateway computer object to the Exchange log folder's Share Permissions.

To add READ permission for a computer object to the Exchange log folder:

1. On the Exchange server, open the **Properties** dialog for the log folder
2. Select the **Sharing** tab and click the **Permissions** button.
3. In the Permissions dialog, click the **Add...** button.
4. In the **Add** dialog find the SonicWALL Email Security Gateway computer in the list, and click **Add.**
5. Apply the changes by clicking **OK** until you have closed all the dialog boxes.
6. Stop and restart the **Mlfasg Profiler** service from the Services Administrative tool.

Setting up READ permission to the Mlfasg Profiler Service

An alternate method for allowing the `Mlfasg` Profiler Service to have READ permissions to the Exchange log file directory is to run the SonicWALL Email Security Gateway Exchange Profiler Service and log on as a specific user who has READ permissions for this directory. Follow the above steps for adding READ permissions for a computer, but add a specific username object instead of the SonicWALL Email Security Gateway computer object. Then, change the `MlfAsg` Profiler Service property so that the service runs as this user.

To change the user for which the `MlfAsg` Profiler Service runs:

1. Right click the **MlfAsg Profiler Service** in the Services Administrative tool and select **Properties**.
2. In the Properties dialog click the **Log On** tab.
3. Click **This account**.
4. Enter a **Username** and **password** in the corresponding text fields
5. Click **OK** to apply the changes.
6. Stop and restart the MlfAsg Profiler service from the **Services Administrative tool**.

Checking the Profiler Services Output

You can confirm that the Profiler is working by checking the timestamp on the directories and files in `addrbk` directory in the SonicWALL Email Security Gateway installation location.

Below is a sample SonicWALL Email Security Gateway install location:

```
C:\Program Files\MailFrontierEG\data\peruser
```

As email is sent out through the Exchange server, the files and timestamp of the corresponding user's *addrbk* files in these directories are updated approximately every five minutes. Stopping and restarting the `MlfAsg Profiler` service also causes files and their timestamps to be updated in these directories since the last time the `MlfAsg Profiler` service was stopped and restarted.

Alternatively, if you want to reprocess all the log files, you can delete all files in the Exchange Profiler log directory except the logging level and install directories and then stop and restart the `MlfAsg Profiler` service.

If the Profiler does not appear to be working, check the `mlfexchp.log` file, which is located in the directory where you installed the user profiler. This file indicates if the XML file created by the Exchange user profiler that contains allowed list data has successfully posted to SonicWALL Email Security Gateway. If the user profiler is still not working, see the "Troubleshooting from the Command Line".

Troubleshooting from the Command Line

You can troubleshoot the Exchange Profiler by typing the a command similar to the following in a command line window:

```
mlfexchp.exe -[command] –[log type] log file air... -[url]
http://https:// -[interval] minutes -logginglevel
```

<Xref_Color>Table 3 lists commands that you can include in the line above.

Table 3 Troubleshooting Commands

Commands	Description
debug	Runs in as a console application
service	**Starts a service** **NOTE: Use** net start MailFrontier Exchange Profiler Service **instead of** service**.**
install	**Installs and starts a service**
remove	**Removes the service**
Log Types	e2k **– Exchange 2000 Log Format** **e55 – Exchange 5.5 Log Format**
URL	**Example 1:** http://*EGmachine*/addrbk **Example 2:** https://*EGmachine*/addrbk- for SSL enabled
Interval (optional)	This interval is in minutes. If you do not enter a value, the timer will default to every 5 minutes.

For more information on troubleshooting, see Chapter 11 of the SonicWALL Email Security *Administrator's Guide*.

Debug Examples:

Console application (on Exchange server):

mlfexchp.exe –debug –url http://*egmachine*/addrbk

Console application (not on Exchange server):

mlfexchp.exe –debug –e2k C:\logs \\blackcomb\blackcomb.log –url http://*asgmachine*/addrbk 2

Securing Exchange Profiler Communication with SonicWALL Email Security Gateway

1. Obtain and import an SSL certificate from a certificate authority, and configure SonicWALL Email Security Gateway to use the certificate. See "Secure Socket Layer" on page 183 for instructions.
2. Install the SSL-signed certificate that SonicWALL Email Security Gateway uses on the server running the Exchange Profiler as follows:
   - From the browser, access **Tools>Internet Options**.
   - Click the **Content** tab.
   - Click the **Certificates** button.
   - Click the **Import** button.
3. The Certificate Import wizard appears.
   Follow the prompts.

Installing the User Profiler for Outlook

You can install the Outlook User Profiler by either using the self-extracting `.EXE` file or creating your own install script using the `.BAT` and `.REG` files. The required files can be found under the directory `Profilers\MicrosoftOutlook` in SonicWALL Email Security Gateway installation directory.

Using the Self-Extracting .EXE (interactive installer)

1. Copy the `InstOutlookProfiler.exe` program file from the `Profilers\MicrosoftOutlook` to the user's desktop.
2. From the `Profilers\Microsoft` Outlook directory, double click `InstOutlookProfiler.exe` and follow the prompts.
3. When the installer ask you for your SonicWALL Email Security Gateway server name and its HTTP port number, enter the hostname and port numbers (default values are port are port `80` for a regular connection, and port 443 for a secure connection).

NOTE: If you want to run the Outlook User Profiler silently, specify the **`/s flag with -server host:port`**

EXAMPLE:

```
instOutlookProfiler.exe /s -server httP;//mountain:80
```

To test if the Outlook User Profiler successfully created allowed list addresses, log in to SonicWALL Email Security Gateway Web server as a user. Click the **People** icon. All the Allowed list addresses should appear.

Creating Your Own Installation Script Using the .BAT and .REG Files

1. Edit the example `InstallUserProfiler.bat` file so that it contains a URL for your SonicWALL Email Security Gateway Web server and has a location from which the users can copy the required files.
2. Edit the `eg_webserver.reg` file so that it contains the proper installation path to the `mlfusero.dll` as specified in the `InstallUserProfiler.bat` file.
3. Register the User Profiler on each individual's computer. You can do this through a domain login script.
4. On the user's desktop where you want to run the User Profiler, invoke the remote batch file. This copies and registers the User Profiler. It also copies a `.REG` file and runs `regedit` on it to register the Web server with which the Outlook User Profiler communicates. The Outlook User Profiler is activated the next time the user starts Outlook.
5. To test if the Outlook User Profiler successfully created Allowed list addresses, log in to SonicWALL Email Security Gateway Web server as a user. Click the **People** icon. All the Allowed list addresses should appear.

Login Scripts

If your organization uses login scripts, a sample login script, named `InstallUserProfiler.bat,` is included in the `Profilers\MicrosoftOutlook` folder in SonicWALL Email Security Gateway installation directory. The script copies over the DLL to your user's computer, registers the DLL, and inserts one key into the Windows Registry.

Note that you can invoke `InstallUserprofiler.bat` as part of an Exchange Server logon script.

Securing Outlook Profile communication with SonicWALL Email Security Gateway

1. Obtain and import an SSL certificate from a certificate authority, and configure SonicWALL Email Security Gateway to use the certificate. See “Secure Socket Layer” on page 183 for instructions.
2. Install the SSL signed certificate that SonicWALL Email Security Gateway uses on the users’ personal computers as follows:
3. From the browser, access **Tools>Internet Options.**
4. Click the **Content** tab.
5. Click the **Certificates** button.
6. Click the **Import** button.

   The Certificate Import wizard appears. Follow the prompts.

Installing the Lotus Notes User Profiler

You can install the Lotus Notes User Profiler by either using the self-extracting `.EXE` file or creating your own installer.

Using the self extracting .EXE (Interactive Installer).

1. Copy the `instLotusProfiler.exe` program file from the `Profilers\LotusNotes` directory to the user's desktop.
2. The installer prompts you for your SonicWALL Email Security Gateway server name and its HTTP port number.

Note To run the Lotus Notes User Profiler silently, specify the `/s` flag with `-server host:port`, for example:

```
instOutlookProfiler.exe /s -server http://mtlilac:80
```

3. To test if the Lotus Notes User Profiler successfully created Allowed lists, log in to SonicWALL Email Security Gateway Web server as a user. Click the **People** icon. All the Allowed list addresses should appear.

Creating Your Own Installer For Lotus Notes

1. Register the `mlfuserl.dll` in the `Profilers\LotusNotes` directory by copying it into the `Lotus\Notes` directory.
2. Edit the `notes.ini` file and add the line `EXTMGR_ADDINS=MLFUSERL`. If `EXTMGR_ADDINS` already exists, append it to the line using `MLFUSERL`.
3. Set an `HKEY_CURRENT_USER\Software\MailFrontier` string value for Web server to tell the Lotus Notes Profiler where to post the data. Include the host and port in this value.

```
EXAMPLE:
http://asg.company.com:80/addrbk
```

Login Scripts for Lotus Notes

If your organization uses login scripts, the installation program, `InsLotusProfiler.exe,` can easily be scripted to run in silent mode.

Installing Sendmail and Postfix Profilers for Solaris

For installation instructions for these two profilers, see the *readme.txt* file in the SonicWALL Email Security Gateway directory, `Profilers\SolarisSendmail` or `Profilers\SolarisPostfix.`

Configuring Advanced Settings

The Advanced Settings window enables you to configure logging levels, customize the SMTP banner, specify LDAP page size, and other advanced features. Under most circumstances, you would not need to change these settings.

Configure the following settings:

1. **Log Level**: Use this setting to change the log level for SonicWALL Email Security Gateway. By default, logging is enabled at level 3. You can set event logging from level 1, for maximum logging, to level 6, for minimum logging. The log files roll over when they reach 50 MBytes. At most, there are five revisions of the file at any time.

   NOTE: Do *not* adjust the log level unless you are troubleshooting a specific problem with the help of SonicWALL Email Security's Technical Support staff.

2. **Customize the SMTP banner**. Use this setting to customize the SMTP banner. When remote SMTP servers contact SonicWALL Email Security Gateway to send email through it, they see an SMTP header that identifies the server with whom they are communicating as a SonicWALL Email Security server. Some companies might want to hide this information and present their own custom SMTP banner header information. Be sure to use valid characters and syntax for an SMTP header.

3. **Replace** SonicWALL Email Security **in "Received:" headers**: Use this setting to replace the name in the Received: header. If you do not want to have the SonicWALL Email Security name in the "Received" headers when sending good email downstream to your servers, use this field to specify another value.

4. **LDAP Page Size:** use this setting to change the LDAP size. Many LDAP servers, such as Active Directory, specify the maximum page size to query. If SonicWALL Email Security Gateway exceeds this page size, it can cause performance problems both on the LDAP server and on SonicWALL Email Security Gateway. In the rare circumstances that this needs to be adjusted, please consult with SonicWALL Email Security Technical Support.

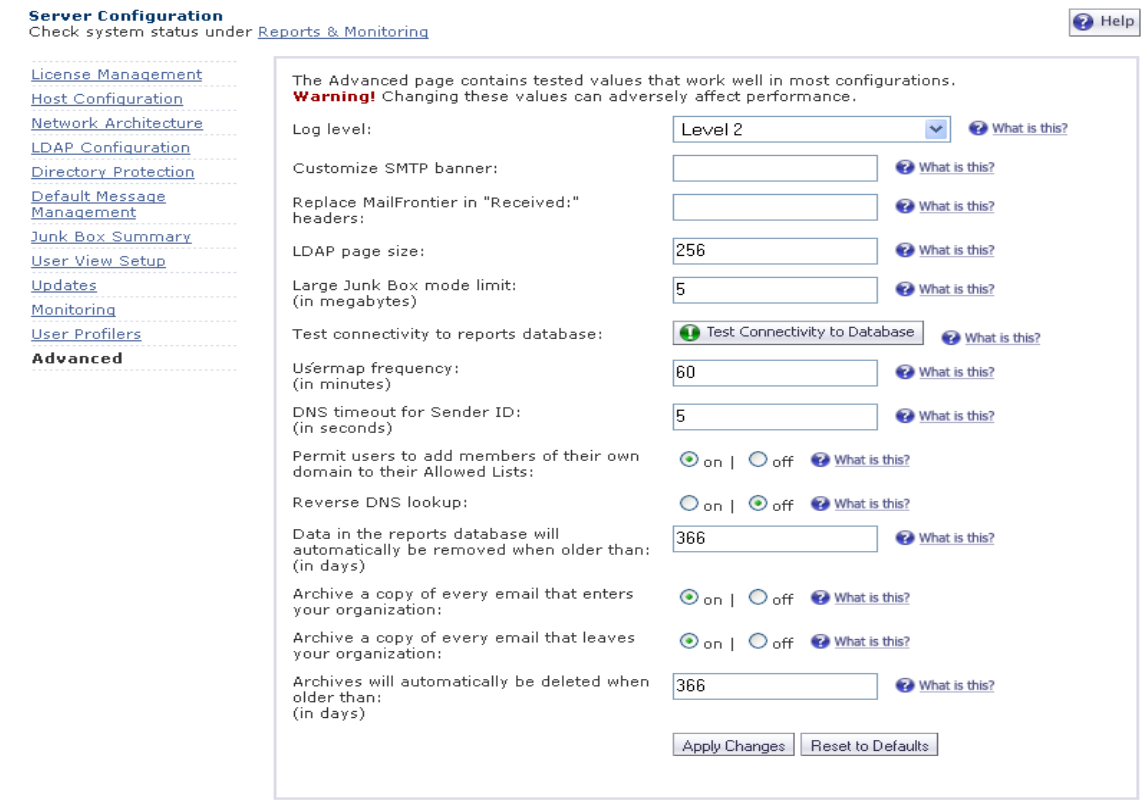


Figure 6.19 Advanced Settings

5. **Large Junk Box mode limit: (in megabytes):** Use this setting to determine how to view the Junk Box. This setting does not affect the per-user Junk Box view. In the Admin Junk Box Web interface, if the Junk Box reaches a large size, SonicWALL Email Security Gateway presents a different view that makes more sense for large volumes of information. For example, it does not load the entire quarantine into RAM so that you can sort by column, but it does allow a more powerful search mechanism inside any one day of the quarantine. Depending on your preferences, you may want this cutoff to be lower so your Junk Box has much higher performance, or you might like the cutoff higher so you get the other small Junk Box view all the time. The default value is 5MB.

6. Click the Test Connectivity to reports database button to verify that you can access the Reports database. See the Reports and Monitoring chapter in this guide for more information on accessing and customizing reports.

7. **Usermap frequency (in minutes):** Use this setting to change the usermap frequency.
A *Usermap* is a local cache of the LDAP server containing the list of email aliases per user. Usermap frequency is the interval between refreshes of the list of users on SonicWALL Email Security Gateway. This does not affect user's ability to log on, because that is always a real-time reflection of the LDAP directory. This setting applies to the list of aliases and lists of members of groups. In most cases, this setting is only increased to lower the load on your LDAP server. Depending on your other SonicWALL Email Security Gateway settings, accessing the user list once every 24 hours is acceptable and results in less load on the LDAP server.

8. **DNS timeout for Sender ID:** Enter the number of seconds to search for the DNS record of the sender. If SonicWALL Email Security Gateway cannot find the DNS record in the number of seconds you specify, it times out and does not return the DNS record of the sender. The default value is two seconds. You can set this value from 1 to 30 seconds. For more information about SPF, see "Authenticating the Sender's Domain via Sender ID" in the SonicWALL Email Security *Administrator's Guide*.

9. **Permit users to add members of their own domain to their Allowed Lists:** Use this check box to enables users to add people within your domain to their Allowed List. For example, if you work at *example.com* and check this check box, all users at *example.com* can be added to your Allowed list. As a result, their email messages to internal users are not filtered by SonicWALL Email Security. You can either add people manually or SonicWALL Email Security automatically adds each person to whom users send email.
   The default setting is **On**.
10. **Reverse DNS lookup:** This service converts an Internet IP address of the form `xxx.xxx.xxx.xxx` to the host name by searching Domain Name Service (DNS) tables and by querying the Pointer (PTR) record. The default setting is **Off.** Changing this check box can impact gateway performance.
11. **Data in the reports database will be removed when older than:** Enter the number of days of data that you want to preserve for reporting information. Lowering this number means less disk space will be used, but you will not have report data older than the number of days specified. The default value is 366 days. If your organization's email volume is very high, you may want to consider reducing this number.
12. **Archive a copy of every email that enters your organization:** When email archiving is enabled, folders containing the entire contents of every email are created in the logs directory of each SonicWALL Email Security Gateway server that analyzes email traffic.
13. **Archive a copy of every email that leaves your organization:** When email archiving is enabled, folders containing the entire contents of every email are created in the logs directory of each SonicWALL Email Security Gateway server that analyzes email traffic.
14. **Archives will automatically be deleted when older than:** Enter the number of days of data that you want to preserve for archiving purposes. Lowering this number means less disk space will be used, but email archives older than the number of days specified will not be available. The default value is 10 days. If your organization's email volume is very high, you may want to consider reducing this number.

CHAPTER 7

Reports and Monitoring

Monitoring SonicWALL Email Security Gateway

SonicWALL Email Security Gateway allows you to view system status and data through the Reports and Monitoring module. You can view statistics for different time periods and some reports allow you optionally download the data in CSV format.

You can also create custom reports by specifying a time period for the data, and download the report for analysis or email the report.

Note SonicWALL Email Security Gateway uses the Firebird Database Engine to generate reports. Make sure that there is no other installation of the Firebird Database Engine on the same server as SonicWALL Email Security Gateway.

By default, SonicWALL Email Security Gateway retains 366 days of reporting information in the database. You can change this setting in **Server Configuration > Advanced > Data in reports database will be removed after** field. Lowering this number means less disk space will be used, but you will not have report data older than the number of days specified. If your organization's email volume is very high, you may want to consider lowering this number.

Reports Dashboard

SonicWALL Email Security Gateway displays the **Dashboard** window, as shown in <Xref_Color>Figure 7.1 , on administrator login. The **Dashboard** provides a lot of information about SonicWALL Email Security Gateway at a glance. These charts are updated hourly and display the statistics for the last 24 hours.

Figure 7.1 Reports Dashboard

Good Email vs Junk Email

Displays the number of good messages versus junk messages. Junk message count includes spam, likely spam, phishing, likely phishing, viruses, likely viruses, Directory Harvest Attacks (DHA), and messages that trigger policy events.

Spam vs Likely Spam

Displays the number of email messages that are definitely spam and the number of messages that are likely spam. You can also find this information in the “Spam vs Likely Spam Reports” on page 92.

Junk Email Breakdown

Displays the number of junk messages broken down into the following categories:

- Spam
- Virus
- Phishing
- Policy
- Directory Harvest Attack (DHA)

You can also find this information in “Junk Email Breakdown” on page 92.

Top Spam Recipients

Displays the total number of spam received by the top 12 recipients in your organization in the last 24 hours. You can also find this information in “Top Spam Recipients” on page 92.

Inbound vs Outbound Email

Displays the number of inbound email messages compared to the number of outbound email messages. This chart is displayed only if the Outbound Module is licensed. You can also find this information in “Inbound vs Outbound Email” on page 87.

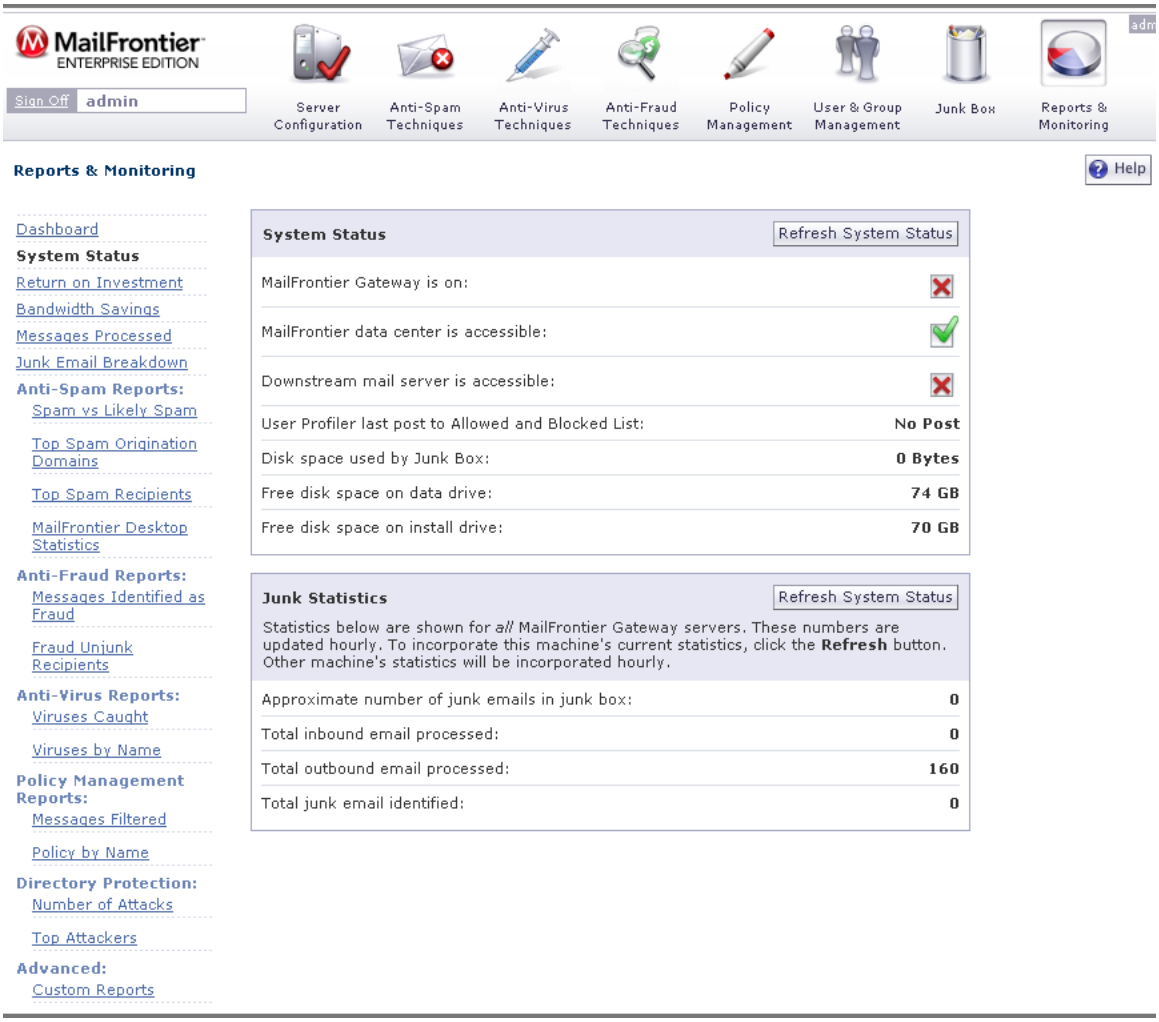
Top Outbound Email Senders

Displays the number of outbound email messages sent by the top 12 senders in your organization in the last 24 hours. This chart is displayed only if the Outbound Module is licensed. You can also find this information in “Top Outbound Email Senders” on page 87.

System Status

The System Status window shows the status of SonicWALL Email Security Gateway and the status of connections with other systems that it needs to communicate with, as shown in <Xref_Color>Figure 7.2 on page 88. A green check indicates the system is functioning as expected and a red **X** indicates it is not.

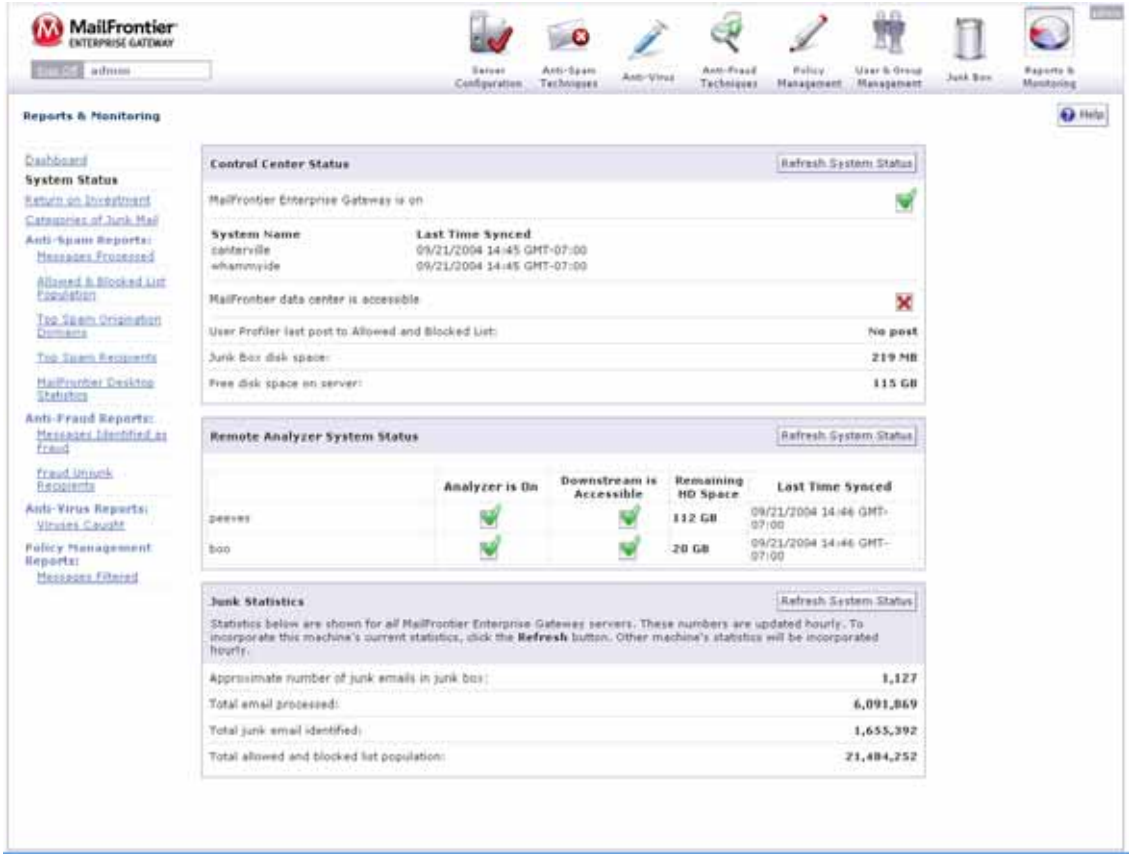
Figure 7.2 System Status for All in One Configuration



The lower half of the System Status window shows junk statistics, including the approximate number of junk messages stored, the number of inbound and outbound messages processed, and total number of junk messages identified.

Depending on how the system is configured, the system status page will show different information. If the system is configured to be an **All in One configuration**, the window displays the status of the setup, as shown in <Xref_Color>Figure 7.2 . If the system is configured to be a **Split Architecture**, the window displays the status of both the Control Centers and the Remote Analyzers, as shown in <Xref_Color>Figure 7.3 .

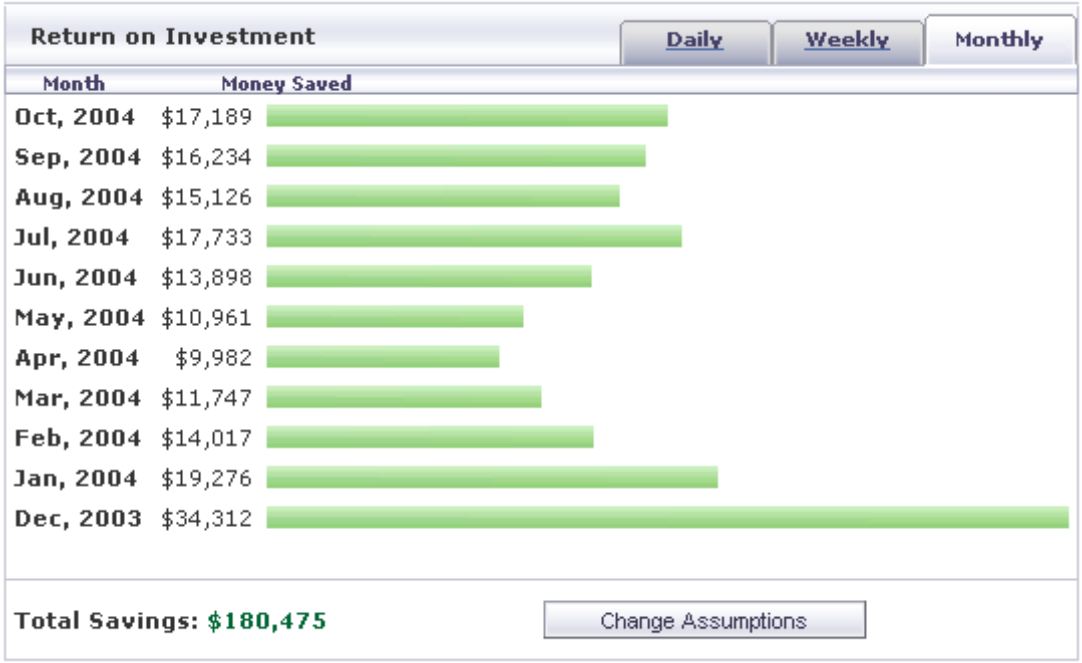
Figure 7.3 System Status for Split Configuration



Return on Investment

SonicWALL Email Security provides a tool to help determine the Return on Investment (ROI) for your organization's investment in SonicWALL Email Security Gateway. You can customize this tool to reflect your organization's costs of doing business.

Figure 7.4 Return on Investment



You can determine your organization's return on investment on a daily, weekly, or monthly basis from using the SonicWALL Email Security Gateway product. ROI numbers are computed from a formula and data accumulated by SonicWALL Email Security Gateway's `mlfUpdater` and the `usermap.xml` file is input into the formula.

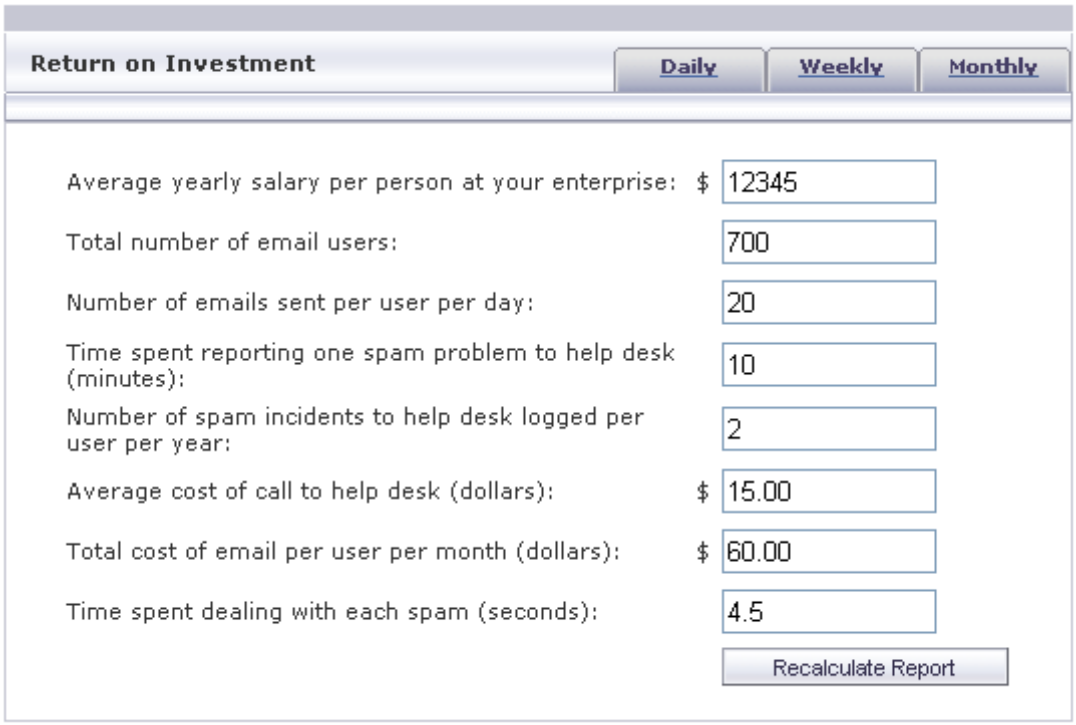
Determining the ROI for your Organization

To determine the savings from preventing unwanted email, click the **Change Assumptions** button to enter figures that reflect your organization.An input window appears with default values, as shown in <Xref_Color>Figure 7.5 .

To change the values so that they match your organization's experience:

1. Enter the appropriate values for your organization for salary, number of users, and other factors that contribute to the cost of dealing with unwanted email.

Figure 7.5 Enter Your Own ROI Values



2. Click the **Recalculate Report** button after you enter your values; a revised ROI report appears.

Bandwidth Savings

The Bandwidth Savings report displays the number of megabytes of bandwidth that SonicWALL Email Security Gateway saves your organization. SonicWALL Email Security Gateway lowers your organization's network costs through the following actions:

- Removing the high volume of junk messages that go through your network.
- Quarantining junk messages in the Junk Box.
- Deleting junk messages before they enter your network.

Inbound Messages Processed

This report displays the total number of inbound messages processed by SonicWALL Email Security Gateway along with the total number of junk messages and good messages.

Outbound Messages Processed

This report displays the total number of outbound messages processed by SonicWALL Email Security Gateway along with the total number of junk messages and good messages.

Inbound vs Outbound Email

This report displays the number of inbound and outbound messages processes by SonicWALL Email Security Gateway. This report is available only if outbound module is licensed.

Top Outbound Email Senders

This report displays the number of outbound email messages sent by the top 12 senders in your organization. This report is available only if outbound module is licensed.

Junk Email Breakdown

This report gives a percentage and numeric breakdown of the various categories of junk received, including Spam, Likely Spam, Viruses, Likely Viruses, Phishing, Likely Phishing, Policy events, and Directory Harvest Attacks (DHA).

Anti-Spam Reports

SonicWALL Email Security provides the following anti-spam reports:

- Spam vs Likely Spam
- Top Spam Origination Domains
- Top Spam Recipients
- SonicWALL Email Security Desktop Statistics

Spam vs Likely Spam Reports

This report displays the total number and percentage breakdown of spam and likely spam messages.

Top Spam Origination Domains

This report displays the alleged domains that sent your organization the most spam emails during the time period you select.

NOTE: Most spam messages use spoofed addresses, hence the domains listed in this report may not be the actual originators of the spam.

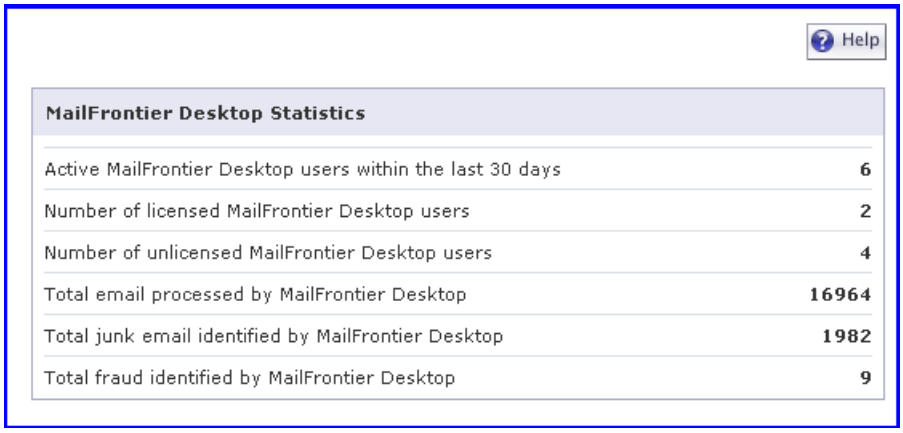
Top Spam Recipients

This report displays the users in your organization who receive the most spam.

SonicWALL Email Security Desktop Statistics

You can monitor statistics for SonicWALL Email Security's Desktop product if they are deployed in your organization. This window tracks the use of SonicWALL Email Security Desktop product inside your corporation. SonicWALL Email Security Desktop and SonicWALL Email Security Gateway are integrated with one another. When you junk a message while using SonicWALL Email Security Desktop, a thumbprint of that message is sent to SonicWALL Email Security Gateway. The junked email messages are added to the collaborative database, which tracks new trends in spam and other junk email, and helps prevent unwanted email.

Figure 7.6 SonicWALL Email Security Desktop Product Statistics



Note Statistics are displayed in this window only if SonicWALL Email Security Desktop product is installed on desktops in your organization.

Anti-Phishing Reports

SonicWALL Email Security Gateway provides the following Anti-Phishing reports:

- Messages Identified as Phishing
- Phishing Unjunk Recipients.

Messages Identified as Phishing

This report lists the total number messages identified as phishing.

Phishing Unjunk Recipients

This report displays a list of each phishing email that has been unjunked by the recipient. The report contains the name of the recipient, the message they unjunked, and the time the message was received.

Anti-Virus Reports

If you have licensed the Anti-Virus module, you can view the number of viruses detected by the SonicWALL Email Security Gateway and the names of the most prevalent viruses detected.

Inbound Viruses Caught

This report lists the number of viruses detected by SonicWALL Email Security Gateway in the inbound email traffiic.

Inbound Viruses by Name

This report lists the names of viruses detected by SonicWALL Email Security Gateway in the inbound email traffic.

Outbound Viruses Caught

This report lists the number of viruses detected by SonicWALL Email Security Gateway in the outbound email traffiic.

Outbound Viruses by Name

This report lists the names of viruses detected by SonicWALL Email Security Gateway in the outbound email traffic.

Policy Reports

If you have created policy filters in SonicWALL Email Security Gateway to manage email traffic, the following policy reports provides statistics on messages that triggered the policy filters

Inbound Policy Messages Filtered

This report lists the total number of inbound email messages that SonicWALL Email Security Gateway has filtered based on policies that you have configured.

Inbound Policy by Name

This report lists the inbound policies by name that were triggered by inbound email traffic.

Outbound Policy Messages Filtered

This report lists the total number of outbound email messages that SonicWALL Email Security Gateway has filtered based on policies that you have configured.

Outbound Policy by Name

This report lists the outbound policies by name that were triggered by inbound email traffic.

Directory Protection Reports

SonicWALL Email Security Gateway provides protection against directory attacks. Following directory protection reports are available to give more information on the directory attacks your organization is subjected to:

- Number of Attacks
- Top Attackers

Number of Attacks

This report lists the total number of incoming email messages that had incorrect email addresses.

Top Attackers

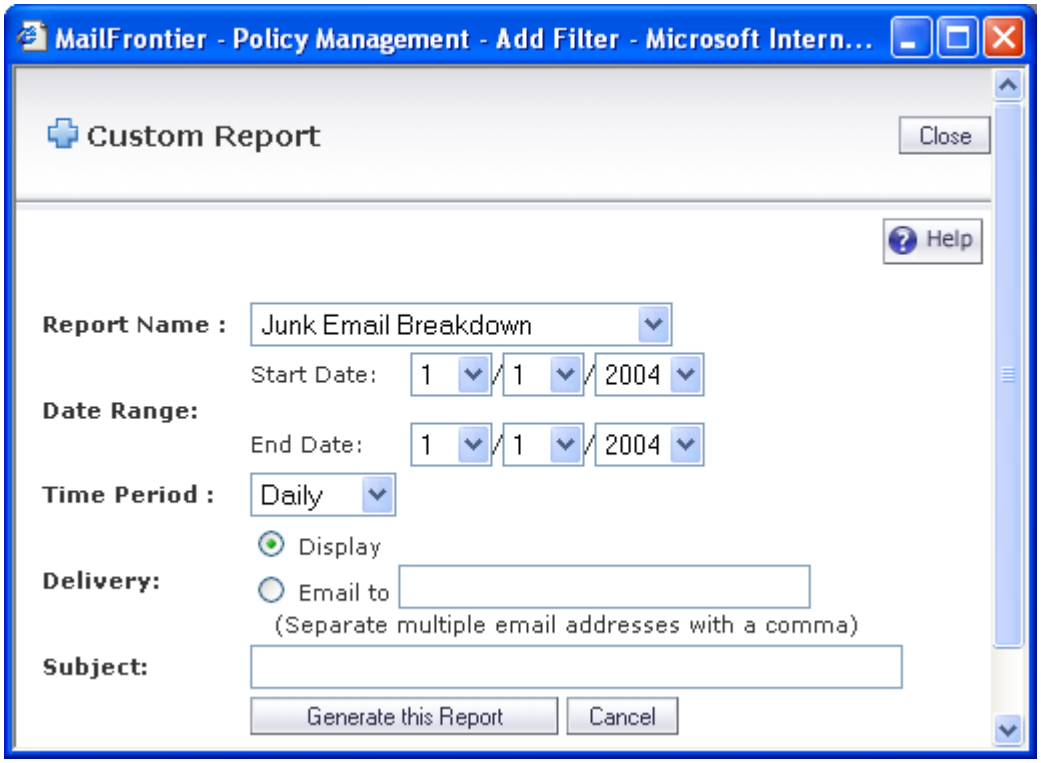
This report lists the alleged domains from which the most frequent Directory Harvest Attacks (DHA) originate.

Note Most junk messages use spoofed addresses, hence the domains listed in this report may not be the actual originators of the message.

Custom Reports

SonicWALL Email Security allows you to customize reports. You can choose the type of report, a range of dates for the data, or a number of hours for the data. You can also email the reports to another user.

Figure 7.7 Custom Report Window



To customize reports:

1. Select the type of report from the **Report Name** drop-down list.
2. Select the **Start** and **End Dates** from the **Date Range**.
3. Select **Hourly**, **Daily**, or **Monthly** from the **Breakdown** drop-down list.

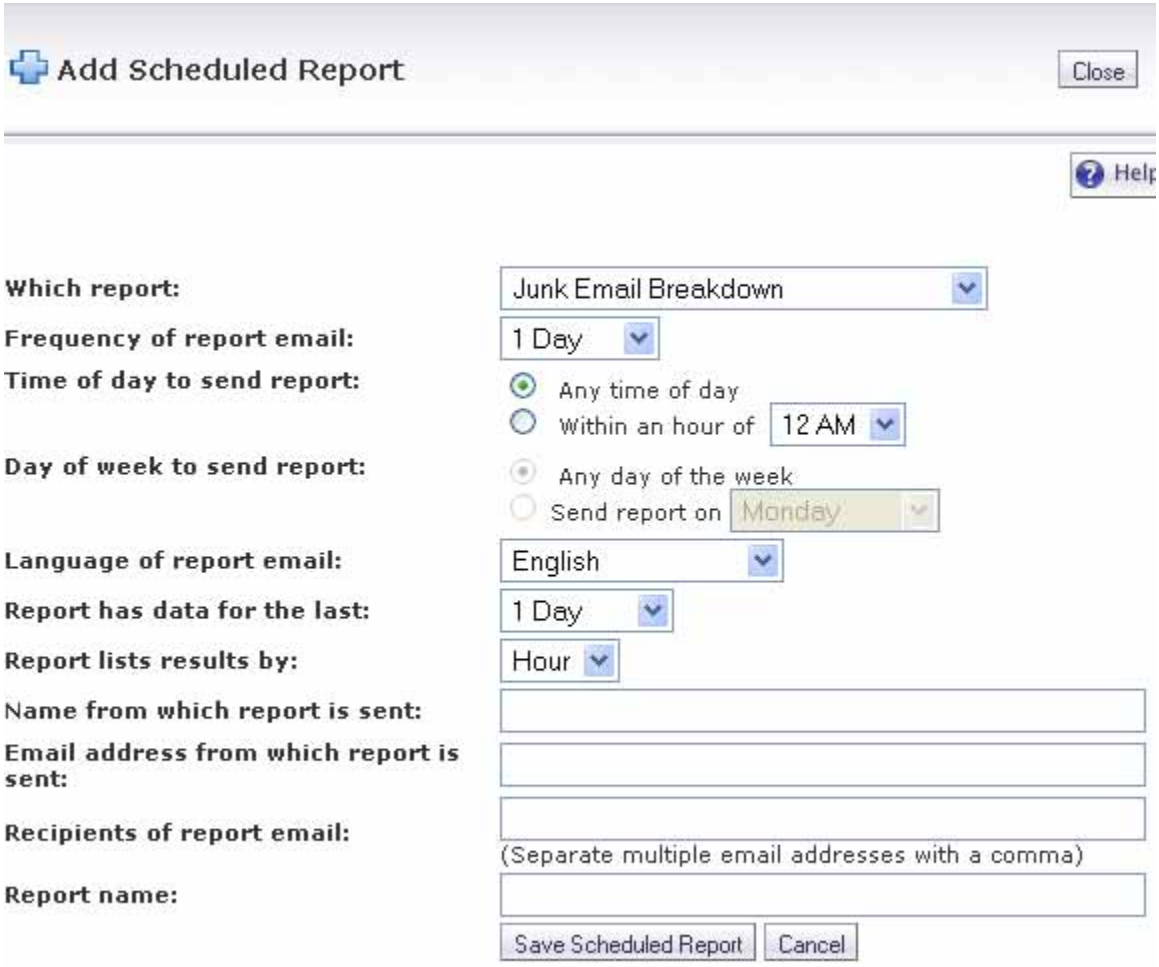
   You can select a period of up to 48 hours for hourly reports.
4. Select either the **Display** or the **Email to** radio button.
   - To run a report now, select **Display** and click the **Run This Report** link.
   - To email a report, select **Email to** and enter the recipients' email addresses in the text box. Separate each address with a comma. You can optionally enter a subject.

Scheduled Reports

SonicWALL Email Security allows you to schedule email delivery of reports. You can choose the type of report, a time span the data covers, the list of recipients, etc.

Data in scheduled reports is displayed in the time zone of the server on which SonicWALL Email Security Gateway stores email data (either an All in One or a Control Center), just like the reports in the Reports & Monitoring section of the UI. Scheduled report emails are sent according to the time zone on that computer as well.

Figure 7.8 Add Scheduled Report Dialog



To schedule delivery of a report:

1. Select the type of report from the **Which Report** drop-down list.
2. Select the **frequency** of the report email from the drop-down list.
3. Select the **time of day** at which you would like to receive the report email. This will be in the time zone of the server on which SonicWALL Email Security Gateway stores email data (either an All in One or a Control Center), just like the reports in the Reports & Monitoring section of the user interface.
4. Select the **day of the week** on which you would like to receive the report email.
5. Select the **language** in which you would like to receive the report email.

6. Select the time span the report will cover. For example, suppose the report email frequency is 3 Days, the time span selected is 7 Days, and the report is sent at 10 AM every day. A report sent on April 24th at 10 AM will cover roughly the time period starting April 21 at 10 AM and ending April 24 at 10 AM.
7. Select the time period by which you want to see results listed. This is the unit of time to use in the bar graph. For example, if *Hour* is chosen, a bar line will be shown for each hour in the specified timespan.
8. Specify the name of the sender of report emails. This is a human-readable name that will appear in your mail client as the sender of the report email. This does not need to be a real name.

   Examples: *Charles Nelson Really, My Daily Scheduled Report*, SonicWALL Email Security *Gateway Administrator, Joe Bloggs*

   Please use only 7-bit ASCII text.
9. Specify the email address from which this report is sent.
10. Enter a list of **email recipients** in the text box. Separate multiple email addresses with a comma.
11. Enter a name for this scheduled report. This name will appear in the page that shows the list of scheduled reports. It will also be the subject line for the email message when the scheduled report is sent.

CHAPTER 8
Anti-Spam Techniques

Managing Spam

SonicWALL Email Security Gateway uses multiple methods of detecting spam and other unwanted email. These include using specific Allowed and Blocked lists of people, domains, and mailing lists; patterns created by studying what other users mark as junk mail, and the ability to enable third-party blocked lists.

You can define multiple methods of identifying spam for your organization; users can specify their individual preferences to a lesser extent. In addition, SonicWALL Email Security provides updated lists and collaborative thumbprints to aid in identifying spam and junk messages.

Spam Identification

SonicWALL Email Security Gateway uses a multi-prong approach to identifying spam and other unwanted email. It is useful to understand the general operation so you can build your lists appropriately.

When an email comes in, the sender of the email is checked against the various allowed and blocked lists first, starting with the corporate list, then the recipient's list, and finally the SonicWALL Email Security-provided lists. If a specific sender is on the corporate blocked list but that same sender is on a user's allowed list, the message is blocked, as the corporate settings are a higher priority than a user's.

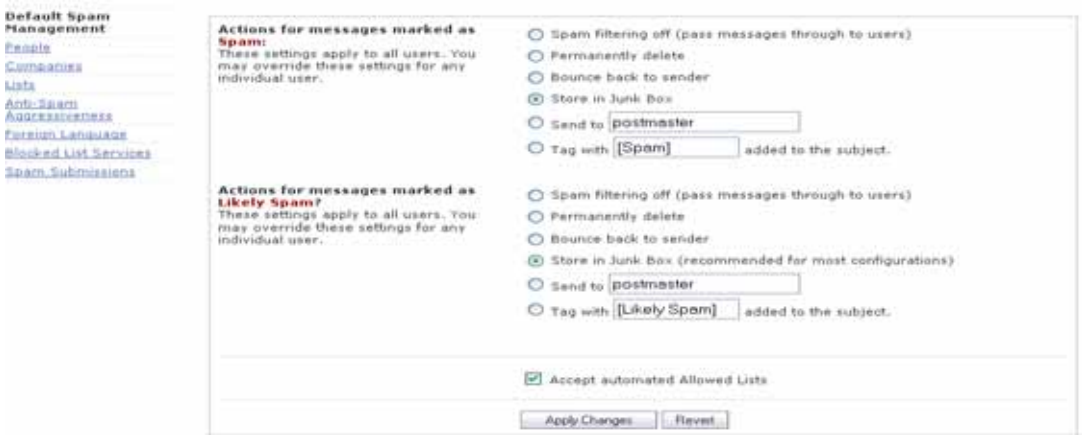
Note that the more detailed lists take precedence over the more general lists. For example, if a message is received from `aname@domain.com` and your organization's Blocked list includes domain.com but a user's Allowed list contains the specific email address `aname@domain.com`, the message is not blocked because the sender's full address is in an Allowed list.

After all the lists are checked, if the message has not been identified as junk based on the Allowed and Blocked lists, SonicWALL Email Security analyzes messages' headers and contents, and use collaborative thumbprinting to block email that contains junk.

Managing Spam through Default Settings

Use the Default Spam Management window shown in <Xref_Color>Figure 8.1 to select options for dealing with spam and likely spam.

Figure 8.1 Default Spam Management Window



To manage messages marked as spam or likely spam:

1. Choose one of the following responses shown in Table 1 on page 100.

Table 1 Spam Management Response

Response	Effect
Spam filtering off	**SonicWALL Email Security Gateway does not filter messages for spam. All messages are passed through to the recipient.**
Permanently Delete	**The email message is permanently deleted.** **CAUTION: If you select this option, your organization risks losing wanted email.**
Bounce Back to Sender	**The message is returned to sender with a message indicating that it was not deliverable.**
Store in Junk Box	**The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions.** **This option is the recommended setting.**
Send to	**Enter the email address of the person to receive this email.**
Tag With	**The email is tagged with a term in the subject line, for example, [JUNK] or [Possible Junk?]. Selecting this option allows the user to have control of the email and can junk it if it is unwanted.**

2. Check the **Accept Automated Allowed List** check box to accept automated lists that are created by User Profilers. User Profilers analyze your outbound traffic and automatically populate per user white lists. This helps reduce the false positives.

Note If this check box is unchecked in the Corporate, Group, or User windows, User Profilers have no effect.

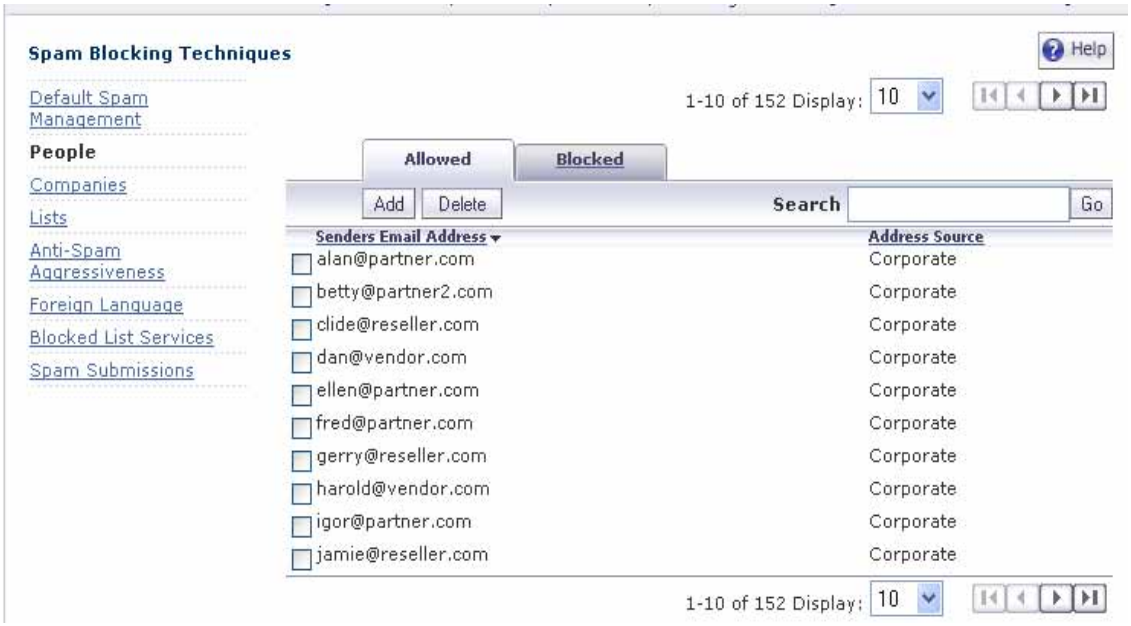
Caution When you go on vacation, deselect this box so that your vacation-response reply does not automatically place all recipients on your Allowed list.

3. Click **Apply Changes**.

Adding People to Add and Blocked Lists for the Organization

You can add specific people's email addresses to organization-wide Allowed or Blocked lists. Use the window displayed in <Xref_Color>Figure 8.2 on page 101.

Figure 8.2 Adding People to Allowed or Blocked Lists



This window displays the email address of senders on the organization's Allowed or Blocked lists. The source of the address is shown in the right-hand column.

Note These settings apply to the entire organization. Individual users can add or block people for their personal lists by clicking **Anti-Spam Techniques>People** in their SonicWALL Email Security user accounts. To see an individual user's lists, you must log in as that user. For more information, see "Signing In as a User" on page 144.

Search

To search for an address, enter all or part of the email address. For example, entering sale displays `sales@domain.com` as well as `forsale@domain.com`.

Add

To add people to the Allowed or Blocked lists:

1. Choose the **Allowed** or Blocked tab.

2. Click the **Add** button
3. Enter one or more email addresses, separated by carriage returns, to add to the chosen list.

Email addresses are case-insensitive; SonicWALL Email Security converts the address to lowercase.

Note You cannot put an address in both the Allowed and Blocked list simultaneously. If you add an address in one list that already exists on the other, it is removed from the first one.

Companies or Domains

You can allow and block email messages from entire domains. If you do business with certain domains regularly, you can add the domain to the Allowed list; SonicWALL Email Security allows all users from that domain to send email. Similarly, if you have a domain you want to block, enter it here and all users from that domain are blocked.

Note SonicWALL Email Security does not support adding top-level domain names such as `.gov` or `.abc` to the Allowed and Blocked lists.

Add

To add domains to the Allowed or Blocked lists:

1. Choose the **Allowed** or **Blocked** tab.
2. Click the **Add** button.
3. Enter one or more domains, separated by carriage returns.

Domain names are case-insensitive and are converted to lowercase.

NOTE: A domain cannot be on both the Allowed and Blocked list at the same time. If you add a domain to one list and it already exists on the other, it is removed from the first list.

Mailing Lists

SonicWALL Email Security Gateway enables you to add mailing lists, such as `listserv` lists, to your Allowed list, as shown in <Xref_Color>Figure 8.3 on page 103.

Figure 8.3 Mailing Lists

Mailing list email messages are handled differently than individuals and domains because SonicWALL Email Security Gateway looks at the recipient's address rather than the sender's. Because many mailing list messages appear spam-like, entering mailing list addresses prevents misclassified messages.

Add

To add mailing lists:

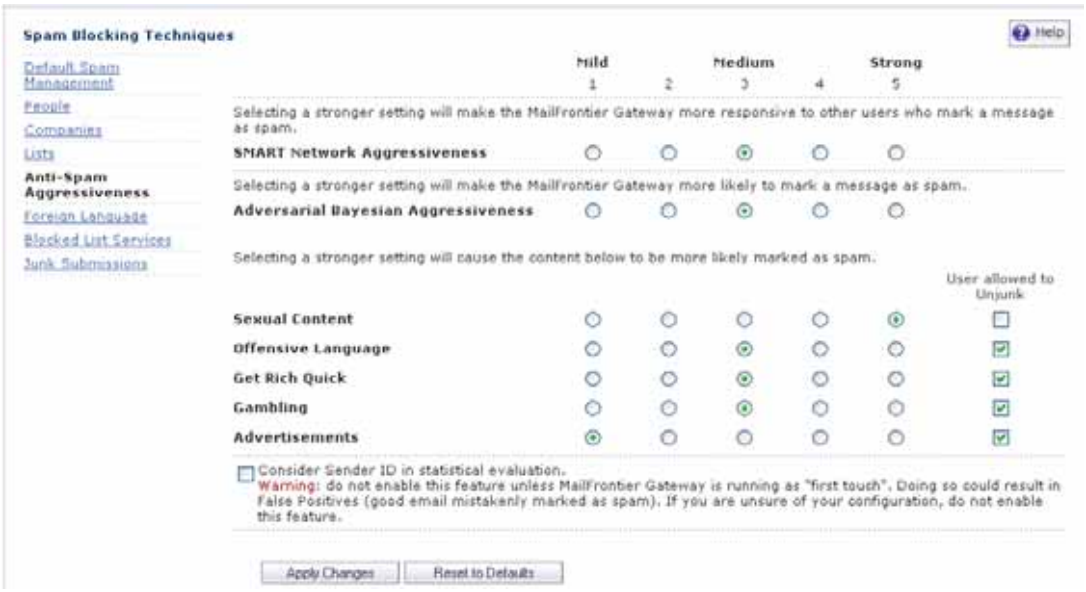
1. Click the **Add** button
2. Enter one or more email addresses, separated by carriage returns.

Email addresses are case-insensitive; the message is converted to lowercase.

Anti-Spam Aggressiveness

The Anti-Spam Aggressiveness window, as shown in <Xref_Color>Figure 8.4 on page 104, allows you to tailor SonicWALL Email Security to your organization's preferences. Configuring this window is optional. SonicWALL Email Security recommends using the default setting of Medium (or 3) unless you require different settings for specific types of spam blocking.

Figure 8.4 Rules and Collaborative Settings



Configuring SMART Network Aggressiveness Settings

SMART Network refers to SonicWALL Email Security user community. Every email that is junked by an user in SMART Network is summarized in the form of thumbprints. A *thumbprint* is an anonymous record of the junked email that contains no information about the user who received the mail or the contents of the mail.

You can adjust SMART Network settings to customize the level of influence community input has on spam blocking for your organization. Updates are provided to your gateway server at defined intervals.

To adjust your settings, click one of the radio buttons from Mild (1) to Strong (5). A setting of 5 indicates that you are comfortable with the collective experience of the SonicWALL Email Security user community, and do not want to see more email. A setting of 1 or 2 indicates that want to judge more email for yourself and rely less on the collective experience of SonicWALL Email Security's user community.

Configuring Adversarial Bayesian Aggressiveness Settings

The Adversarial Bayesian technique refers to SonicWALL Email Security's statistical engine that analyzes messages for many of the spam characteristics. This is the high-level setting for the Rules portion of spam blocking and lets you choose where you want to be in the continuum of choice and volume of email. This setting determines the threshold for how likely an email message is to be identified as junk email.

Use this settings to specify how stringently SonicWALL Email Security Gateway evaluates messages.

- If you choose **Mild** (check box 1 or 2), you are likely to receive more questionable email in your mailbox and receive less email in the Junk Box. This can cause you to spend more time weeding unwanted email from your personal mailbox.

- If you choose **Medium** (check box 3), you accept SonicWALL Email Security's spam-blocking evaluation.
- If you choose **Strong** (check box 4 or 5), SonicWALL Email Security rules out greater amounts of spam for you. This can create a slightly higher probability of good email messages in your Junk Box.

For example, in <Xref_Color>Figure 8.4 on page 104 the administrator has set aggressiveness to Strong (5), to rule out greater amounts of spam.

Determining Amounts and Flavors of Spam

You can determine how aggressively to block particular types of spam, including sexual content, offensive language, get rich quick, gambling, and advertisements.

For each of the spam flavors:

- Choose **Mild** (check box 1) to be able to view email that contains terms that relate to these topics.
- Choose **Medium** (check box 2 through 4) to cause SonicWALL Email Security to tag this email as likely junk.
- Choose **Strong** (check box 5) to make it more likely that email with this content is junked.

For example, in <Xref_Color>Figure 8.4 on page 104, the administrator has determined that they want to receive no email with sexual content by selecting Strong (5). They are less concerned about receiving advertisements, and selected Mild (1). You can also choose whether to allow users to unjunk specific flavors of spam.

Authenticating the Sender's Domain via Sender ID

Check the **Consider Sender ID in statistical evaluation** check box, as shown in Figure 8.4, "Rules and Collaborative Settings," on page 104.

About Sender ID

Many senders of junk email messages spoof addresses to make their email appear more legitimate and compelling. When you send an email message, the email contains information about the domain from which the message was sent. Sender ID, sometimes called Sender Policy Framework (SPF) is a system that checks the sender's DNS records. SonicWALL Email Security Gateway determines whether the IP address from which the message was sent matches the purported domain. Many organizations publish their list of IP addresses that are authorized to send email so that recipient's MTAs can authenticate the domain of messages that claim to be from that address.

SonicWALL Email Security Gateway uses the following system to determine if the sender is authorized to send email from the purported address:

1. Stores the IP address of the SMTP client that delivered the message, which is the Source IP address.
2. Finds the sender of the message, and stores the domain that the message claims to be from.
3. Using the Domain Name System (DNS), queries the domain for its Sender ID record, if it is published. Those records are published by many domain owners, and create a list of IP addresses that are authorized to send mail for that domain.
4. Validates that the domain authorizes the Source IP address in its SPF record.

Below is a simple example:

- SonicWALL Email Security Gateway receives a message from `192.0.2.128`
- In the message, SonicWALL Email Security Gateway finds `From: John.Smith@example.com` so it uses `example.com` as the domain.

- SonicWALL Email Security Gateway queries `example.com` for its SPF record
- The SPF record published at `example.com` lists `192.0.2.128` as a system that is authorized to send mail for `example.com`, so SonicWALL Email Security Gateway gives this message an `SPF = pass` result. This information is taken into account by SonicWALL Email Security Gateway in the determination of spam.

Sender ID or SPF Implementation Notes

To use Sender ID or SPF effectively, SonicWALL Email Security Gateway *must* be the first-touch server. SonicWALL Email Security Gateway factors each message's SPF score as a portion of information used by its spam- detection engine. SonicWALL Email Security Gateway needs the Source IP address of the SMTP client sending messages. Thus, if your SonicWALL Email Security Gateway is downstream from another MTA, for example, Postfix or SendMail, this check will not provide useful information, since all of the messages will come from the IP Address of your Postfix or SendMail server.

NOTE: SonicWALL Email Security Gateway performance might vary if you enable Sender ID.

Publishing Your SPF Record

SonicWALL Email Security strongly recommends that you publish your SPF records to prevent spammers from spoofing your domain. When spammers spoof your domain, your domain can receive a high volume of bounced messages due to fraudulent or junk email that appears to come from your domain. Implementing SPF prevents your company's branding from being diluted. For assistance in setting up your SPF records, go to http://spf.pobox.com/wizard.html.

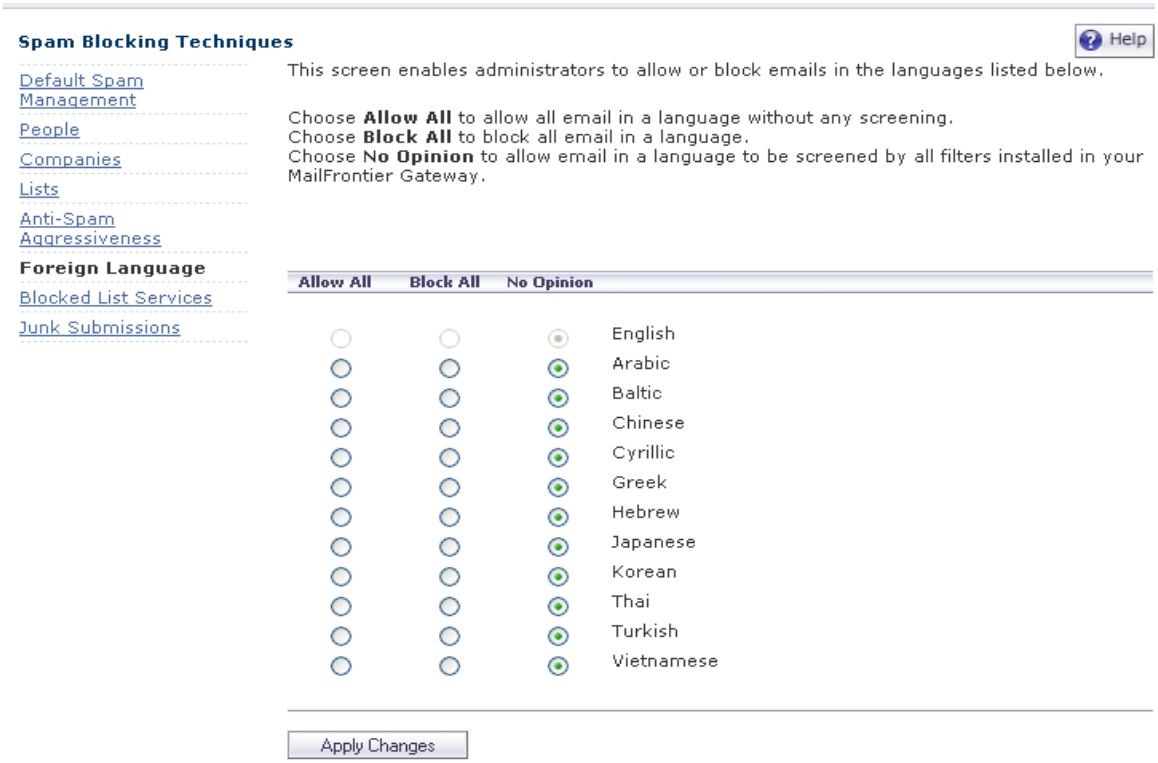
To see an example of an SPF record, you can use a tool such as `nslookup` from your favorite shell. As an example, to query SPF records for AOL, type:

```
nslookup -query=TXT aol.com
```

Foreign Languages

You can allow, block, or enter no opinion on email in foreign language character sets. If you enter **No opinion**, SonicWALL Email Security Gateway judges the content of the email message based on the SonicWALL Email Security modules that are installed.

Figure 8.5 Foreign Languages



Black List Services

Public and subscription-based black list services, such as the Mail Abuse Prevention System (MAPS), Real-time Blackhole List (RBL), Relay Spam Stopper (RSS), Open Relay Behavior-modification Systems (ORBS) and others, are regularly updated with domain names and IP addresses of known spammers. SonicWALL Email Security Gateway can be configured to query these lists and identify spam originating from any of their known spam addresses, as shown in “Black List Services” on page 108.

NOTE: RBL support in Solaris version of SonicWALL Email Security Gateway is limited. SonicWALL Email Security recommends against the use of RBL in Solaris version of the product.

Figure 8.6 Black List Services

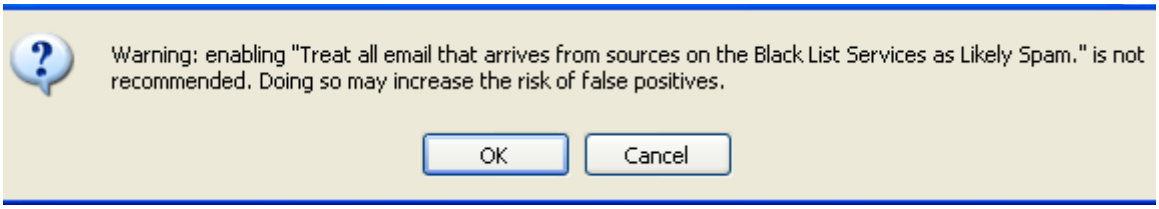
Add

Click **Add** and enter the server name of the black list service, for example `list.dsbl.org`. Each black list service is automatically enabled when you add it.

Email that Arrives from Sources on the Black Lists Services

Check the **Treat all email that arrives from sources on Black List Services as Likely Spam** check box to prevent users from receiving messages from known spammers. If you check this box, SonicWALL Email Security Gateway displays the following message, as shown in <Xref_Color>Figure 8.7 .

Figure 8.7 Warning about Real-time Black List Servers

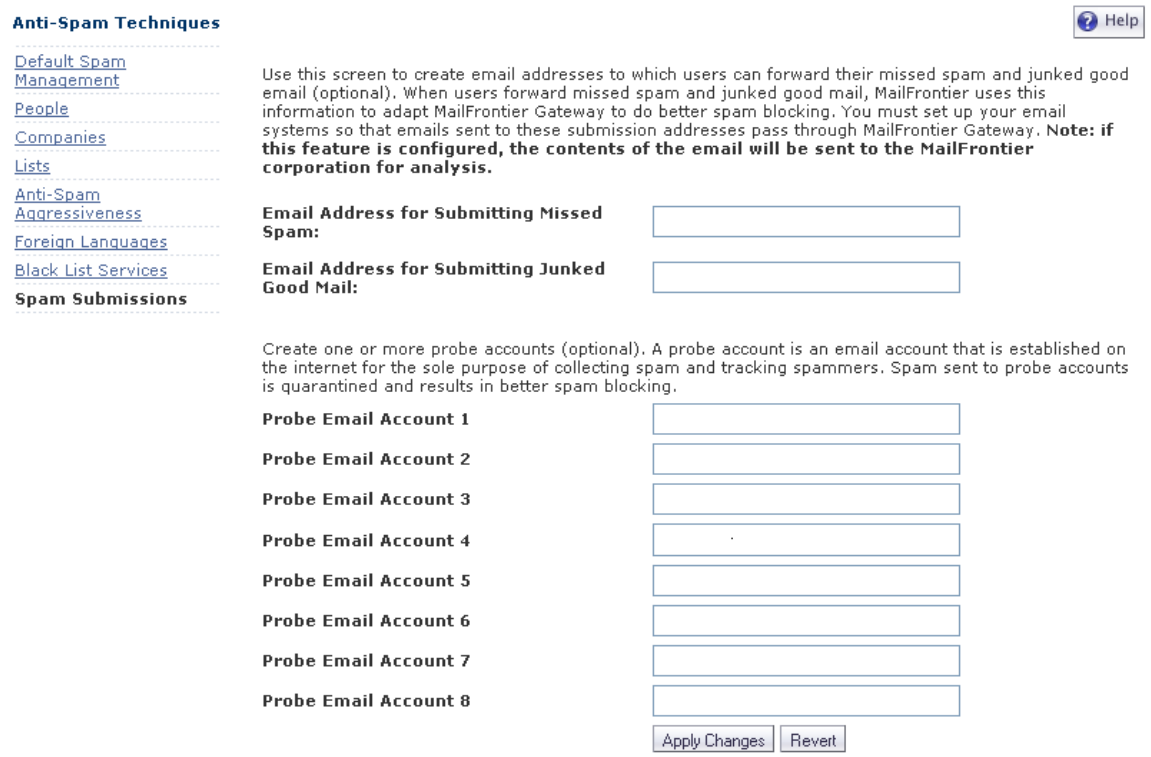


Managing Spam Submissions and Probe Accounts

Use the Spam Submissions page, shown in <Xref_Color>Figure 8.8 , to manage email that is miscategorized and to create probe accounts to collect spam and catch malicious hackers. Managing miscategorized email and creating probe accounts increases the efficiency of SonicWALL Email Security's

spam management. This page enables administrators and users to forward the following miscategorized email messages to their IT groups, create probe accounts, and accept automated allowed lists to prevent spam.

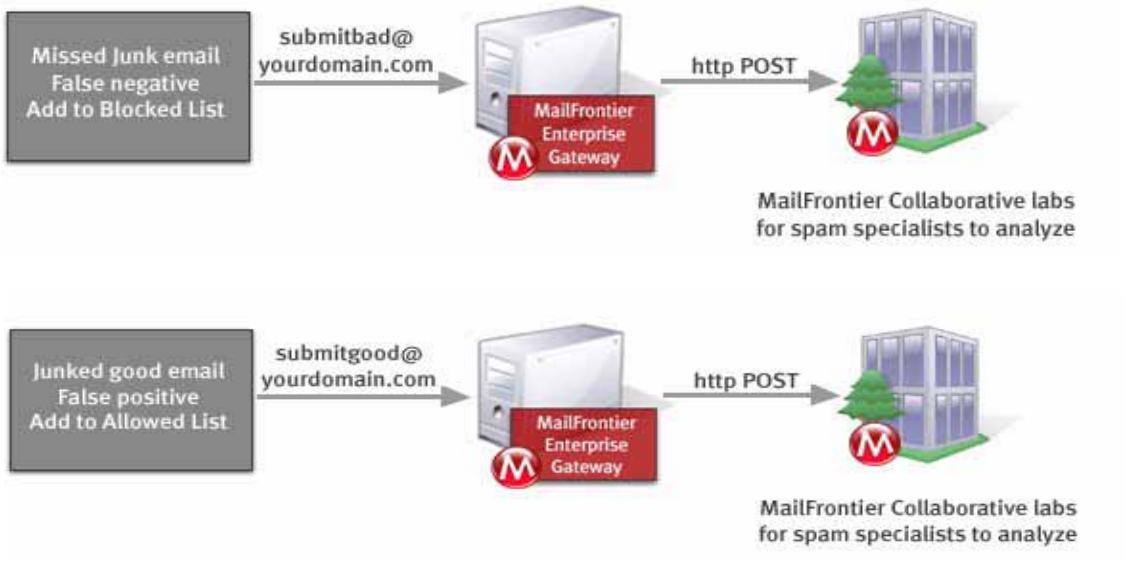
Figure 8.8 Spam Submission Window



Managing Miscategorized Messages

The following diagrams illustrate the process of junk submissions. They show how junk email that was missed by SonicWALL Email Security Gateway (also known as false negatives) is sent to SonicWALL Email Security's Collaborative laboratory for analysis. They also show how good email that was junked by the SonicWALL Email Security Gateway (also known as false positives) is sent to SonicWALL Email Security's Collaborative laboratory for analysis.

Figure 8.9 Submitting missed and miscategorized messages



What Happens to Miscategorized Email Messages

The following happens when an email message is miscategorized:

- For false negatives, SonicWALL Email Security Gateway adds the sender address of the junked email to the user's Blocked List so that future email messages from this sender are blocked. (The original sender is blacklisted for the original recipient.)
- For false positives, SonicWALL Email Security Gateway adds the addresses of good email senders that were unjunked to the user's Allowed List. (The original sender is whitelisted for the original recipient.)
- These messages are sent to the global collaborative database. Good mail that was unjunked is analyzed to determine why it was categorized as junk.

Forwarding Miscategorized Email to SonicWALL Email Security Gateway

You must set up your email system so that email sent to the `submitbad@your_domain.com` and `submitgood@your_domain.com` passes through SonicWALL Email Security Gateway.

NOTE: The email addressed to `submitbad@your_domain.com` and `submitbad@your_domain.com` must pass through the SonicWALL Email Security Gateway so that it can be operated on.

Configuring Submit-Junk and Submit-Good Email Accounts

Mail is considered miscategorized if SonicWALL Email Security Gateway puts wanted (good) email in the Junk Box or if SonicWALL Email Security Gateway delivers unwanted email in the user's inbox. If a user receives a miscategorized email, they can to update their personal Allowed list and Blocked list to customize their email filtering effectiveness. This system is similar to the benefits of running SonicWALL Email Security Desktop (formerly Matador) in conjunction with SonicWALL Email Security Gateway, and clicking Junk or Unjunk messages, but does not require SonicWALL Email Security Desktop to be installed.

The email administrator can define two email addresses within the appropriate configuration page in SonicWALL Email Security Gateway, such as `submitjunk@your_domain.com` and `submitgood@your_domain.com`. As SonicWALL Email Security Gateway receives email sent to these addresses, it finds the original email, and appropriately updates the user's personal Allowed and Blocked list.

NOTE: Users must forward their miscategorized email directly to these addresses after you define them so that SonicWALL Email Security can learn about miscategorized messages.

Problem with Forwarding Miscategorized Email to SonicWALL Email Security for Analysis

A problem can arise if the user sends an email to `submitjunk@your_domain.com`, and the local mail server (Exchange, Notes, or other mail server) is authoritative for this email domain, and does not forward it to SonicWALL Email Security Gateway. There are a few ways around this problem; the most common solution is included below as an example.
To forward the missed email to SonicWALL Email Security for analysis:

1. Add the `submitjunk` and `submitgood` email addresses as `submitjunk@eg-host.your_domain.com` and `submitgood@eg-host.your_domain.com` into the SonicWALL Email Security Gateway Junk Submission text boxes.

   NOTE: Create an A record in your internal DNS that resolves `eg-host.your_domain.com` to your SonicWALL Email Security Gateway server's IP address.

2. Tell users to forward mail to `submitjunk@EG-host.your_domain.com` or `submitgood@EG-host.your_domain.com.`

The mail goes directly to the SonicWALL Email Security Gateway servers.

Probe Accounts

Configure the **Probe Email Account** fields to cause any email sent to your organization to create fictitious email accounts from which mail is sent directly to SonicWALL Email Security, Inc. for analysis. Adding this junk email to the set of junk email messages that SonicWALL Email Security blocks enhances spam protection for your organization and other users.

Probe accounts are accounts that are established on the Internet for the sole purpose of collecting spam and tracking hackers. SonicWALL Email Security suggests that you use the name of a past employee as the name in a probe account, for example, `fredjones@example.com`.

NOTE: If you configure probe accounts, the contents of the email will be sent to SonicWALL Email Security, Inc. for analysis.

Managing Spam Submissions

To manage spam submissions:

1. Click **Anti-Spam Techniques>Spam Submissions.**
   The Spam Submission window appears, as shown in <Xref_Color>Figure 8.8 .
2. Enter an email address in **Submitting Missed Spam**.
   For example, you might address all missed spam email to `mailto:submitmissedspam@`*`your_domain.com`*.
3. Enter an email address in **Submitting Junked Good Mail**.
   For example, you might address all misplaced good email to `mailto:submitgood@`*`your_domain.com`*.
4. Establish one or more **Probe Email Accounts**.
   Enter the email address of an account you want to use to collect junk email. The email address does not have to be in LDAP, but it does have to be an email address that is routed to your organization and passes through SonicWALL Email Security Gateway. For example, you might create a probe email account with the address `mailto:probeaccount1@`*`your_domain.com`*.

   CAUTION: a probe account should NOT contain an email address that is used for any purpose other than collecting junk email. If you enter an email address that is in use, the owner of that email address will never receive another email - good or junk - again, because all email sent to that address will be redirected to the SonicWALL Email Security corporation's data center.
5. Click the **Apply Changes** button.

CHAPTER 9
Anti-Virus Techniques

SonicWALL Email Security's Anti-Virus modules enable you to protect your organization from inbound email-borne viruses and prevent your employees from sending viruses with outbound email. Once SonicWALL Email Security Gateway has identified the email message or attachment that contains a virus or likely contains a virus, you choose how to manage the virus-infected email. Virus-protection is available as optional modules and can be enabled by the SonicWALL Email Security Gateway administrator for the entire organization.

How Virus Checking Works

The Anti-Virus modules use virus-detection engines to scan email messages and attachments for viruses, Trojan horses, worms and other types of malicious content. The virus-detection engines receive periodic updates to keep them current with the latest definitions of viruses. SonicWALL Email Security Gateway supports McAfee ® and Kaspersky virus-detection engines. You can choose to buy and deploy one or both virus-detection engines supported by SonicWALL Email Security. Messages determined to be dangerous by McAfee or Kaspersky engine are categorized as *Viruses.*

NOTE: The Kaspersky Anti-Virus module is only available on the SonicWALL Email Security Gateway for Windows. McAfee Anti-Virus module is available on both Windows and Solaris.

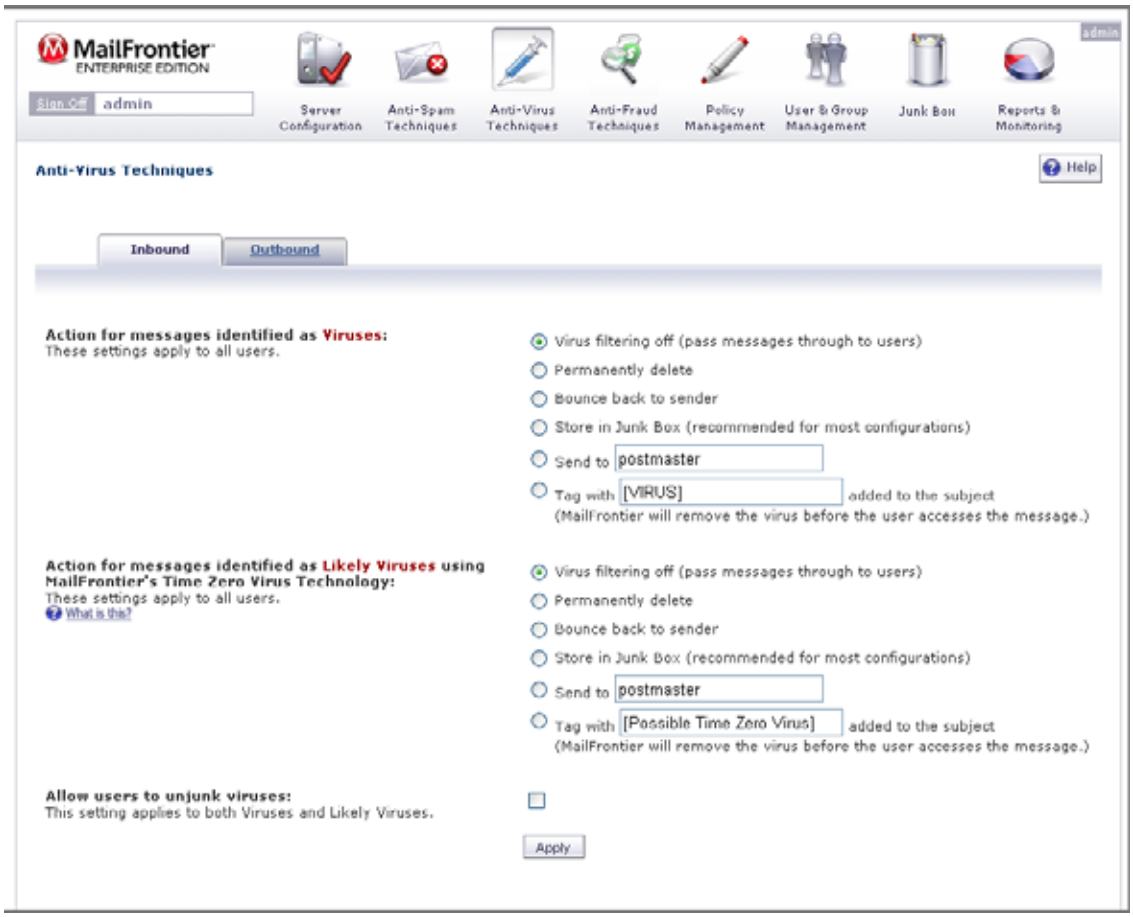
When any one of the virus-detection engines is activated, you also get the benefit of SonicWALL Email Security**'s Time Zero Virus Technology**. This technology uses heuristic statistical methodology and virus outbreak responsive techniques to determine the probability that a message contains a virus. If the probability meets certain levels, the message is categorized as *Likely Virus.* This technology complements virus-detection engines and enabling this technology provides the greatest protection for *time zero viruses*, the first hours that a virus is released, when major anti-virus companies have not yet modified their virus definitions to catch it.

Preventing Viruses and Likely Viruses in Email

To configure anti-virus protection:

1. Click the **Anti-Virus Techniques** icon. The Anti-Virus window appears, as shown in Figure 9.1.

Figure 9.1 Anti-Virus Techniques



If you have licensed more than one virus-detection engines, both will work in tandem. If you have licensed SonicWALL Email Security Outbound module, licensed virus-detection engines can be used on both inbound and outbound paths.

The following table explains the options for dealing with email-bourne *Viruses* or *Likely Viruses*, as shown in Figure 9.1, and the consequences of these actions

Table 1 Actions to take when a Virus or Likely Virus is Detected

Action	Consequence	Additional Information
Virus Filtering Off	**SonicWALL Email Security Gateway passes this email through to users without stripping the viruses or likely viruses.**	**This choice provides *no* screening for viruses or likely viruses.**
Permanently Delete	**SonicWALL Email Security Gateway permanently deletes this message.**	**This is a secure option for the enterprise because the virus or likely virus is permanently deleted. However, neither the receiver nor the sender knows that the email message contained a virus or likely virus, and once the message is deleted, you *cannot* retrieve it.**
Bounce Back to Sender	**SonicWALL Email Security Gateway bounces email back to the sender with the virus removed.**	**The sender is notified of the virus or likely virus in the email.**
Store in Junk Box	**SonicWALL Email Security Gateway stores email in the Junk Box. If you click the Allow Users to Unjunk button, users can unjunk the message.**	**Mail is stored in Junk Box. If you click the Allow Users To Unjunk button users can receive the message, with the virus or likely virus removed. NOTE: SonicWALL Email Security recommends this option because you can retrieve the message after SonicWALL Email Security strips the virus.**
Tag with [VIRUS] or [LIKELY VIRUS]	**SonicWALL Email Security Gateway delivers email to the addressee and strips the virus. The subject is tagged with [VIRUS], or [LIKELY VIRUS] or another administrator-specified term.**	**You can enter another tag in the text box or use the default [VIRUS] or [LIKELY VIRUS].**

2. Determine how to treat email messages that contain *Viruses* or *Likely Viruses* and select the action to take.
3. Click the **Allow Unjunk** checkbox to allow users to view messages with viruses from Junk Box.

Note SonicWALL Email Security removes the virus from the message before the user retrieves it.

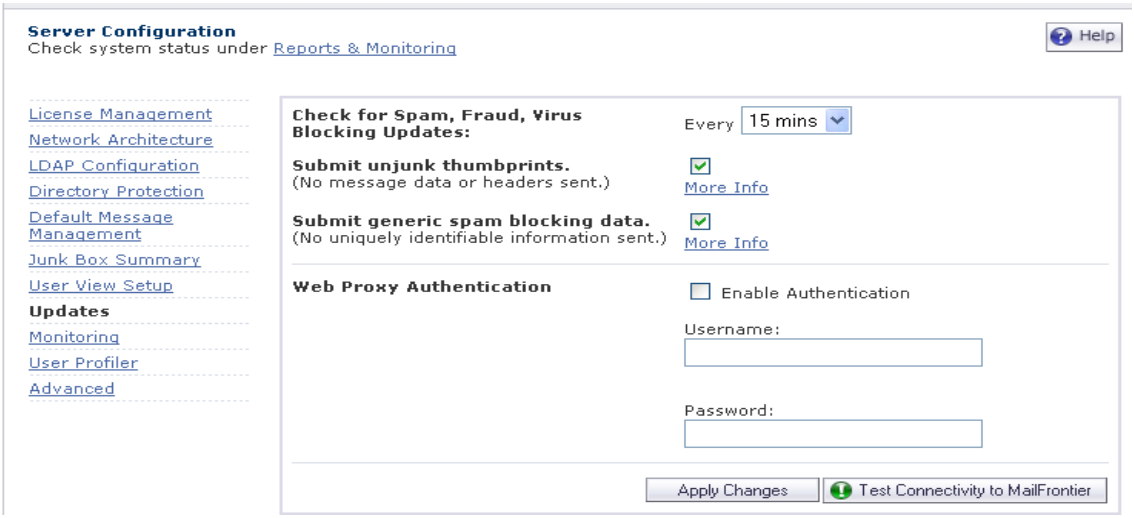
4. Click **Apply Changes**.

Checking for Updates

To determine how frequently you want to check for virus definition updates:

1. Click **Server Configuration > Updates**.
   The **Updates** window, shown in Figure 9.2, appears.

Figure 9.2 Checking for Virus Updates



2. Choose a time interval from the dropdown list adjacent to **Check for Spam, Phishing, and Virus Blocking Updates**.

   You can choose every 5 minutes to every 2 hours.

3. Click the **Apply Changes** button

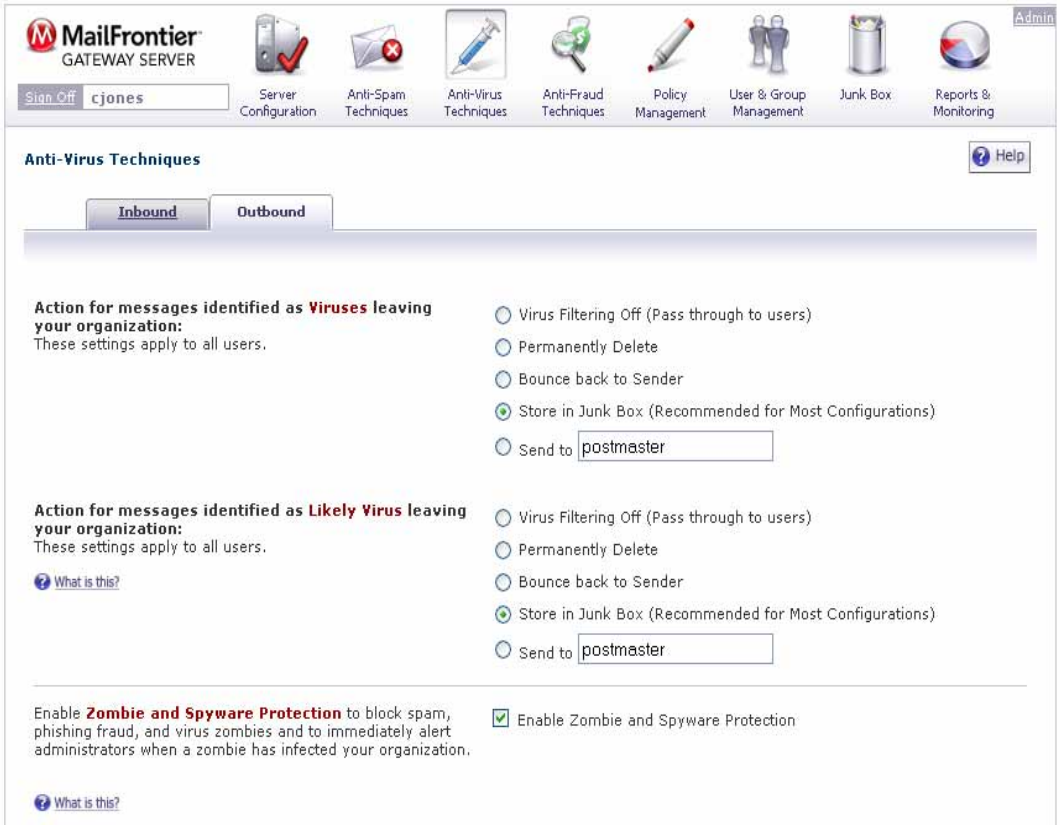
Zombie and Spyware Protection

It is possible that unauthorized software is running on a computer within your organization sending out junk email - spam, phishing, virus or other unauthorized content - messages. This scenario could happen happened if your organization was subjected to a virus attack called Trojans or an user downloaded some thing from the web and unauthorized software got installed without user's knowledge. These unauthorized software programs that send out malicious content are called **Zombies** or **Spyware**.

SonicWALL Email Security's **Zombie and Spyware Protection** technology brings the same high standard of threat protection available on the inbound email path to email messages leaving your organization through the outbound path.

To enabled **Zombie and Spyware Protection**, select **Anti-Virus Techniques** icon, click on the **Outbound** tab and check the box **Enable Zombie and Spyware Protection**.

Figure 9.3 Enable Zombie and Spyware Protection



CHAPTER 10
Anti-Phishing Techniques

Protecting Against Email Fraud

SonicWALL Email Security Gateway's Anti-Phishing module protects organizations against email containing fraudulent content. There are two audiences for fraud: the consumer and enterprise users. SonicWALL Email Security Gateway focuses on preventing fraud that enters the enterprise via email. Email is an entry point for malicious hackers.

What is Enterprise Phishing?

There are numerous types of enterprise phishing.

- *Consumer phishers* try to con users into revealing personal information such as social security numbers, bank account information, credit card numbers, and driver's license identification. This is known as *identity theft*. Recouping from having a phisher steal your identity can take many hours and can cost consumers many dollars. Being phished can bring your life to a virtual standstill as you contact credit card companies, banks, state agencies, and others to regain your identity.
- *Enterprise phishers* attempt to trick users into revealing the organization's confidential information. This can cost thousands of executive and legal team hours and dollars. An organization's electronic-information life can stop abruptly if hackers deny services, disrupt email, or infiltrate sensitive databases.

Phishing aimed at the IT group in the organization can take the following forms:

- Email that appears to be from an enterprise service provider, such as a DNS server, can cause your organization's network to virtually disappear from the Web.
- Hacking into your web site can cause it to be shut down, altered, or defaced.
- Email might request passwords to highly sensitive databases, such as Human Resources or strategic marketing information. The email might take the form of bogus preventive maintenance.
- Other information inside the organization's firewall, such as Directory Harvest Attacks (DHA) to monitor your users.

Phishing can also take the form of malicious hackers spoofing your organization. Email is sent that appears to come from your organization can damage your community image and hurt your customers in the following ways:

- Spoofed email can ask customers to confirm their personal information.

- Spoofed email can ask customers to download new software releases, which are bogus and infected with viruses.

Preventing Phishing

Phishing harms organizations and consumers by raising the price of doing business, which raises the cost of goods and services. SonicWALL Email Security prevents phishing through:

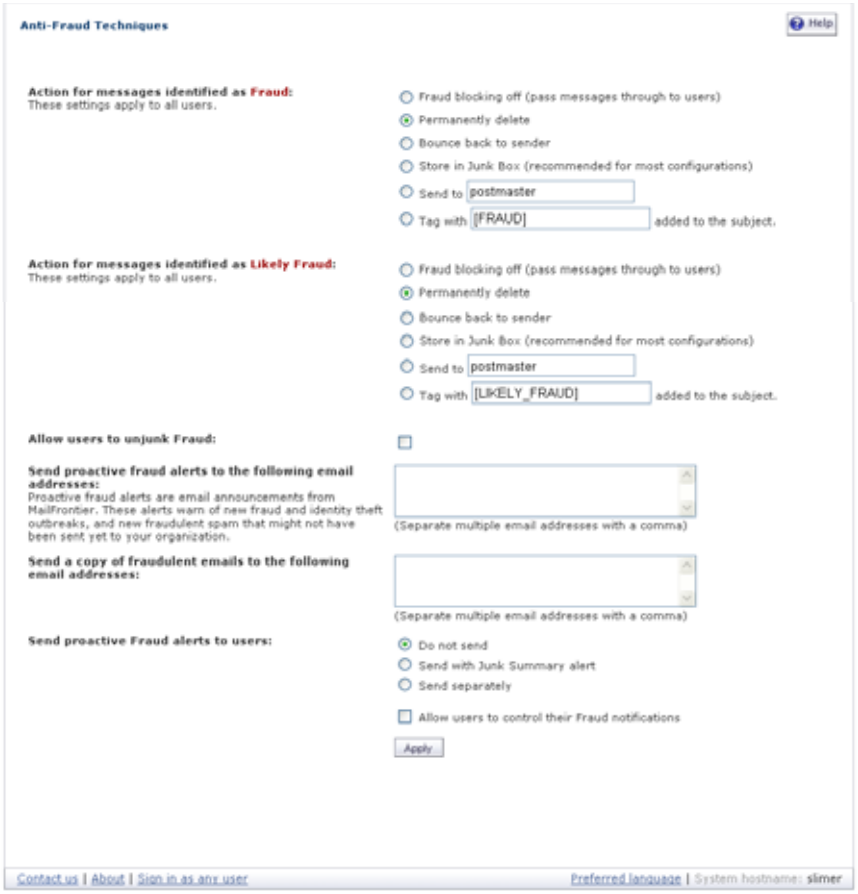
- Adapting SonicWALL Email Security's spam-fighting heuristics to phishing
- Divergence Detection™—ensures that all contact points are legitimate. Contact points include email addresses, URLs, phone numbers, and physical addresses.
- Sender ID or Sender Policy Framework (SPF)—a system that attempts to validate that a message is from the domain from which it purports to be. Sender ID authenticates that the domain from which the sender's message reports matches one of the IP addresses published by that domain.
  SonicWALL Email Security factors Sender ID pass or fail into its junk algorithm. For more information about Sender ID, see "Authenticating the Sender's Domain via Sender ID" on page 105.

Configuring Phishing Protection

To configure SonicWALL Email Security Gateway to screen for phishing:

1. Click the **Anti-Phishing icon**.
   The window in Figure 10.1, "Anti-Phishing Window," on page 121 appears.

Figure 10.1 Anti-Phishing Window



2. Click the radio button to choose which action to take for messages that contain **Phishing**.
3. Click the radio button to choose which action to take for messages that contain **Likely Phishing**.
4. Check the **Allow users to unjunk phishing messages** checkbox if you want to allow users to unjunk fraudulent messages.
5. Enter one or more email addresses of people designated to receive **proactive phishing alerts**.
6. To send copies of fraudulent email messages to a person or people designated to deal with them, enter the recipients' email addresses in the **Send copies of emails containing phishing attacks to the following email addresses** text box.
7. SonicWALL Email Security enables you to **send proactive phishing notifications to users**. Select one of the following radio buttons:
   - **Do not send**
   - Send with Junk Summary alert
   - **Send separately**
8. Click the **Allow users to control their phishing notifications** check box to give users control. If you allow users to control their phishing notifications, they can choose whether or not to receive notifications and whether they should receive notifications as part of their Junk Summaries or separately, as shown in Step 7.
9. Click **Apply**.

Use SonicWALL Email Security's Community to Alert Others

Phishing is continuously evolving and adapting to weaknesses in the organization's network. Malicious hackers use any known weakness to infiltrate the corporate firewall.

SonicWALL Email Security has tuned and enhanced their spam-management techniques to prevent phishing. SonicWALL Email Security also collects incidences of phishing and summarizes the email addresses, text, phone numbers, and domains of phishing perpetrators in a database, which stores the thumbprints of the phishing message.

Report Phishing and Other Enterprise Fraud to SonicWALL Email Security

SonicWALL Email Security alerts organizations to phishing attacks. SonicWALL Email Security needs you to report fraudulent email messages to mailto:fraud@MailFrontier.com. Reporting phishing enables SonicWALL Email Security to alert other users to the phishing attacks you experienced.

CHAPTER 11

Policy Management

SonicWALL Email Security's Policy Management module enables you to write policies to filter messages and their contents as they enter or exit your organization. Policies can be defined only by an administrator. Typical use of policies include capturing messages that contain certain business terms, such as trademarked product names, company intellectual property and dangerous file attachments.

Basic Concepts for Policy Management

Policy Management enables you to filter email based on message contents and attachments. You can filter for specific terms that you want, such as terms in your product or terms you do not want in your organization's email.

You manage policy by creating filters in which you specify the words to search for in content, senders, or other parts of the email. After filtering for specified characteristics, you can choose from a list of actions to apply to the message and its attachments.

Defining Word Usage

In the context of Policy Management, a *word* is a series of alphabetic characters and numbers with no spaces. Table 1, "Word Usage in Policy Management," on page 124 explains the punctuation rules for words.

Table 1 Word Usage in Policy Management

Punctuation allowed anywhere	**Character**	**Example**
Slash	/	http://mailfrontier.com
Punctuation allowed as first or last character but not in the middle.	**Character**	**Example**
Dollar sign	**$**	**$100**
Percent sign	**%**	**100%**
Punctuation allowed in the middle but not as first or last character	**Character**	**Example**
Period	.	http://example.com **is allowed.** .mail **or** mail. **are not allowed.**
"at" sign	@	joe@sonicwall.com
Ampersand	**&**	**AT&T**
Colon	**:**	http://example.com
Hyphen	**-**	**xxx-yyy**

All other punctuation is used as word separators to split words. Punctuation included in this category includes the following characters:

~ ! # ^ * + = { } [ ] ; " < > , ? \ | `()"

For example, X~Y is treated as two words, X and Y.

Word Matching vs. Phrase Matching

When *Word Matching* is enabled, words can be in any order. For example, if you entered the words *Mars, Venus, Jupiter*, SonicWALL Email Security Gateway would match *Venus, Jupiter*, and *Mars.*

When *Phrase Matching* is enabled, words are matched in the order in which they are entered, so, in the above example, only *Mars, Venus, Jupiter* triggers a match.

Words specified in a single condition statement and separated by commas are always assumed to be the same as an ALL (logical AND) condition where all the words must exist in the content for the condition to be true.

Defining Email Address Matching

Policy Management can do intelligent matching for email addresses in the **From** and **To/CC/BCC** fields. The following table illustrates with examples how address matching works.

Table 2 Intelligent Address Matching

Address field	Matching strings		
	`jdoe`	`company.com`	`jdoe@company.com`
`jdoe@company.com`	Match	Match	Match
`asmith@company.com`	No Match	Match	No Match
`jdoe@yahoo.com`	Match	No Match	No Match

Defining Intelligent Email Attachment Matching

When you create a policy to detect attachments based on file extension, by default, SonicWALL Email Security Gateway will do simple matching based on the specified file extension. If the attachment has been renamed to have a different file extension, this simple matching will not detect that. To accurately detect attachments without relying on the file extension, select **Intelligent Attachment Matching** checkbox. For example, an executable attachment renamed to .txt extension can be matched as an executable. SonicWALL Email Security Gateway supports **Intelligent Attachment Matching** for the following file extensions.

Table 3 Intelligent Matching File Types

File Format	File Type	File Extension
Image	Bitmap format	.bmp
Image	FITS format	.fits
Image	GIF format	.gif
Image	Graphics Kernel System	.gks
Image	IRIS rgb format	.rgb
Image	ITC (CMU WM) format	.itc
Image	JPEG File Interchange Format	.jpg
Image	NIFF (Navy TIFF)	.nif
Image	PM format	.pm
Image	PNG format	.png
Image	Postscript format	.[e]ps
Image	Sun Rasterfile	.ras
Image	Targa format	.tga
Image	TIFF format (Motorola - big endian)	.tif
Image	TIFF format (Intel - little endian)	.tif
Image	X11 Bitmap format	.xbm
Image	XCF Gimp file structure	.xcf
Image	Xfig format	.fig
Image	XPM format	.xpm
Compressed	Bzip	.bz
Compressed	Compress	.Z
Compressed	gzip format	.gz
Compressed	pkzip format	.zip
Archive	TAR (pre-POSIX)	.tar
Archive	TAR (POSIX)	.tar
Excecutable	MS-DOS, OS/2 or MS Windows	.exe
Executable	Unix elf	
Miscellaneous	pgp public ring	
Miscellaneous	pgp security ring	
Miscellaneous	pgp security ring	
Miscellaneous	pgp encrypted data	

Defining Disguised Text Identification

SonicWALL Email Security provides disguised text identification to prevent users in your organization from sending or receiving messages with unwanted words with substituted, inserted, constructed, or deleted characters. Using traditional word matching or spell checking finds exact matches or known frequent misspellings, such as *hte* for *the*.

Disguised text identification is as simple and intuitive as traditional word matching; and is more powerful than using regular expressions to find specific words or terms. In addition, it is far easier to use and less potentially dangerous than regular expressions.

Disguised text identification provides the following types of matches: <Xref_Color>Table 4 shows a few of the multitude of variations.

Table 4 Variations matched

Variations	Resulting Words or Phrases
Constructed characters	**\ / for V, or \./\/ for W, for example,** `\/\/ork at home`
Inserted characters	`-` **or** `_`**, for example,** `c-o-m-m-e-n-t` **or** `f_e_e_s`
Substituted characters	`@` **for** `a` **or** `1` **for** `i`**, for example,** `p@ntyhose` **or** `Sat1sfact10n`
Deleted characters	***wnderful opprtunty***
Imaginative spelling	`Purrfection` **or** `garunteeed suxess`

NOTE: Disguised text identification might result in false positives due to unexpected conditions, and can be computationally intensive.

Disguised text identification is not meant to be a spam catcher. SonicWALL Email Security has developed extensive heuristic statistical techniques for catching spam. Instead, this feature allows you to detect terms that are important to your organization and build policies based on them. You can use this feature to capture specific terms, for example, route incoming messages your product's name with appropriate trademarks for your sales departments. It can also be used to filter outgoing mail. As an example, if your organization prohibits sending source code outside of the company, you could use various programming keywords as hostile terms and route messages with those terms to the appropriate manager.

Inbound vs Outbound Policy

Organizations can create policies to deal with both inbound and outbound messages.

Figure 11.1 Inbound vs Outbound Policy

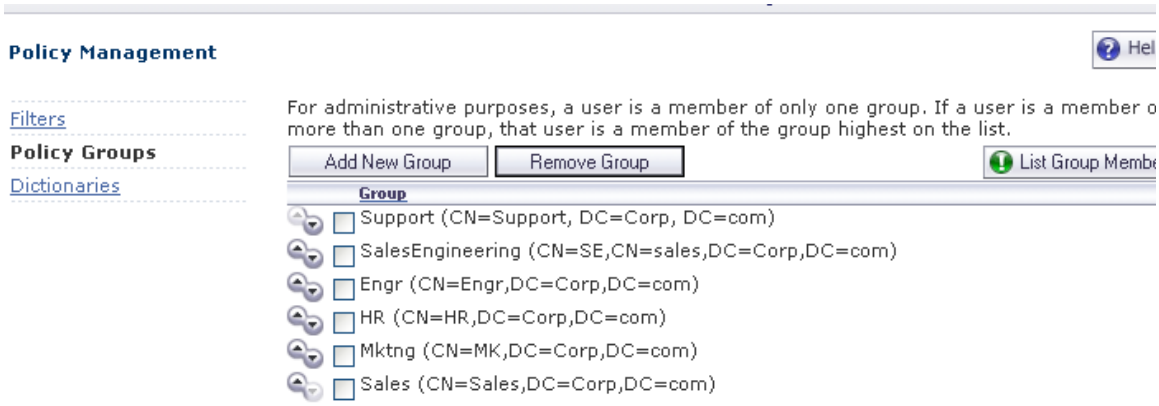
To create inbound policies select **Inbound** tab and click on **Add New Inbound Filters.** Policies created on the inbound path can not be shared with the outbound path and vice versa. To create outbound policies, select **Outbound** tab and click on **Add New Outbound Filter**.

Policy Groups

In some cases, it may be appropriate to associate a policy filter to a group of users rather than the entire organization. For example, you may want a policy filter to be applied to all incoming email messages sent to your sales team and no one else in your organization.

If you want policy filters you create to be applied to particular group of users, you first have to create policy groups from LDAP. Policy groups, once created, can be associated with either inbound or outbound policies.

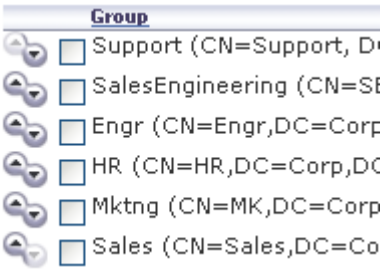
Figure 11.2 Policy Groups



To manage policy groups, select **Policy Groups** link under **Policy Management** module as shown in Figure 11.2. From this screen, you can manage all policy groups for your SonicWALL Email Security Gateway setup. To add a new policy group, select **Add New Group button**. To remove a group, check the group(s) to be removed and select the **Remove Group** button. You can view the members of a group by selecting that group and clicking on the **List Group Members** button.

If an user is present in more than one group, that user is treated to be a member of the group that is listed highest in the list. You can change group ordering, by clicking on the arrows to the left of listed groups. To change the order in which groups are listed, use the up and down arrow icons to the left of the groups.

Figure 11.3 Groups

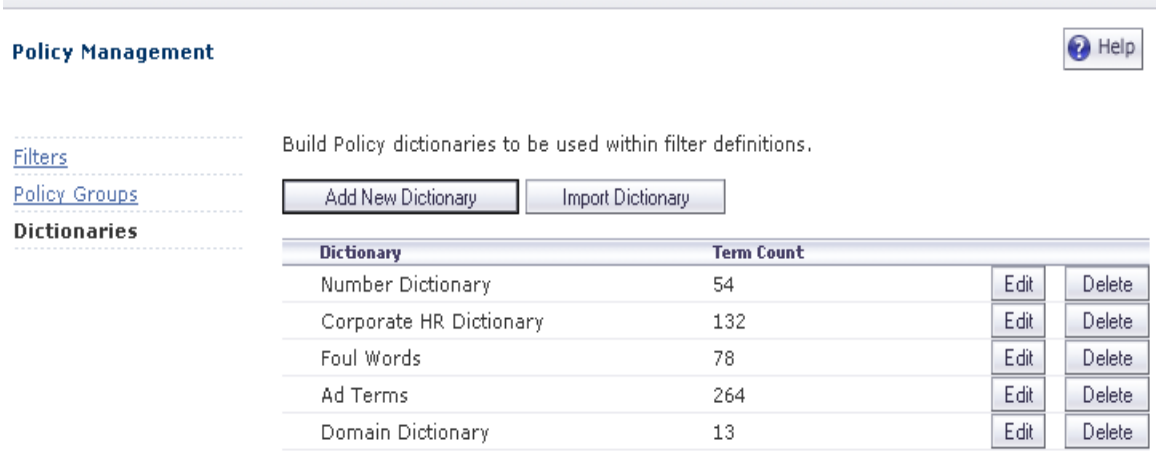


For example in the above illustration, if *jdoe@company.com* is listed under both *SalesEngineering* and *Sales*, the policy filter that is associated with *SalesEngineering* will be applied to email messages for *jdoe@company.com*.

Dictionaries

A Dictionary is a convenient collection of set of words or phrases that you can group together for use in Policy Filters. A dictionary can be specified as a search value in Policy Filter.

Figure 11.4 Dictionaries

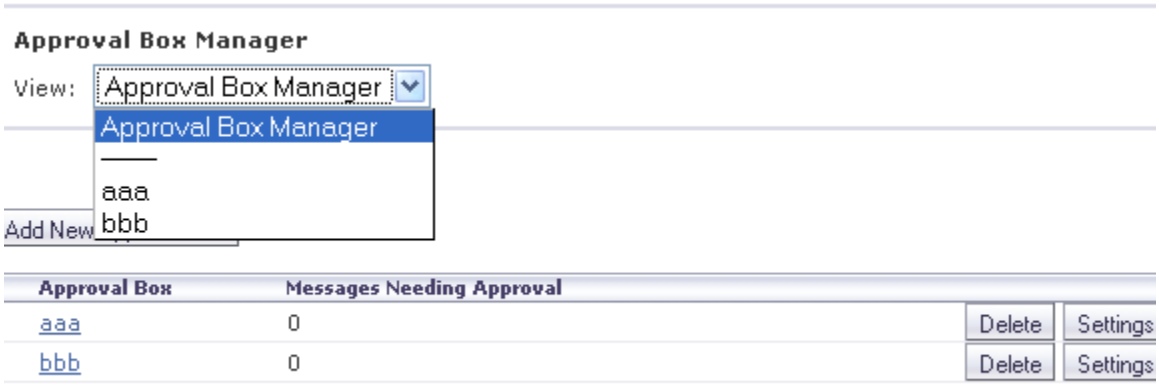


Dictionaries can be created or modified either manually or by importing from a file in the file system. To manually add/edit a dictionary, click on the **Add New Dictionary** button. To import from a file on the file system, click on the **Import Dictionary** button. The imported file should one word or phrase per line and each line should be separate by <CR>.

Approval Boxes

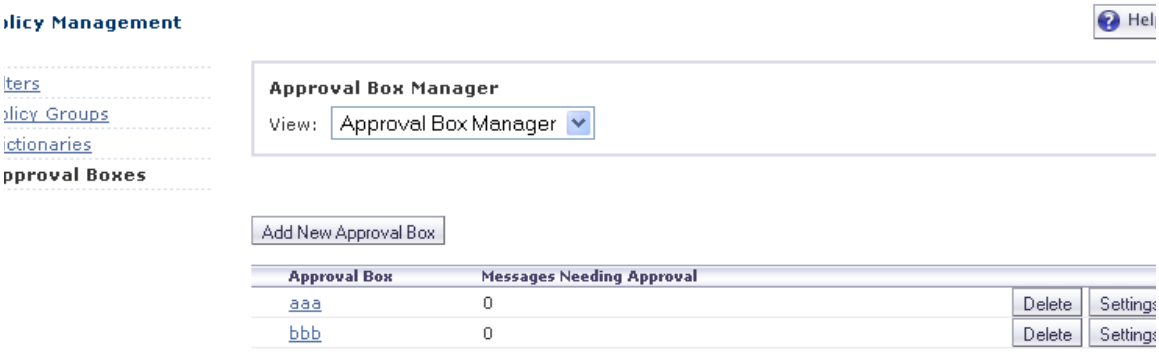
An Approval Box is a list of stored email messages that are waiting for an administrator to take action. They will not be delivered until an administrator approves them for delivery. The **View** drop-down list allows you to have two different views of Approval Boxes: the manager view and the individual approval box view

Figure 11.5 View Drop-down List



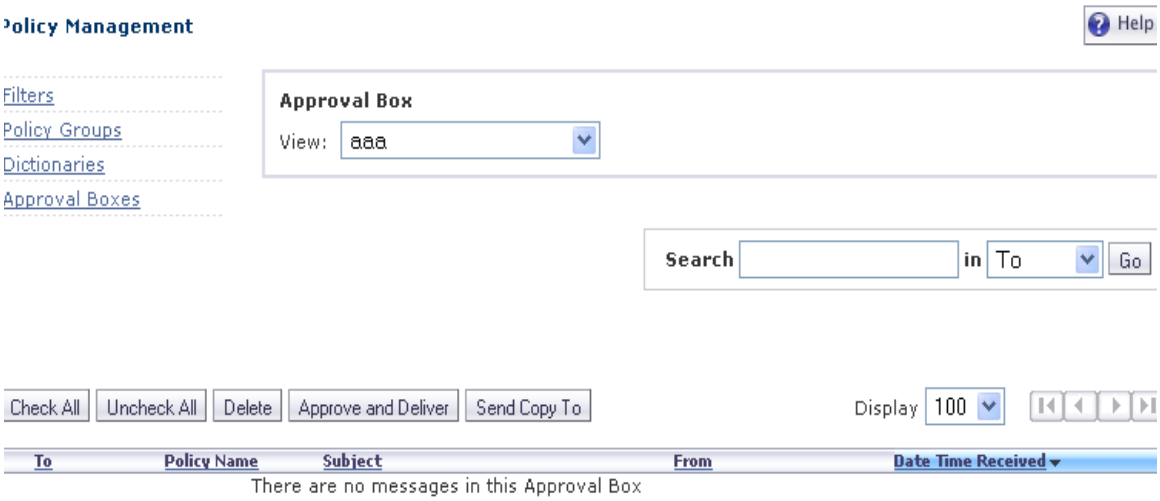
To see a list of the Approval Boxes that have been created, choose **Approval Box Manager** from this list. The Approval Box Manager view allows you to edit or delete existing Approval Boxes, and to create new Approval Boxes.

Figure 11.6 Approval Box Manager View



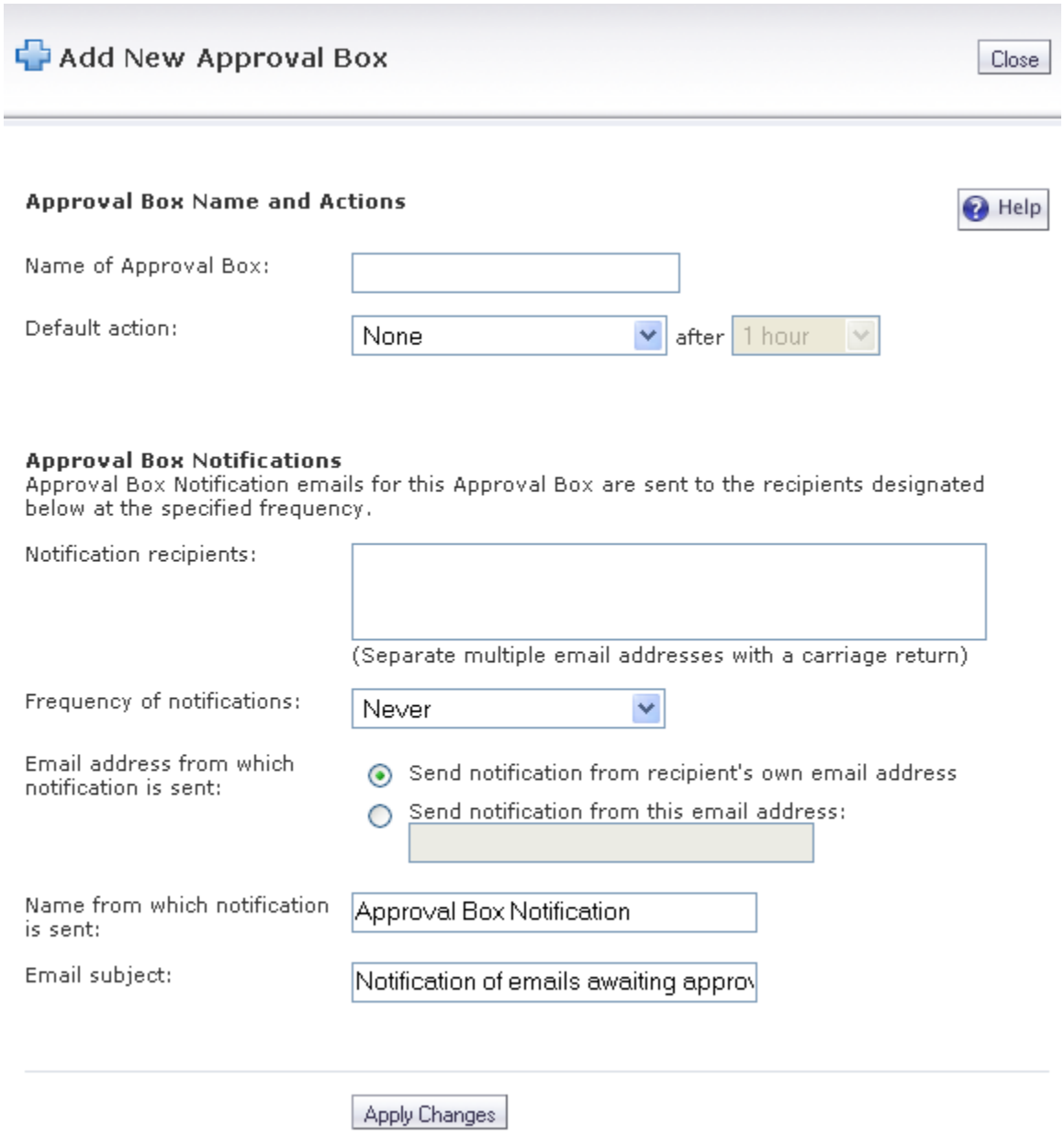
To see the contents of a particular Approval Box, choose the desired Approval Box name from the **View** drop-down list. This page allows you to search the messages stored in that Approval Box and to take action on any of those messages.

Figure 11.7 Individual Approval Box View for a Box named "aaa"



To store messages in an Approval Box, you must first create the Approval Box by clicking the **Add New Approval Box** button on the Approval Box Manager page. Then, go to the **Policy Management > Filters** page and create a policy filter that has Store in Approval Box as its Action, and choose the desired Approval Box for email messages caught by that filter.

Figure 11.8 Add New Approval Box



1. Enter a **name** for this Approval Box. This name will appear in the page that shows the list of approval boxes and in the drop-down list that allows you to select the detailed view of individual approval boxes.
2. Select a Default action to be taken. This action will automatically be taken on the message waiting for approval if the administrator does not respond to the notification within the period of time specified.
3. Enter a list of **email recipients** in the text box. Separate multiple email addresses with a carriage return.
4. Select the **frequency** of the notification emails from the drop-down list.

5. Specify the email address from which this notification is sent.
6. Specify the name of the sender of notification emails. This is a human-readable name that will appear in your mail client as the sender of the notification email. This does not need to be a real name.

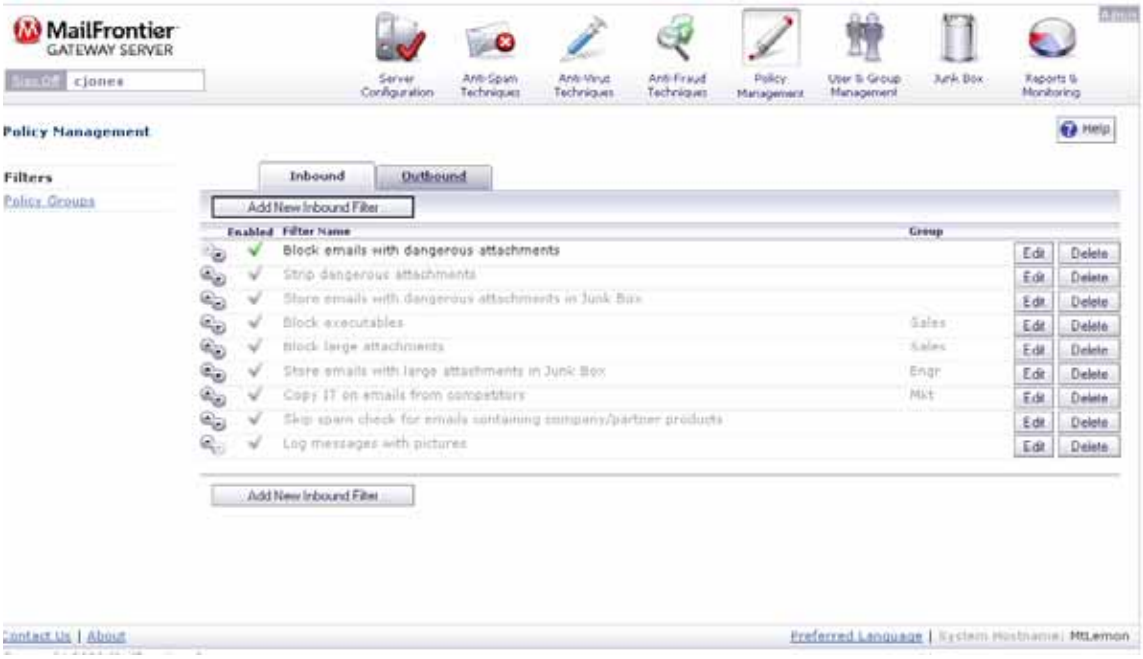
   Examples: *Charles Nelson Reilly, Approval Box Notification*, SonicWALL Email Security *Gateway Administrator, Joe Bloggs*

   Please use only 7-bit ASCII text.
7. Select the **email subject** line for this notification.
8. Click the **Apply Changes** button to save your changes to this approval box notification.

Policy Filters

A Policy Filter is an action or actions you want SonicWALL Email Security Gateway to take on messages that meet the conditions you define. To create and manage policy filters, select **Filters** link under **Policy Management** module.

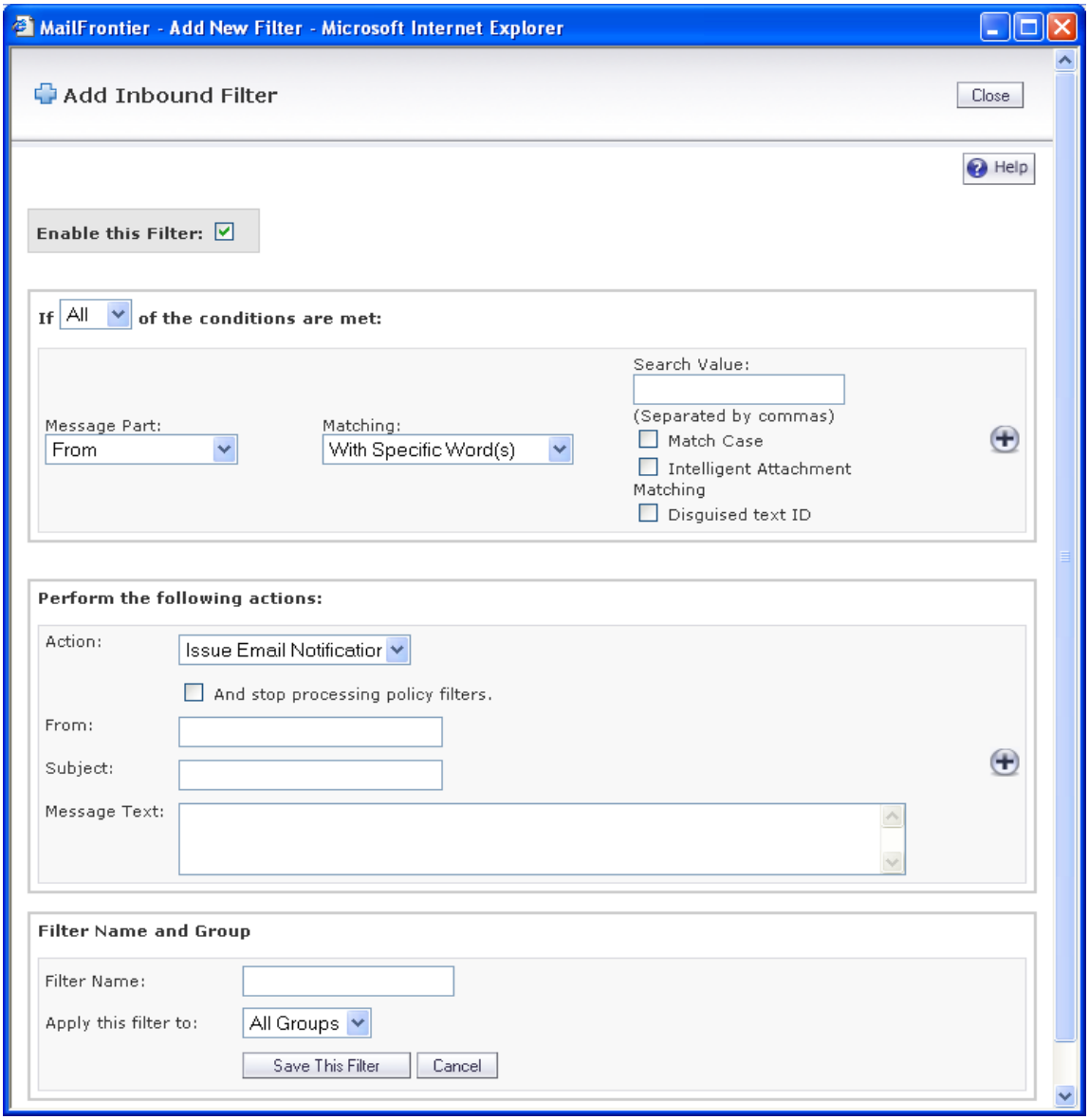
Figure 11.9 Policy Filters



Select the **Inbound** or **Outbound** tab to create filters for inbound or outbound email messages respectively.

1. Click the **Add New Inbound (Outbound) Filter** button.
   The **Add Inbound (Outbound) Filter** window appears, as shown in <Xref_Color>Figure 11.10 on page 133.

Figure 11.10 Adding a Filter



Note The fields in the window will change based on the action you choose.

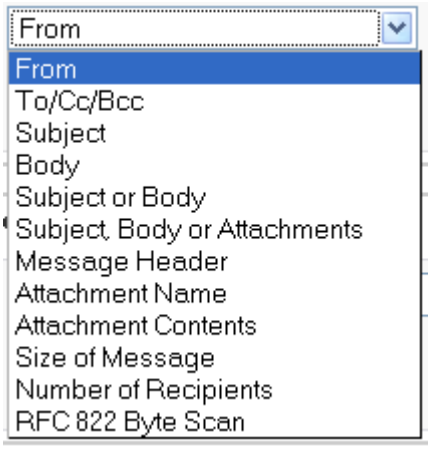
2. The **Enable this Filter** checkbox is checked by default. Uncheck the checkbox to create rules that do not go into effect immediately.
3. Choose whether the filter matches **All** of the conditions or **Any** of the conditions

Match	Action
All	**Causes email to be filtered when *a11* of the filter conditions apply (logical AND)**

Any **Causes email to be filtered when *any* of the conditions apply (logical OR)**

4. Choose the part of the message to filter.

Figure 11.11 Message Part filter drop-down list



The message part filter conditions are described in the table below:

Message Part	Action
From	**Filter by the sender's name**
To/Cc/Bcc	**Filter by the names in the To: cc: or bcc: fields**
Subject	**Filter by words in the subject**
Body	**Filter based on information in the body of the email**
Subject or Body	**Filter based on information in the subject and body of the email**
Subject, Body, or Attachments	**Filter based on information in the subject, body, and attachments of the email**
Message header	**Filter by the RFC822 information in the message header fields, which includes information including the return path, date, message ID, received from, and other information**
Attachment name	**Filter attachments by name**
Attachment contents	**Filter based on information in the email attachments**
Size of message	**Filter messages based on the size of the message**
Number of recipients	**Filter messages based on the number of recipients**
RFC 822 Byte Scan	**Scan the entire email message**

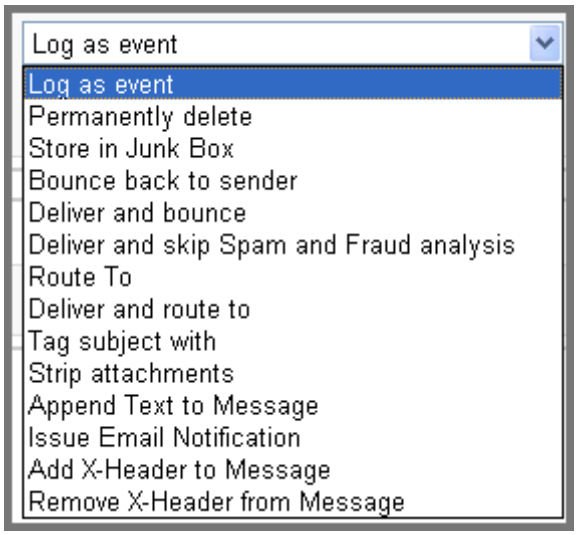
5. Choose the matching operation. The choices for matching operation vary with the message part being matched against. The following table describe the matching operations available.

With Specific Word(s)	**message part contains *all* of the specified words**
Without Specific Word(s)	**message part *does not* contain any of the specified words**
With Specific Phrase	**message part contains *all* the words in the order entered**
Without Specific Phrase	**message part contains *none* of the words in the order entered**
Starts With	**message part starts with the specified word(s)**
Ends With	**message part ends with the specified word(s)**

Enter the words or phrase that you want to filter in the **Search Value** text box. Separate multiple terms with commas, for example: *Mars, Venus*. Select the appropriate check boxes: **Match Case**, **Intelligent Attachment Matching** and **Disguised Text Identification**.

Note **Disguised Text Identification** can not be used together with **Match Case** and can be selected only for **Body** and **Subject** message parts.

6. Click the **plus sign** (+) to add another layer of filtering. See “Junk Emails with Attachments over 4MB” on page 138.
   You can add up to 20 filters.
   Filters are similar to rock sifters. Each additional filter adds further screens that test email for additional conditions.
7. Choose the response action from the **Perform the following actions** drop-down list.



The following table describes the different actions and the effect they have on the message.

Table 5 Filter Responses to Messages that Trigger Policy Alerts

Response	Effect
Log as event	**The email message is logged. No further processing in Policy management occurs (default). This option stores a log of all messages so that the administrator has a record and can analyse traffic patterns. The log is in the `mfe` log. NOTE: Policy management logs all messages as events regardless of the action specified.**
Permanently delete	**The email message is permanently deleted and no further processing occurs in any SonicWALL Email Security module occurs. This option does not allow the user to review the email and can cause good email to be lost.**
Store in Junk Box	**The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions. The user has the option of unjunking the email.**
Store in Approval Box	**The email message is stored in the Approval Box. It will not be delivered until an administrator approves it for delivery.**
Bounce back to sender	**The message is returned to sender with an optional message indicating that it was not deliverable.**
Deliver and bounce	**The message is delivered to the recipient and is bounced back to the sender with an optional message.**
Deliver and skip Spam and Phishing Analysis	**The message is delivered without spam or phishing analysis.**
Route to	**The message is routed to the specified email address. The message can be routed to only one email address.**

Table 5 Filter Responses to Messages that Trigger Policy Alerts (continued)

Response	Effect
Deliver and route to	**Deliver to the recipients and also route to the specified email address. The message can be routed to only one email address**
Tag subject with	**The subject of the email is tagged with a the specified term.**
Strip all attachments	**Remove all the attachments from the email.**
Append text to message	**The specified text is appended to the message body.**
Issue email notification	**Sends an email notification to the recipients of the email that triggered the rule.**
Add X-header to message	**Adds a X-header to the email.**
Remove X-header from message	**Removes a X-header from an email.**

When no additional filtering is required on a message, select the **and stop processing policy filters** checkbox. This checkbox is automatically selected and grayed out when you have selected a terminal action.

If additional actions need to be performed on the same message, select the **plus sign** (+) to the right. You cannot add the same action more than once to a specific filter rule. As a result, once an action has been selected, it will not be available in the drop-down list for further selection within the current filter rule.

8. Type a descriptive name in the **Filter Name** text box.
9. Select a policy group you want to apply this filter to. By default, **All Groups** will be selected and this filter will apply to all email messages.
10. Click **Save This Filter**.

Language Support

Policy management supports filtering messages based on non-English terms in the **Search Value.** For example, you can search for a Japanese word or phrase in the body of a message. However, SonicWALL Email Security Gateway does not support adding text strings to email messages in languages other than English and does not support foreign language filter names.

Note To view messages in Asian languages, you might need to install East Asian Language Packs on the server where you run SonicWALL Email Security Gateway.

Managing Filters

The main Policy Management UI,<Xref_Color>Figure 11.9 on page 132, lists all the filters created in the system for the **Inbound** and **Outbound** path. From this view, you can **Add New Filter**, Change the order of filters, **Edit** or **Delete** filters. Filters that have been enabled are indicated with a green tick mark.

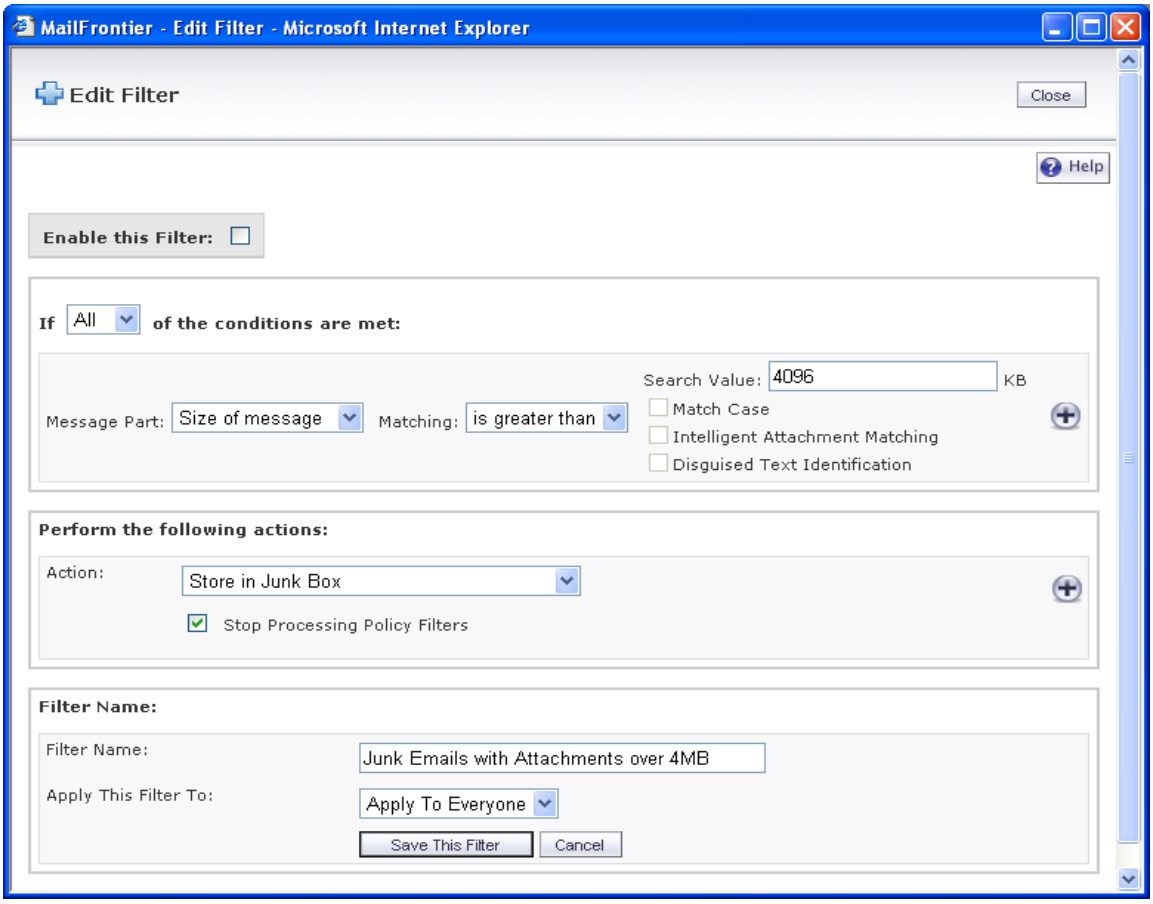
Editing a Filter

To change a filter that has been saved:

1. Click the **Edit** button adjacent to the filter to be changed.

   Figure 11.12 is an example of the Edit Filter window.

Figure 11.12 Edit Filter



2. Change any of the filter conditions.
3. Click **Save This Filter**.

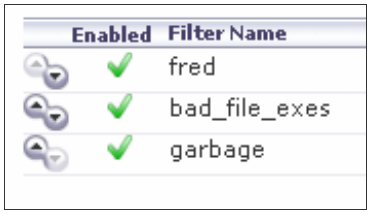
Deleting a Filter

To delete a filter, click the **Delete** button adjacent to the filter.

Changing Filter Order

Filters are processed in the order they appear. When **and stop processing policy filters** checkbox is selected in any policy filter, that filter is the last one to process the message and no further policy filtering will take place on that message.

To change the order of the filters, use the up and down arrow icons to the left of the filters.



Preconfigured Filters

New installations of SonicWALL Email Security Gateway ship with few preconfigured filters. These preconfigured filters are not enabled by default.

NOTE: If you have previously run SonicWALL Email Security Gateway, these filters are not automatically installed. You can create your own filters: see “Policy Filters” on page 132.

Strip Potentially Dangerous File Attachments

This filter, *Strip Potentially Dangerous File Attachments*, strips all attachments from the incoming email messages that triggered the filter conditions. Enable and edit this rule if you want to allow some of these attachments and not others.

Junk Emails with Attachments over 4MB

This filter, *Junk Emails with Attachments Over 4MB*, stores all incoming email messages over 4MB in size in the Junk Box.

Strip Picture and Movie Attachments

This filter, *Strip Picture and Movie Attachments*, strips all attachments from the incoming email messages that triggered the filter conditions. Enable and edit this rule if you want to allow some of these attachments and not others.

Advanced Filtering

Creating a multilayered Filter

You can create filters with multiple conditions chained together and multiple actions to be performed on the message, if the specified conditions are met.

For an example, if the email message is

- sent from NASA and
- the body contains the word Mars

then take the following actions:

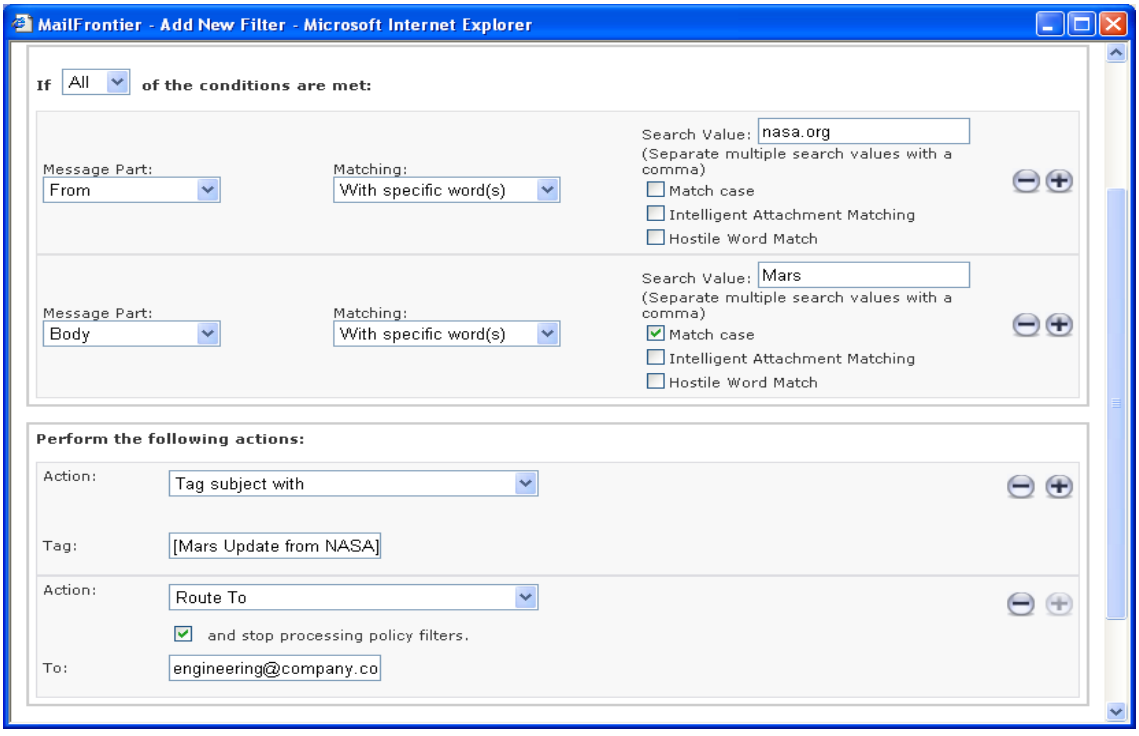
- Tag the subject with the term [Mars Update from NASA] and
- Route the message to *engineering*.

To create a multilayered filter:

1. Click the **Add New Filter** button.
2. Select **All** conditions to be met
3. **With Specific Words** operation, search for `nasa.org` in the message part **From.**
4. Select the + button to the right to add another condition
5. **With Specific Words** operation, search for `Mars` in the message part **Body**. Select **Enable Match** case to get an exact case match.
6. Select the action **Tag Subject With**. Set the **Tag** field to `[Mars Update from NASA]`. Make sure **and stop processing policy filters** checkbox is not enabled.
7. Select the + button to the right to add another action
8. Select the action **Route To** and set the **To** field to `engineering@company.com`. Select **and stop processing policy filters** checkbox to stop further policy filtering on this message.
9. Save the filter.

The following figure illustrates the conditions and actions as specified in the UI.

Figure 11.13 Advanced Filter



Exclusive Actions

The action named **Permanently delete** is an exclusive action and is terminal in nature and no further policy filtering will be possible after this action has been performed. The **and stop processing policy filters** checkbox will be automatically enabled and grayed out if an exclusive action is selected.

Parameterized Notifications

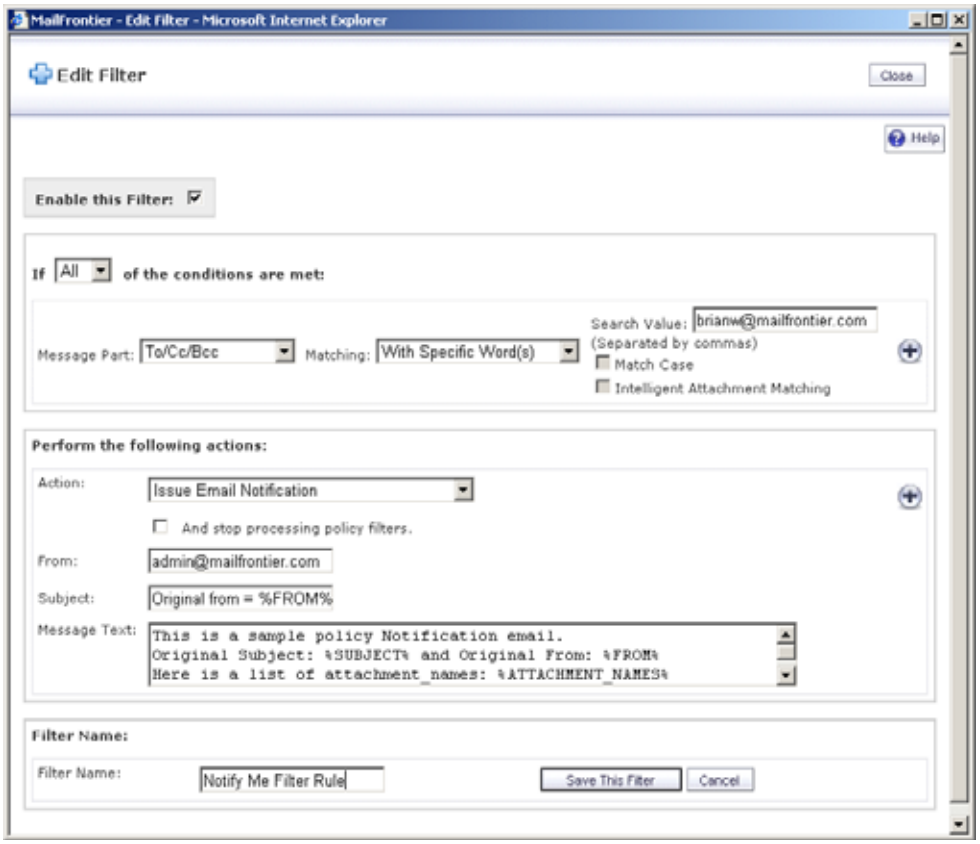
SonicWALL Email Security Gateway supports parameterized notifications wherein you can use pre-defined parameters in the text fields for the **Issue Email Notification** action. These parameters will get substituted with corresponding values when the message is processed. You can use these parameters in either the **Subject** or **Message Text** fields of the **Issue Email Notification** action. The parameters can be used multiple times and are substituted each time they are used. Each parameter entered should start and end with % symbol. The following table lists the supported policy notification parameters and shows the value of these parameters.

Table 6 Policy Notification Parameters

Parameter	Value
%SUBJECT%	the Subject: content from the triggering email
%FROM%	the From: content from the triggering email
%ATTACHMENT_NAMES%	a comma-separated list of attachment names from the triggering email
%FILTER_NAME%	the name of the policy filter which took the action on the triggering email
%MATCHED_TERM%	the Dictionary term which matched in the triggering email

Figure 11.14 is an example of a parameterized notification.

Figure 11.14 Parameterized Notification Filter



CHAPTER 12

User and Group Management

The User and Group Management function allows you to:

- Manage the list of users who can log in to the SonicWALL Email Security Gateway
- Assign roles to individual users or groups of users
- Set spam blocking options for groups of users

This chapter also describes how to assign a delegate to manage your Junk Box. For more information, see “Assigning Delegates” on page 153.

Note To manage users and groups from within this module, you need to have configured your SonicWALL Email Security Gateway setup to synchronize with your organization’s LDAP server. You can configure LDAP settings and queries on the **Server Configuration > LDAP Configuration** page.

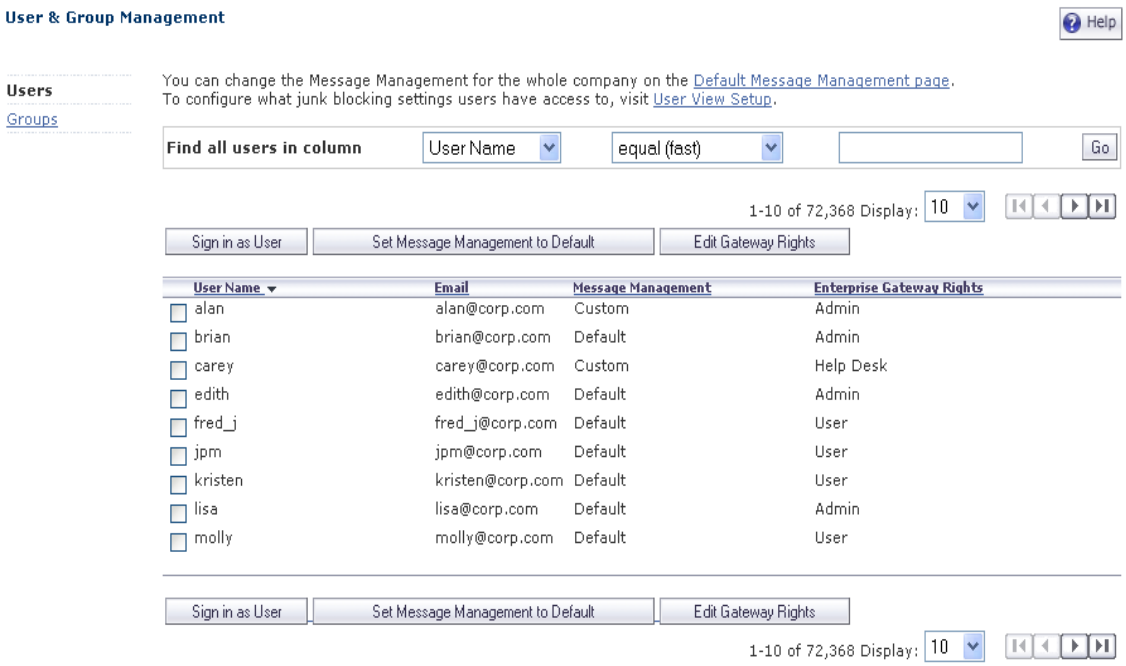
Note SonicWALL Email Security Gateway queries your corporate LDAP server every hour to update users and groups. Changes made to some settings in this section may not be reflected immediately on SonicWALL Email Security Gateway, but are updated within an hour.

Working with Users

To manage users in SonicWALL Email Security Gateway:

1. Click the **User & Group Management** icon.
   SonicWALL Email Security Gateway displays the Users and Groups window, as shown in <Xref_Color>Figure 12.1 on page 144.
2. Select the **Users** link.

Figure 12.1 User Management



From this screen, you can sign in as an user, set their message management settings to corporate default and edit their privileges in the system.

Searching for Users

If there are too many users to display in a window, select the search option from the drop down menu (equal, starts with, or contains), enter the search parameter in the blank field, and click **Go**. The search speed varies according to the search parameter.

Sort

Click **User Name** or **Email** to sort the list of users by that column.

Signing In as a User

Administrators can sign in as any user, see their Junk Box, and change the settings for that user. In addition, you can sign in as a particular user to manage their delegates for them.

Resetting User Message Management Setting to Default

Select one or more users and click **Set Message Management to Default** to restore all settings to the defaults. Be aware that this overrides all individual user preferences the user might have set.

Edit Gateway Rights

Administrators can assign different privileges to different users in the system by assigning them pre-defined roles. To assign a role to an user, select the user and click on **Edit Gateway Rights** button. See “SonicWALL Email Security Gateway Roles” on page 147 for more information.

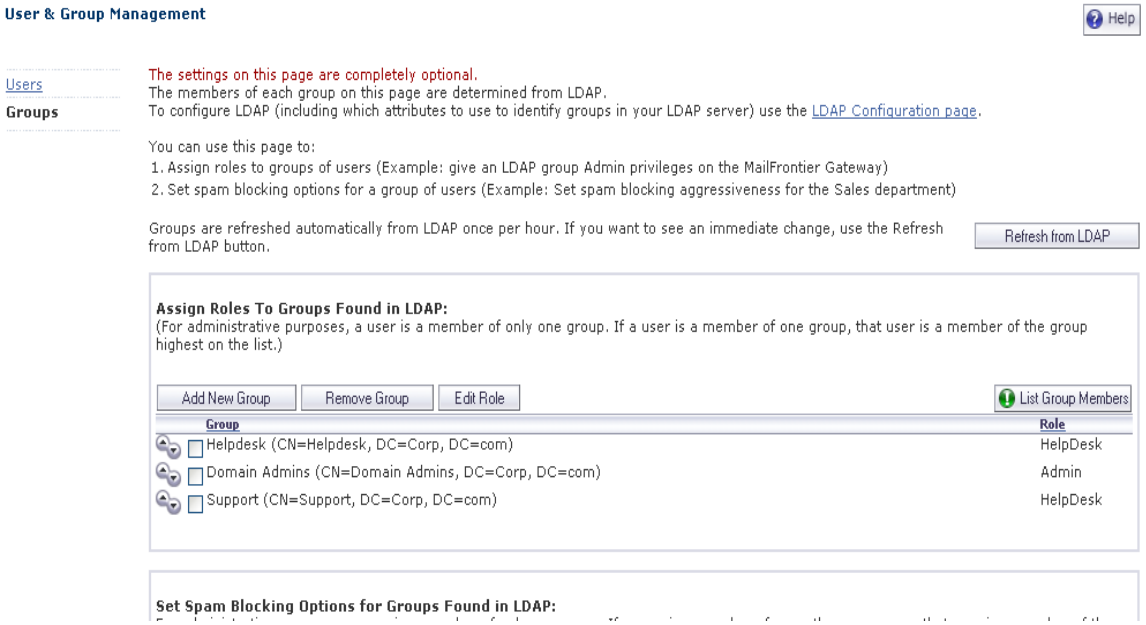
Working with Groups

About LDAP Groups

This section describes how SonicWALL Email Security Gateway lets you query and configure groups of users managed by an LDAP server. Most organization create LDAP groups on their Exchange server according to the group functions, for example: a group configured on their Exchange server called support represents the technical support groups in Exchange.

You must first configure LDAP groups on your corporate LDAP server before configuring the rights of users and groups on SonicWALL Email Security Gateway in the User and Group Management screen.

Figure 12.2 Managing Groups



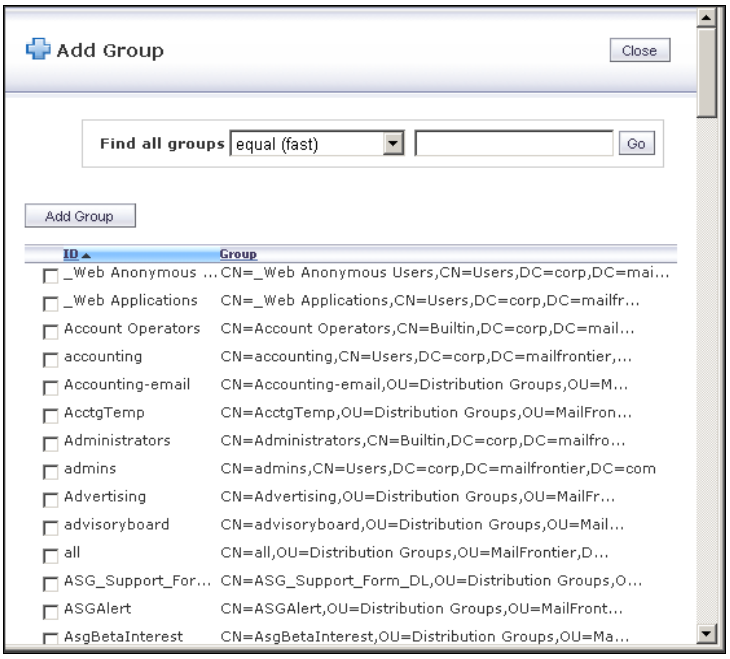
SonicWALL Email Security Gateway allows you to assign roles and set spam-blocking options for user groups. Though a user can be a member of multiple groups, SonicWALL Email Security Gateway assigns each user to the first group it finds when processing the groups. Each group can have unique settings for the aggressiveness for various spam prevention. You can configure each group to use the default settings or specify settings on a per-group basis.

Updates to groups settings in this section do not get reflected immediately. The changes will be reflected the next time SonicWALL Email Security Gateway synchronizes itself with your corporate LDAP server. If you want to force an update, click on the **Refresh From LDAP** button.

Add a New Group

To add a new group, Click **Add New Group** button. The Add Group window appears, as shown in <Xref_Color>Figure 12.3 on page 146 with a list of all the groups to which you can assign roles. You can also add new groups in this window.

Figure 12.3 Add Group



To find a group:

1. Search for the group you want by entering the name in the text box. Choose the search mechanism and search speed: **equals (fast)**, **starts with (medium)**, or **contains (slow)**. Click **Go** to begin the search.

   or

   Scroll through the list of groups to locate the group you want to add.
2. Click the checkbox to include the group.
3. Click **Add Group**.
   A message appears stating that the group was added successfully.

Removing a Group

1. Click the checkbox adjacent to the group(s) to remove.
2. Click the **Remove Group** button.
   A message stating the group was successfully removed appears.

Listing Group Members

1. Click the checkbox adjacent to the group to list.
2. Click the **List Group Members** button.
   Users belonging to that group will be listed in a pop-up window.

SonicWALL Email Security Gateway Roles

Roles are a set of privileges that you can grant any individual user or group of users in the SonicWALL Email Security Gateway. There are five defined roles that can be assigned to any user or group.

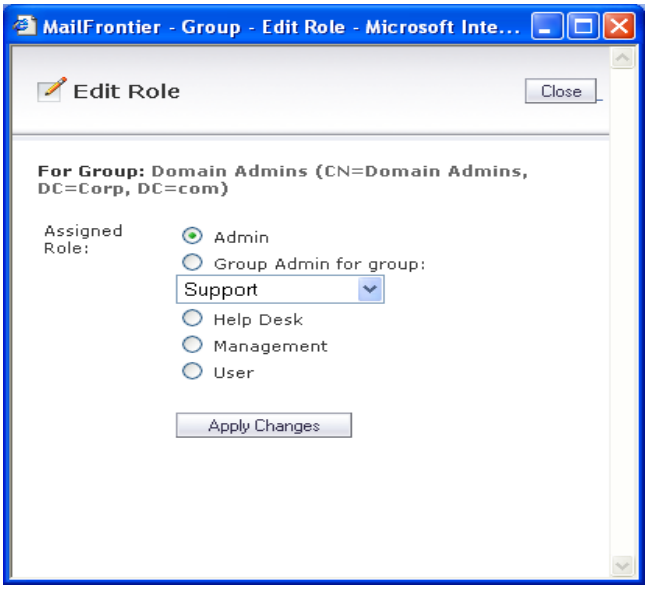
- **Admin:** An administrator role has full rights over the system. Administrators are taken to the system status page after logging in. They can log in as any user to change individual settings and view Junk Boxes, manage the corporate Junk Box, and configure everything.
- **Help Desk:** A Help Desk role can sign in as any user in the system, change their settings and address books, or operate on the Junk Box. This role is not allowed to change any corporate-wide settings and other server configurations.
- **Group Admin**: A group administrator role is similar to the Help Desk role except that this role's privileges are limited to users for the group they are specified to administer. Group Admin role is always associated with one or more groups added to the Spam Blocking Options for Groups section.
- **Manager:** A manager role has access to only system reports.
- **User:** Using the user role, you can allow users in your organization to log in to SonicWALL Email Security Gateway. SonicWALL Email Security displays their Junk Box as the opening window. In addition, you can also allow them access to other areas such as reports, message management, and lists.

Setting a LDAP Group's Role

All members of a group get the role assigned to the group. To set the role of a group:

1. Click the checkbox adjacent to the group to edit.
2. Click **Edit Role**
   A window appears with the group's name and current role.
3. Click the radio button for the appropriate role that you want to assign to the group.
4. Click **Apply Changes**.
   A message appears stating that the group was changed successfully.

Figure 12.4 Edit Group Role

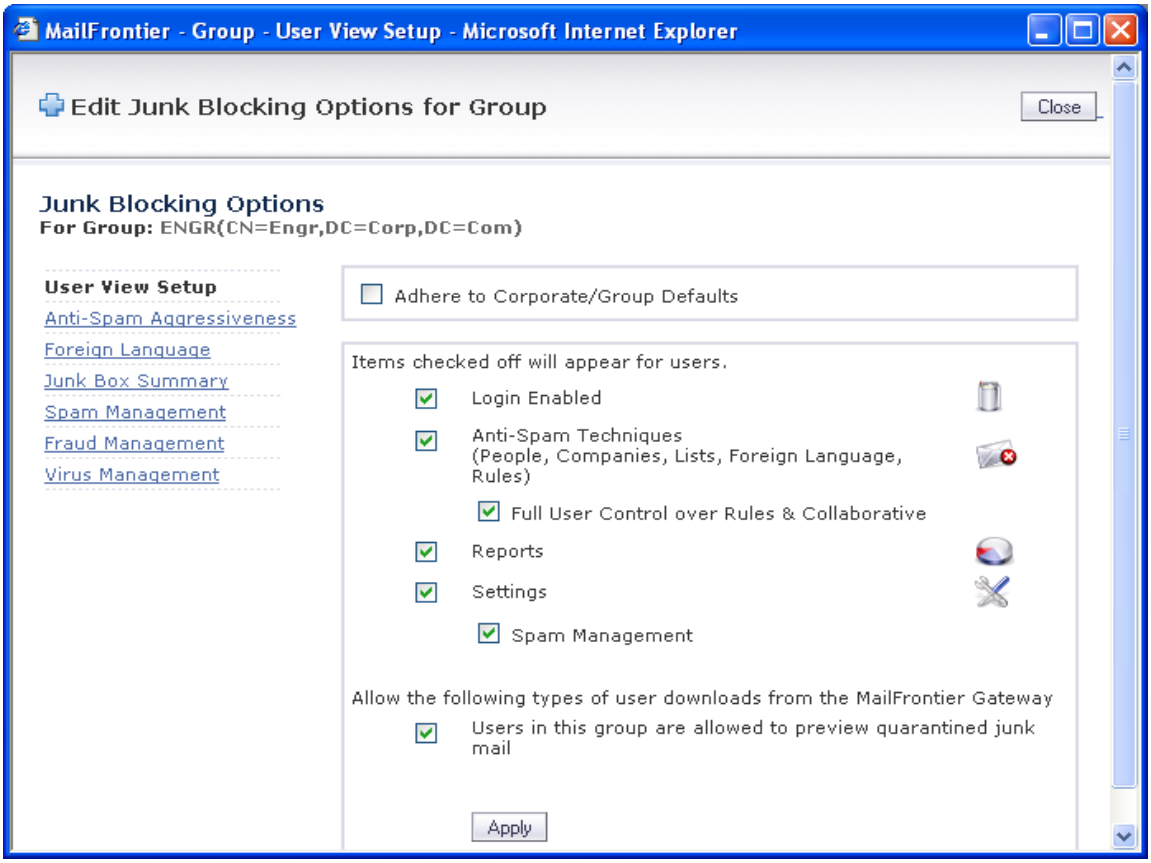


Setting Spam Blocking Options for LDAP Groups

All members of a group get the spam blocking options assigned to the group. To set spam blocking options for an LDAP group:

1. Click the checkbox adjacent to the group that you want to edit.
2. Click the **Edit Spam Blocking Options** button.
   The Edit Spam Blocking Options for Group window appears.

Figure 12.5 Edit Spam Blocking Options



Note

The **Adhere to Corporate/Group Defaults** box is checked by default. By opening this screen, you are now editing the spam blocking options for this one group. There is an **Adhere to Corporate Defaults** check box at the very top of each sub-page in this dialog, this check box only applies to the values on one page and for the current group only. For example, you can adhere to the corporate defaults for the two pages **User View Setup** and **Rules and Collaboration**, and uncheck the box and set custom settings for this one group for Foreign Language and then uncheck the box for and set custom settings for this group for Spam Management.

To enable the specified group to have special privileges, deselect the **Adhere to Corporate / Group Defaults** box.

User View Setup

This controls what options are available to the users in this group when they login to server using their user name and password. You can change the settings on the following items:

- **Login Enabled**—enables users in this group to log into their Junk Box
- A**llow/Block People, Companies, Lists, Foreign Languages, Rules**—Allows or blocks specified people, companies, foreign languages, and rules as these were configured in the user setup.
- **Reports**—let users in this group look at their Spam reports
- **Settings**—enables users in this group to view their settings
- Click the **Allow the following types of user downloads from the** SonicWALL Email Security **Gateway** check box to enable users in this group to preview quarantined junk mail.
- Click **Apply**.

Rules and Collaborative Settings

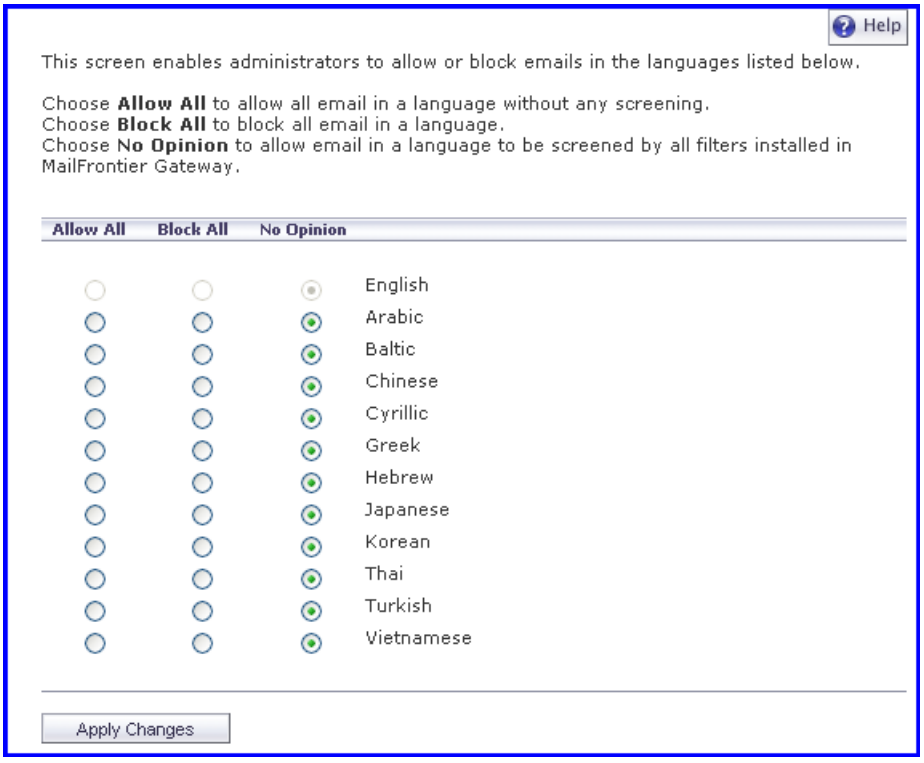
You can configure rules and collaborative settings for groups.

- Choose the appropriate **Collaborative** level for this group.
  You can adjust collaborative settings to customize the level of influence community input has on enterprise spam blocking.
- Choose the appropriate **Aggressiveness** level this group.
- For each category of spam, determine level and whether members of the group are allowed to unjunk their Junk Boxes.
- Click **Apply Changes**.

Configuring Foreign Language for Groups

You can determine the foreign language email that groups can receive.

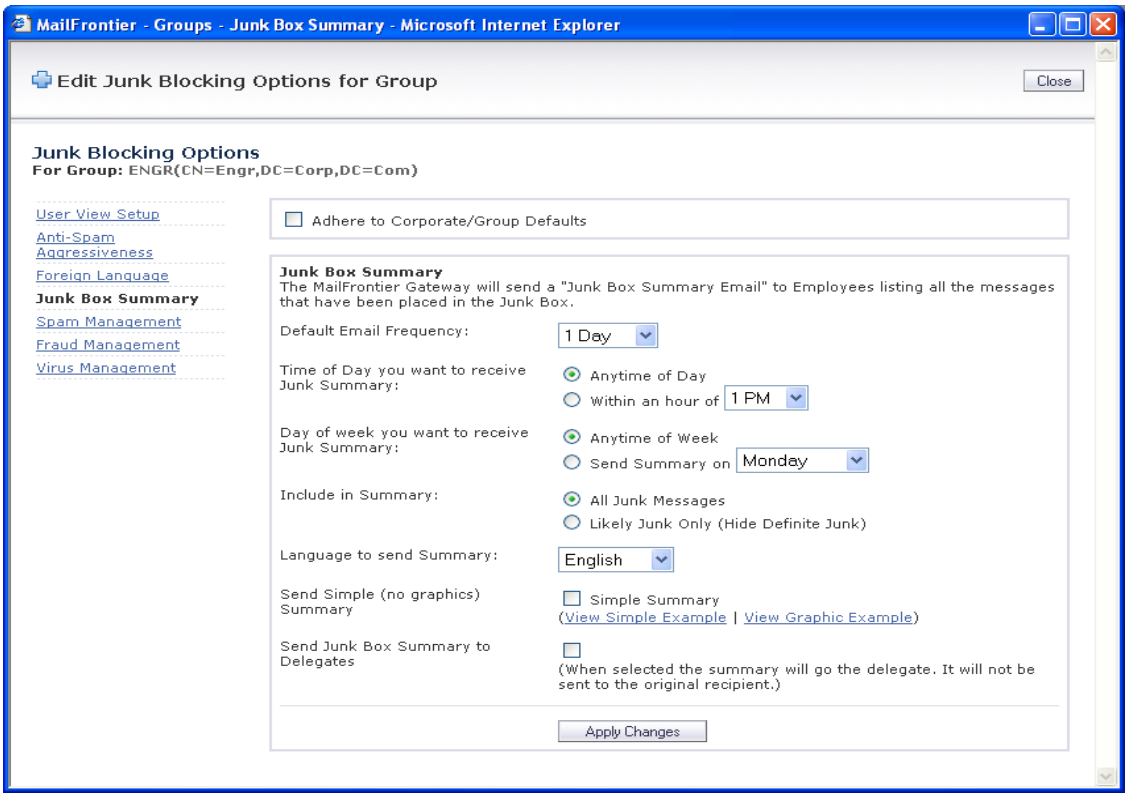
Figure 12.6 Foreign Languages



- Select **Allow All** to allow all users in a group to receive email in the specified language.
- Select **Block All** to block all users in a group from receiving email in the specified language.
- Click **No opinion** to permit email to be subject to the spam and content filtering of SonicWALL Email Security Gateway.
- Click **Apply Changes**.

Managing the Junk Box Summary

Figure 12.7 Editing Junk Box Summary options for a Group



To manage the Junk Box for groups:

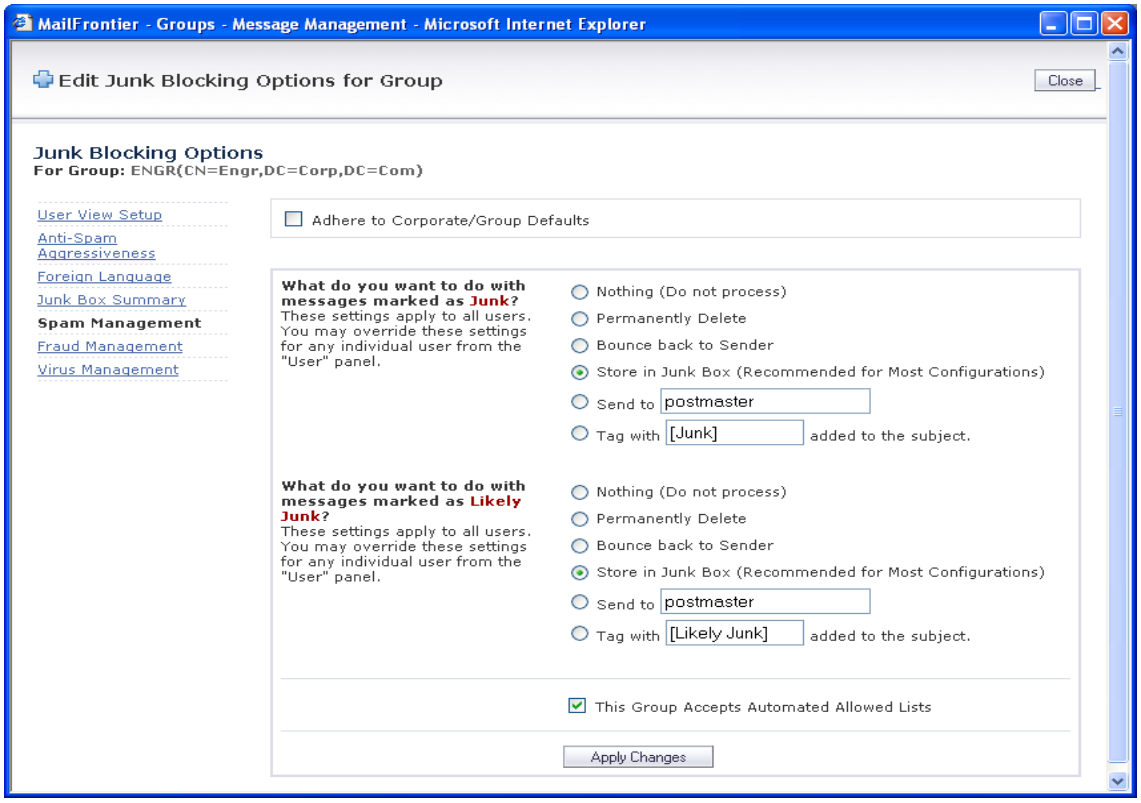
- Choose the **default email frequency** users to receive notification of junk email.
- Choose the **time of day** to receive junk email.
- Choose the **day of the week** to receive junk email.
- Choose what to receive in summary:

Click **Apply Changes**.

Spam Management

You can manage how groups deal with spam through the Spam Management window.

Figure 12.8 Editing Spam Blocking for Groups



To manage messages marked as Spam or Likely Spam for this group:

Choose what you want done with messages:

- **Spam Filtering Off**—passes all messages to users without filtering.
- Permanently Delete
- **Bounce back to sender**—send the message back to the sender.
  Caution: in cases of self-replicating viruses that engage the sender's address book, this can inadvertently cause a denial of service to a non-malicious user.
- **Send to**—you must specify an email address for the recipient.
- **Tag with**—label the email to warn the user. The default is [JUNK].

Click **Apply Changes**.

Phishing Management

The phishing management window gives you the option of managing phishing and likely phishing settings at a group level. Just like spam management options, it allows to you deal with phishing differently for different groups. However, unlike spam management options, these settings cannot be altered for individual users.

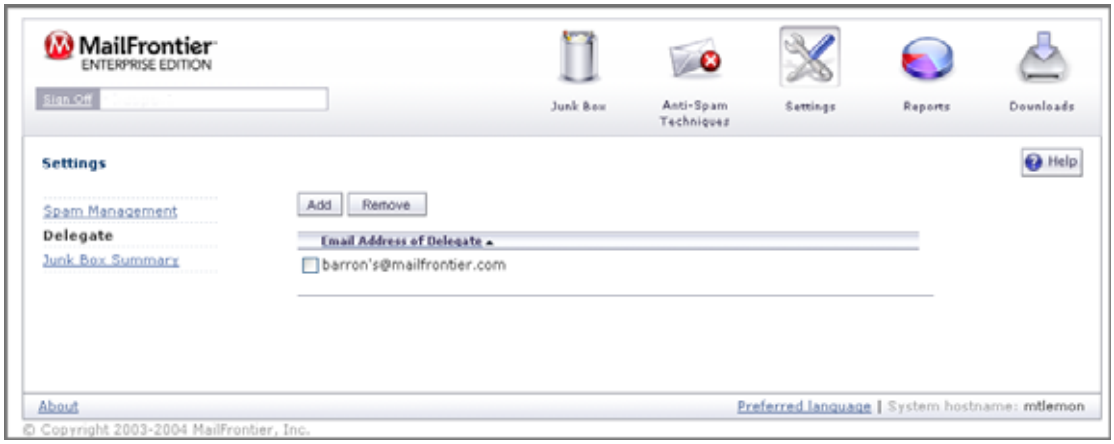
Virus Management

The virus management window gives you the option to manage virus and likely virus settings at a group level. Just like spam management options, it allows to you deal with viruses and likely viruses differently for different groups. However, unlike spam management options, these settings can not be altered for individual users.

Assigning Delegates

Delegates are people who have full access to your individual Junk Box. This includes the ability to change your Junk Box settings and manage the messages in your Junk Box. The most common use of delegates is for an administrative assistant to act as a delegate of the CEO of a company. The assistant frequently has access to all of the CEO's email, so the assistant now would have access to the CEO's Junk Box and Junk Box settings as well.

Figure 12.9 Assigning a Delegate

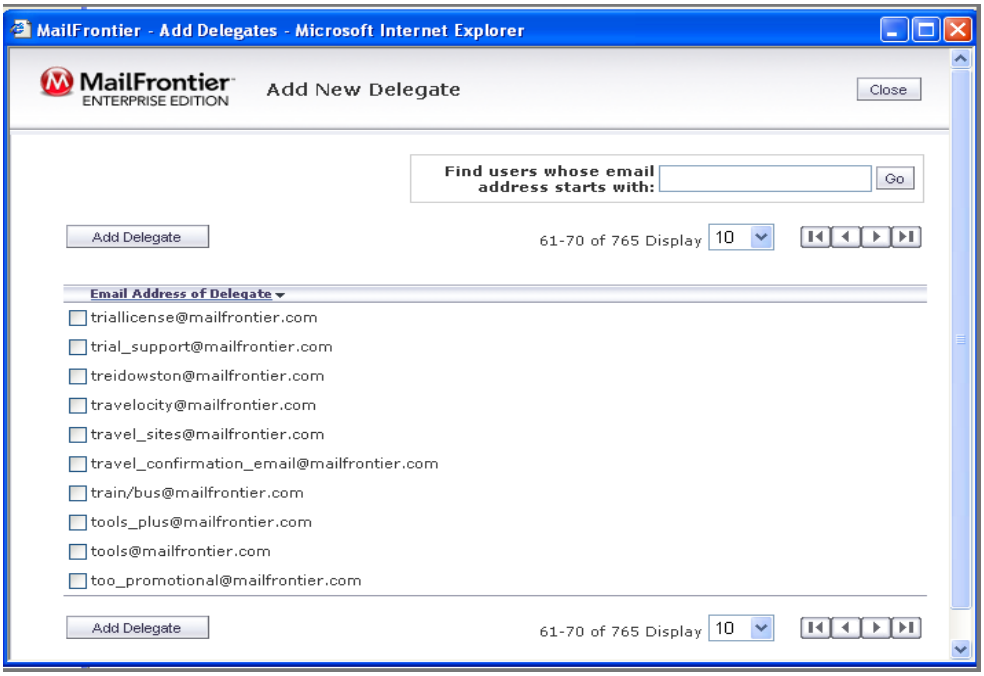


To assign a delegate to manage your Junk Box:

1. Sign in to your individual user account; click the **Sign in as any user link** at the bottom of most SonicWALL Email Security Gateway windows and sign in with your username and password.
2. Go to **Settings>Delegate**.
3. To add a delegate, click the **Add** button.

The Add New Delegate screen appears, as shown in Figure 12.10.

Figure 12.10 Adding a Delegate



4. Enter the email address of the delegate in the text box.
5. Click **Go**.

   A group of people who match the email address appear.
6. Click the checkbox adjacent to the preferred delegate.
7. Click **Add Delegate**.

To remove a delegate, click the Remove button on the Delegate window.

CHAPTER 13
Junk Box

The Junk Box allows you to review and process email messages that have been flagged as junk, virus-infected, organization policy violations, or phishing. You can unjunk or release a falsely identified message. When you or the recipient unjunks an incoming message, SonicWALL Email Security adds the sender of the message to the recipient's Allowed list and delivers the email to the recipient.

The size of the junk box can grow rapidly. By default, the messages are stored in junk box for 30 days and deleted after that. You may need to customize this setting depending on your organization's policies and storage capacity on the shared data directory for messages are stored. To change this setting, go to **Server Configuration > Default Message Management > Store in Junk Box and delete after** and choose a value between 1 and 180 days.

Messages in junk box can be quickly sorted and viewed by threat types. Messages that contain definite spam, phishing, and viruses have red asterisks (*****) adjacent to them. Messages that contain likely spam, phishing, and viruses do not have any marks, as shown in Table 1, "Message Threat Type," on page 156.

Table 1 Message Threat Type

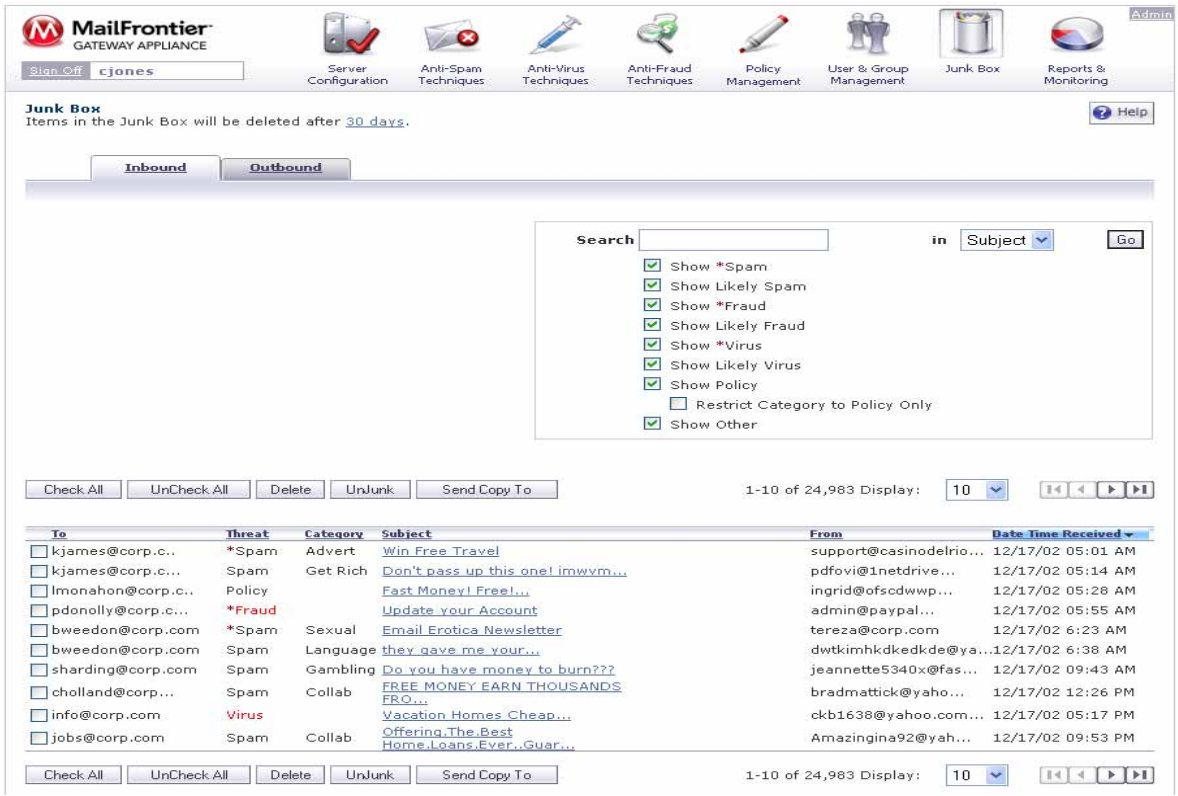
Type of Message	Display
Spam (definite)	*Spam
Likely Spam	Spam
Phishing (definite)	*Phishing
Likely Phishing	Phishing
Virus (definite)	*Virus
Likely Virus	Virus

There are two junk box views - normal mode and detailed search mode. When the size of all the messages in the junk box exceed 5MB, the application automatically switches from normal mode to detailed search mode. This size can be configured on the **Server Configuration > Advanced** page.

Junk Box - Normal Mode

Figure 13.1 displays a corporate Junk Box in normal mode.

Figure 13.1 Junk Box - normal mode



At the top of screen, the number of days messages will be stored in junk box will be displayed. The window also displays the all the messages that have been categorized as the selected threats. You can sort the messages displayed by clicking on the various column headings.

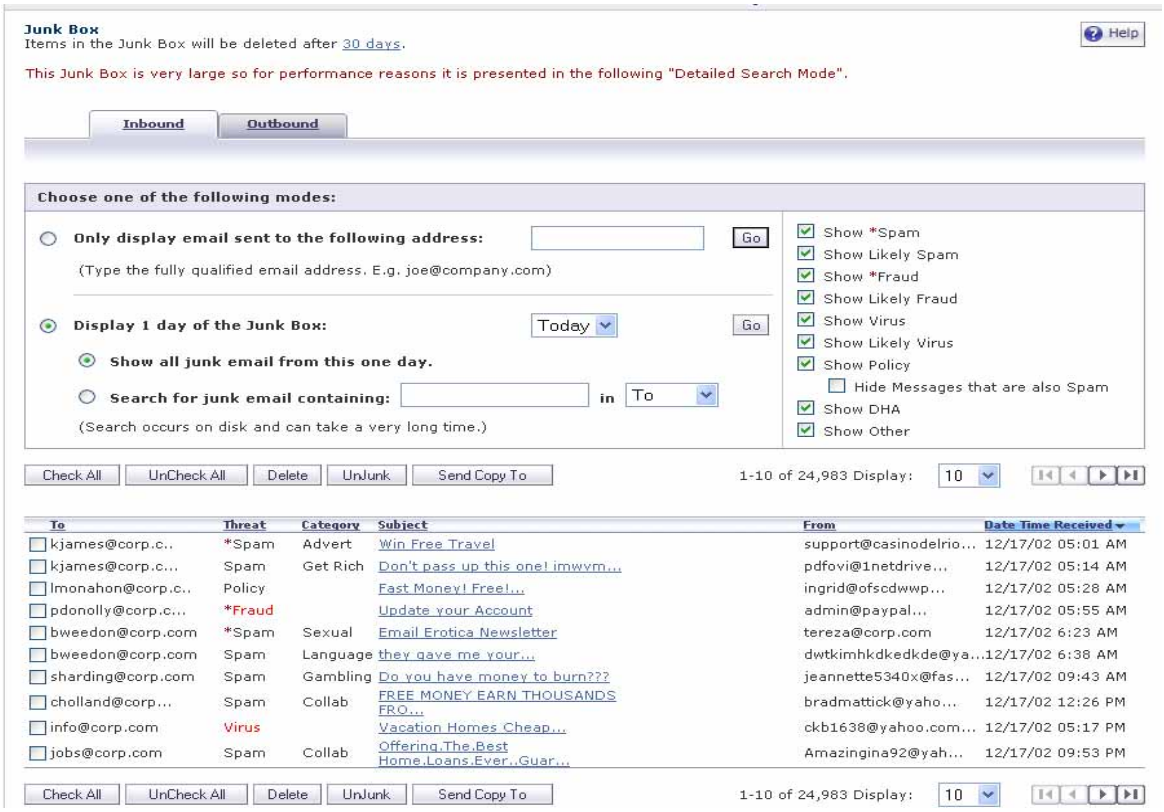
To reduce the number of messages displayed, you can

- search for messages containing specific strings in the following fields: **To**, **Subject**, or **From**. Search is not case sensitive.
- display messages from a specific day. You can enter date formats as `mm/dd/yy` or `mm/dd/yyyy`.
- search for specific threats by selecting various threat checkboxes. For example, you can limit your search to phishing messages only by selecting the *Phishing and Likely Phishing check boxes only.

Junk Box - detailed search mode

If the size of the junk box exceeds approximately 5MB in size, SonicWALL Email Security Gateway switches to the detailed search mode as shown in <Xref_Color>Figure 13.2 .

Figure 13.2 Junk Box - detailed search mode

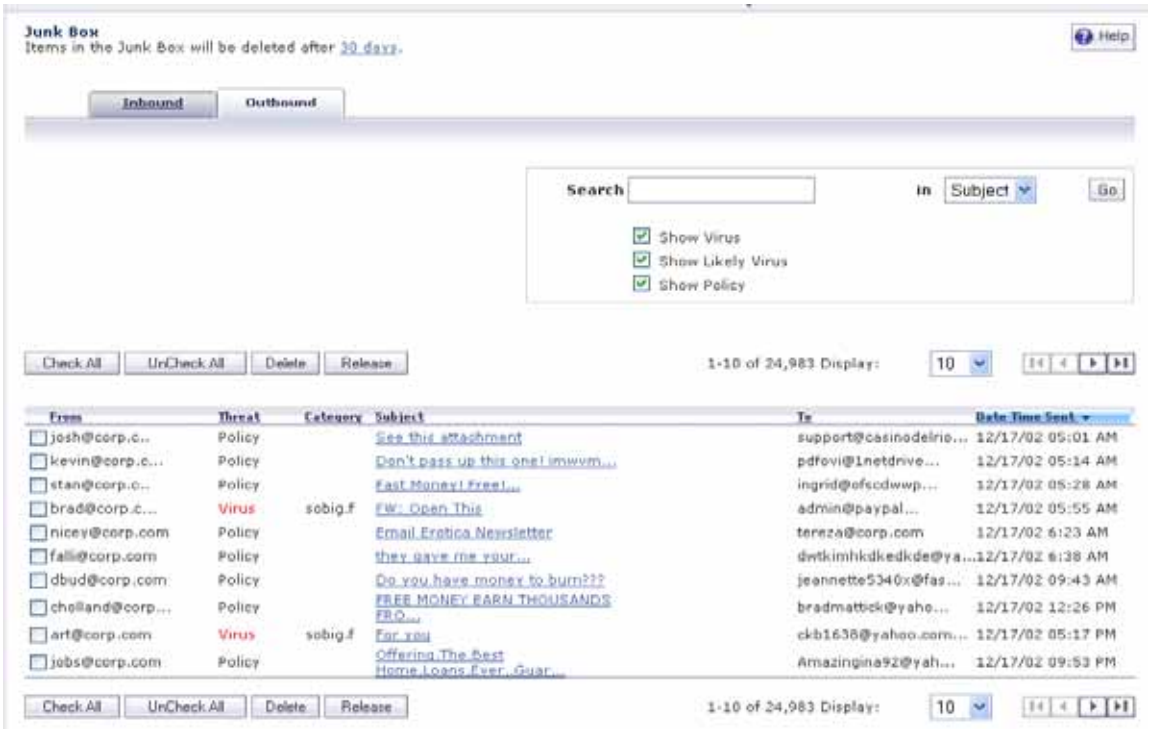


In this mode, you have additional search options to further reduce the number of messages that are displayed.

Outbound Messages Stored in Junk Box

To display the outbound messages in junk box, click on the **Outbound** tab as shown in <Xref_Color>Figure 13.3 . Outbound message management detects messages sent by users in your organization that contain viruses, likely viruses, and message that trigger policy alerts.

Figure 13.3 .Outbound Junk Box



Working with Junk Box Messages

Unjunk

This button is available only on the inbound junk box. Select **Unjunk** to forward the selected messages to the recipient and add the sender of each message to the recipient's Allowed list. Unjunking a message removes it from the Junk Box.

Send Copy To

This button is available only on the inbound junk box. Select **Send Copy To** to forward a copy of the messages (including attachments, if any) to the specified email address. The message will still remain in the Junk Box. This button will only be available to members of administrative group and only if they are allowed to view the messages in the Junk Box.

Release

This button is available only on the outbound junk box. Select **Release** to release the selected messages from the queue and forward them to the recipients. The message will be removed from the Junk Box.

Delete

Deletes the selected messages. Messages are automatically deleted after a set number of days, so there is no need to do this on a regular basis. Set the number of days messages are kept in the junk box through the **Server Configuration > Default Message Management > Number of days to store messages in the Junk Box** field.

Message Details

You can scroll through the messages and click the Subject field to view more information about the message in plain text. Depending on your user access set up, you might see the content of the messages. To control who is allowed to preview the content of messages, go to **Server Configuration > User View Setup**.

<Xref_Color>Figure 13.4 illustrates a junked message shown in text-view mode.

Figure 13.4 Text View Mode of Blocked Message

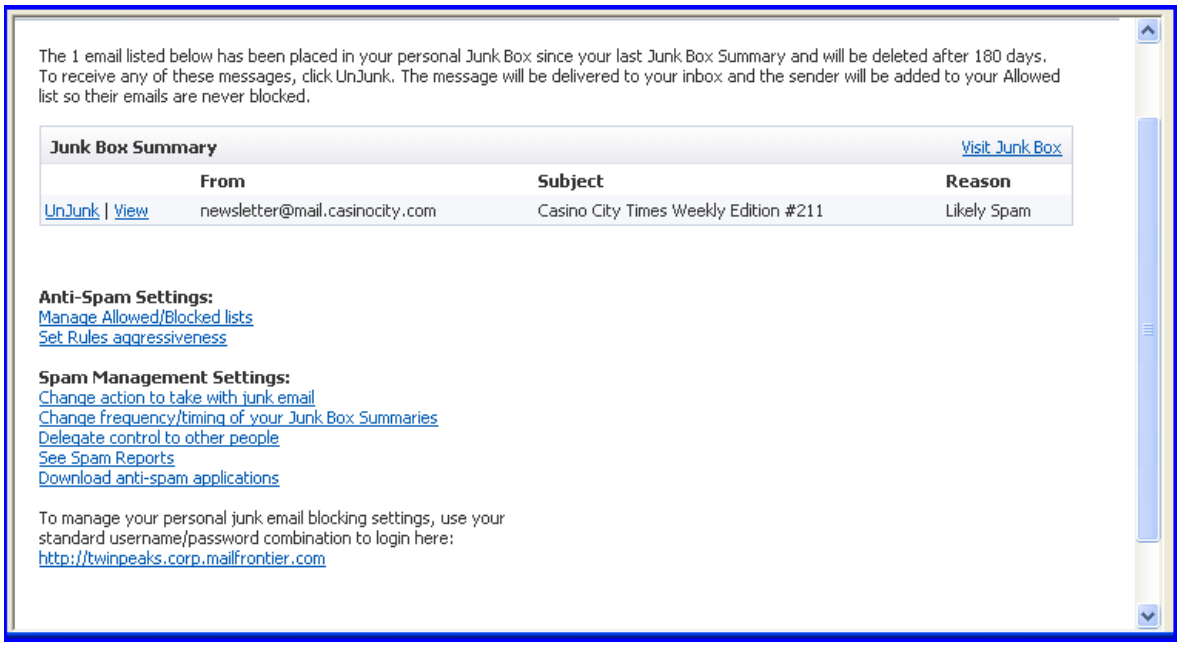
Click **Raw Mode** to view the header information as well as the message, as shown in <Xref_Color>Figure 13.5 .

Figure 13.5 Raw Mode Header and Message Details

Managing Junk Summaries

Both administrators and users receive Junk Box summaries listing the incoming email that SonicWALL Email Security Gateway has classified as junk. From these email messages, users can choose to view or unjunk an email if the administrator has configured these permissions. Figure 13.6 displays the Junk Box summary.

Figure 13.6 Junk Box Summary



From the Junk Box Summary window, users can determine the language, frequency, content, and format of Junk Box summaries.

To configure Junk Box Summaries:

1. Select the timing and frequency for email summaries.
2. Select the language for Junk Box summaries from the **Language of summary email**: list, as shown in Figure 13.7.

Figure 13.7 Languages for Junk Box Summaries

CHAPTER 14

Troubleshooting SonicWALL Email Security Gateway

This chapter describes how to troubleshoot problems that might occur with SonicWALL Email Security Gateway. It also includes alert messages and instructions for modifying alert messages.

In the sections below <MailFrontierEG> refers to the install location for SonicWALL Email Security Gateway.

In the sections below <MailFrontierDATA> refers to the location of the data directory for SonicWALL Email Security Gateway.

Problems with Control Center, Remote Analyzers, and Mail Servers

Mail is Not Delivered

Symptom:

Mail is not being delivered to the destination server, and/or mail is queuing up.

Possible Causes:

A Remote Analyzer and downstream mail server are not communicating.

Recommended Action:

Test the SMTP (Simple Mail Transfer Protocol) server to determine if it is working, type the following telnet command at the DOS prompt or shell:

```
telnet (server name) (port number)
```

If the SMTP server is working, the server responds and sends a message back. To exit this Telnet session, type:

```
quit
```

If the SMTP server is not causing the problem, follow these steps:

1. Using an Internet mail account or some other external mail server, send a good (non-spam) email to yourself at your company email ID to see if it goes through. (Do this to ensure the message goes through the SonicWALL Email Security Gateway).

   If the message goes through, you do not have a problem.

   If the message does not go through, telnet to the SonicWALL Email Security Gateway server on Port 25.
2. If you cannot connect, either the server is not turned on or you have an internal network problem outside of the SonicWALL Email Security Gateway. Contact your Network System Administrator.
3. If you can connect, and the window banner displays “Microsoft”, go to Step 4. If the window banner displays “SonicWALL Email Security,” ensure you can connect to the destination server from the SonicWALL Email Security Gateway server by doing the following:
   - From the SonicWALL Email Security Gateway server, telnet to the destination server.
   - If you cannot connect, contact your Network System Administrator.
   - If you can connect, call SonicWALL Email Security Support.
4. If the window banner includes **Microsoft**, disable Microsoft’s SMTP server as follows:
   - Go to **Control Pane > Administrative Tools>Services**.
   - Select **Simple Mail Transfer Protocol,** and open **Properties** by right-clicking the mouse. Select **Disable.**
   - Go to **Services**, and select **MlfASG Gateway**. Right click to select **Restart**, or select **Restart** from the **Action** menu.

No Spam Arrives

Symptoms:

This symptom only occurs in Split architecture. Based on your company’s history of the amount of spam messages received over a certain time period, there is a longer time than normal since your users have received spam and no new junk messages are being stored in the Control Center, although the Quarantine function is turned on.

Possible Causes:

- Messages are being queued on the Remote Analyzer and backing up because they are not being sent.
- There is a connectivity problem between the Control Center and the Remote Analyzer.

Recommended Action:

1. Go to the <MailFrontierDATA>`\Quarantine` directory.
2. Find the file with the most recent date followed by the name of the Remote Analyzer.

Based on this file date or the time of the last entry in the file, if users should have received spam by now, restart SonicWALL Email Security Gateway service as follows:

1. Go to **Control Panel>Administrative Tools>Services**.
2. Select **MlfASG Gateway**.
3. Select **Restart** from the **Action** menu.

Control Center Updates Ineffective

Symptoms:

Control Center updates are not taking effect. You updated settings from the Control Center for the Remote Analyzer, but they are not taking effect.

Possible Causes:

Connectivity problems between the Remote Analyzer and Control Center.

Recommended Action:

1. Look at your most recent Replicator Log for the Control Center located in your <`MailFrontierEG>/Logs` directory, for example: `rpl.10132003195002.`
2. If `QUEUEING` is showing in the **Action** field, ensure that the Control Center can communicate to the Remote Analyzer by testing connectivity as follows:
   - Go to **Server Configuration > Network Architecture**, and click the **Test Connectivity** button from the Control Center.
   - If connectivity to the Control Center fails, at the DOS prompt from the Control Center, type:

   `ping (`*`Remote Analyzer name`*`)`
3. If you cannot connect to the Control Center, check that the server is turned on. If not, see your Network System Administrator.
4. If connectivity is successful, restart the Tomcat service on the Remote Analyzer.
5. Restart the SonicWALL Email Security Gateway from the Control Center. You must restart both SonicWALL Email Security Gateway and Tomcat.

To restart Tomcat:

1. Go to **Control Panel>Administrative Tools>Services**.
2. Select **Apache Tomcat 4.1**.
3. Select **Restart** from the **Action** menu.

To restart the SonicWALL Email Security Gateway:

1. Go to **Control Panel>Administrative Tools>Services**.
2. Select **MlfASG Gateway**.
3. Select **Restart** from the **Action** menu.

Reports have no data

Symptoms:

Reports suddenly lost all reports data.

Possible Causes:

You changed the system host name.

Recommended Action:

1. Go to the <`MailFrontierEG>/reportdb` directory.
2. Rename the directory with the old host name to the new host name.
3. Restart SonicWALL Email Security Gateway.

Problems with Configuring SSL and LDAP Settings in the SonicWALL Email Security Gateway

Could Not Find Trusted Certificate

Symptoms:

SonicWALL Email Security displays a `Could not find trusted certificate error` when testing the LDAP login on the **Server Configuration > LDAP Configuration** page.

Possible Cause:

The SSL Certificate that the LDAP server provided is not trusted. The signer of the SSL certificate does not have a Certification Authority Certificate installed in the Java Runtime Environment's cacerts keystore.

Recommended Action:

Install a Certification Authority Certificate in the Java Runtime Environment's cacerts keystore.
See Importing and Installing the LDAP Server Certificate in "Secure Socket Layer" on page 183.

If you are using Windows and have a `%JAVA_HOME%\jre\lib\security\jssecacerts` file, ensure that the LDAP server's SSL certificate and/or its Certification Authority's certificate is installed there.

Note: If a `jssecacerts` file is present, the `cacerts` file is ignored.

Could Not Connect to Specified Host or Port

Symptoms: SonicWALL Email Security displays the `Could not connect to specified host or port` message when testing for LDAP login on the LDAP Configuration window.

Possible Causes:

- The TCP connection to the LDAP server failed to either find the specified server, or could not connect to the specified port.
- The LDAP server might not be correctly configured for SSL on the correct port.

Recommended Action:

Fully specify the LDAP server's hostname on the **Server Configuration>LDAP Configuration** window (for example, `ldapserver.int.xyzcompany.com`).

If this does not solve the problem, verify on the server that the specified port has a socket listening by using the `netstat –a –n` command. If the socket is not listening, the LDAP server is not configured properly for SSL.

SonicWALL Email Security Gateway Server Alert Messages

Below are some common alert messages that SonicWALL Email Security Gateway server can send to the email addresses specified in the monitoring configuration window. See "Modifying Alert Messages" on page 167 for instructions on how to disable most alerts.

Machine_name.domain 25 Connect Failed [date] [timestamp]

This alert indicates your `MlfASG Gateway` service is not running, or the monitoring test that attempts to connect to your downstream server has failed.

These alerts are sent every 5 minutes until the issue is resolved. You might experience one of these alerts if your server is busy (peak mail flow, directory harvest attack, and others). Verify that your downstream server is accessible and your MlfASG Gateway service is running. However, you might receive one of these alerts occasionally, when there is no problem in your mail flow or with the SonicWALL Email Security Gateway Server.

Machine_name.domain Thumbprint Service is Down [timestamp]

This alert indicates your MlfASG Updater service is not running.
The recommended action is to start the MlfASG Updater service in the service panel.
Monitoring is controlled by the "`thumbupdateproc`" tag in monitorconf.xml

Machine_name.domain Thumbprint file is stale [timestamp]

This alert indicates the SonicWALL Email Security collaborative database has not been updated recently. To maintain effectiveness it is important to have this database updated frequently.

This alert might also indicate a problem with accessing the collaborative database. Please confirm that the database does not have any write-permission restrictions.

The collaborative database file name is
`<MailFrontierEG>\PluginDefault\collab\thumprint.db`

If you have received multiple alerts and write permissions have been ruled out as a possible cause, verify that the server in question has port 80 access to the internet. Test internet access to port 80:

1. Click the **Server Configuration** > **Updates**.
2. Click the **Test Connectivity to** SonicWALL Email Security button.

If the in-product test to the SonicWALL Email Security data center is successful, contact SonicWALL Email Security Technical Support for further assistance, as this might indicate a problem with downloading updates from the SonicWALL Email Security hosted datacenter to your server.

Monitoring is controlled by the `replicatorproc` tag in `monitorconf.xml.`

Machine_name.domain SonicWALL Email Security Gateway LDAP Warning: usermap is stale. [timestamp]

This message indicates your `Usermap.xml` file has not been updated recently. By default, `Usermap.xml` is updated once an hour. You can configure the update period in the **Advanced** page; however, SonicWALL Email Security recommends that you use the default setting.

`Usermap.xml` is created by querying your LDAP server for user accounts. This is an important file to keep updated for several reasons, but most importantly if you are using DHA—if this file is not updated after adding new users to LDAP, the email sent to this user will be captured by DHA.

Monitoring is controlled by the `collabdb` tag in `monitorconf.xml.`

Machine_name.domain Replicator Service is Down [timestamp]

This message indicates your replication service is not running.

The recommend action is to start the MlfASG Replicator service in the service panel. The monitoring is controlled by the "`file_replication`" tag in `monitorconf.xml.`

Machine_name.domain:25 Out of disk space [date] [timestamp]
This message indicates the hard disk drive that your data resides on is running out of disk space. By default, an alert is sent if there is less than 10Mbs of free space.

You can change the amount of space remaining that will cause an alert by editing `server.xml`.

To edit, open server.xml with any text editor. By default server.xml is located in the data directory, `<MailFrontierEG>\data\server.xml.`

Add the line identified in bold text below:

```
<config writeversion="2">
      <quarantine free="1 G"/>
      <trace level="info"/>
```

This example changes the disk space to 1 Gbyte. If remaining disk space falls below 1 Gbyte, an alert is sent. Once you add this line, save changes and restart the `MlfASG` services.

If you want to change the setting to Megabytes, use "M" instead of "G; for example:
`<quarantine free="5 M"/>` sends an alert if less than 5 Mbytes of free space is available.

Cannot Read Data Store

The configuration data store is inaccessible, for example, network fileshare is down

Out of Sockets

Out of local socket resources.

Connect Failed: the SonicWALL Email Security SMTP server appears to be down

Internet cannot connect.

No Banner

The SonicWALL Email Security SMTP server is up, but no SMTP banner appears on the window.

Not MLF

The SMTP banner was received, but it is not a SonicWALL Email Security server.

Out of disk space

The quarantined mail area is full.

Cannot communicate with your LDAP Server any more

The SonicWALL Email Security Gateway is unable to fetch a new user map from LDAP.

Modifying Alert Messages

To turn off or modify monitoring alerts for the thumbprint service, thumbprint file, `usermap.xml`, and replicator service, you will need to edit the `monitorconf.xml` file located in `<MailFrontierEG>`.

To edit `monitorconf.xml`, open the file using a text editor, such as Notepad. The file should look similar to the one below.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
      <config>
      <collabdb enabled="true" alert_interval="30"/> affects
      Machine_name.domain Thumbprint file is stale [timestamp]
      <file_replication enabled="true" alert_interval="30"/> affects
      Machine_name.domain SonicWALL Email Security Gateway LDAP Warning:
      usermap is stale. [timestamp]
      <replicatorproc enabled="true" alert_interval="5"/> affects
      Machine_name.domain Replicator Service is Down [timestamp]
      <thumbupdateproc enabled="true" alert_interval="5"/> affects
      Machine_name.domain Thumbprint Service is Down [timestamp]
      </config>
```

Change the `enabled=″true″` section of the line to `enabled=″false`" for any alert you want to stop receiving. Once you make the change, save your changes.

SonicWALL Email Security strongly recommends keeping alerts active.

Note The thumbprint service, thumbprint file, `usermap.xml` and replicator service monitoring intervals can not be sent more frequently than once every 5 minutes.

Appendix A

LDAP

This Appendix details specific LDAP configuration settings for popular mail server environments, such as Microsoft Exchange and Lotus Domino.

The Configuration Parameters below refer to the Table 1, “Installation Checklist,” on page 25 and Table 2, “Installation Checklist,” on page 32.

Configuring Microsoft Active Directory

Microsoft Exchange 2000 uses Microsoft Active Directory (AD) for user login, email address and email aliases.

LDAP Server

Server Name (configuration parameter M): In this field, enter the IP address or DNS name of one of your Active Directory servers. Different Active Directory servers in the same domain tree replicate their information amongst each other. Any AD server should have all the data required by SonicWALL Email Security Gateway. If you have more than one tree then specify the Global Catalog.

Port (configuration parameter N): The default LDAP port is 389. Unless your Active Directory server has been configured for another port (highly unlikely), use the default port number. If you are specifying a Global Catalog, use port 3268.

Login Information

Anonymous Bind: Do *not* use this setting with Active Directory. Active Directory servers can be configured to allow for anonymous access. However, by default, Active Directory the anonymous access setting does not provide enough directory information for SonicWALL Email Security Gateway.

Login (configuration parameter O): Specify a user login that has access to browse the Active Directory and has site-level permissions to add and delete people in the directory. By default, Active Directory allows all users to browse the directory. However, if your Active Directory does not allow this, use a login name with administrative privileges.

CAUTION: This user *must* have site-level permissions; otherwise, mail will be halted.

The proper format for the login name is:

NT-DOMAIN\USERNAME

For example, if your NT Domain is MYCORP, the syntax for the login name is: MYCORP\Administrator. If you do not know your NT-DOMAIN name, see “Windows Domains ” on page 171.

LDAP Query

Directory Node to Search (configuration parameter Q):
Specify your top level Active Directory domain using LDAP syntax. For example, if your top level Active Directory domain name is *mycorp.com*, the LDAP syntax is:

```
dc=mycorp,dc=com.
```

Note If you have more than one Directory Node that you intend to use, you can separate multiple nodes by separating them with an ampersand (&). For example:

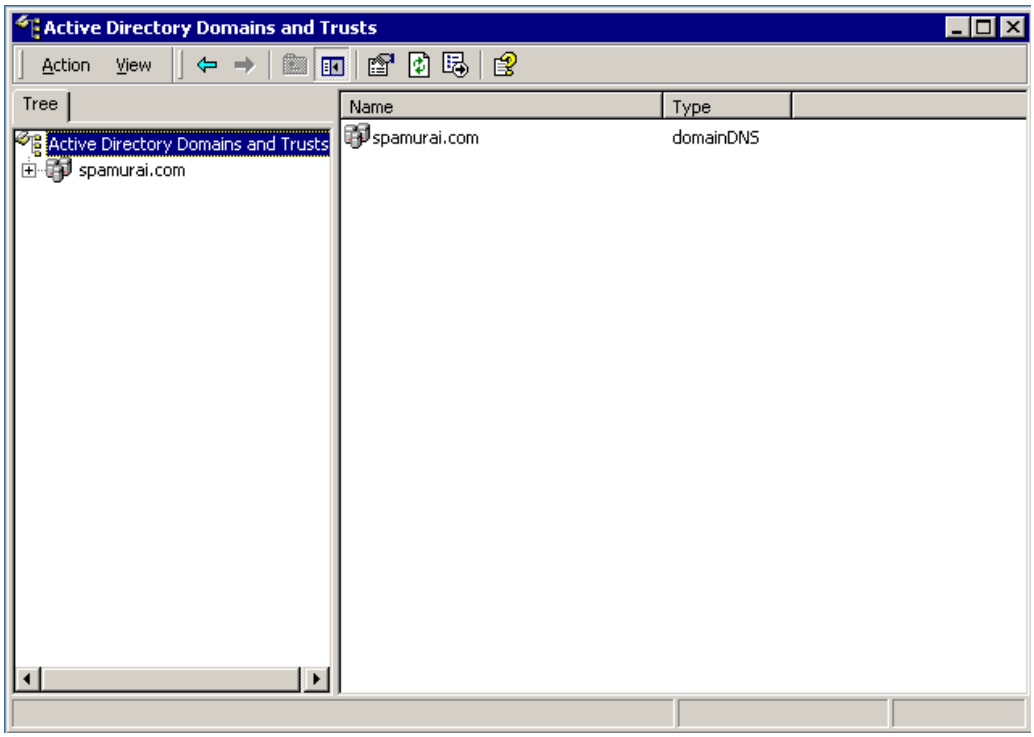
```
DC=sales,DC=xyz,DC=com&DC=engr,DC=xyz,DC=com
```

To discover your Active Directory domain(s), from an Active Directory server go to **Start->Programs->Administrative Tools->Active Directory Domains and Trusts.**

All your Active Directory domains are listed in this window, as shown in Figure A.1, “Active Directory Domains and Trusts,” on page 170. In the example, `spamurus.mailfrontier.com` is the Active Directory Domain name. The LDAP syntax is:

```
dc=spamurus,dc=mailfrontier,dc=com
```

Figure A.1 Active Directory Domains and Trusts



Filter: The Active Directory default filter for getting the users is the following:

```
(&(|(objectClass=group)(objectClass=person))(mail=*)(sAMAccountName=*))
```

This filter provides SonicWALL Email Security Gateway with all the necessary information for users and distribution lists. The default filter for getting groups is:

```
(objectClass=group)
```

User Login Name Attribute: The Active Directory default user login attribute is the following:

```
sAMAccountName
```

Email Alias Attribute: The Active Directory default email alias attributes are:

```
proxyAddresses, legacyExchangeDN
```

Group Name Attribute: The Active Directory default group name attribute is:

```
cn
```

Group Member Attribute: The Active Directory default attribute that contains the members of a group is:

```
member
```

Attributes indicate groups that users belong to: The Active Directory default attribute that contains the groups a user belong to is:

```
memberOf
```

Windows Domains

User authentication requires the use of Windows NT/NetBIOS Domain Names. Just like the Windows 2000 login screen, the SonicWALL Email Security Gateway login screen has three elements, the User name, Password and Domain. SonicWALL Email Security Gateway uses a convention that should be familiar to users. Enter each of your Windows Domains into the Domain List. (configuration parameter R)

To discover your **Windows Domain Name**, enter these commands from an Active Directory server:

1. Go to **Start > Programs > Administrative Tools > Active Directory Domains and Trusts.**
2. Select one of the **Active Directory** domains listed on the left side of the screen.
3. Click **Action > Properties** from the menu.

Figure A.2 Domain Properties Page Showing the Windows Domain Name

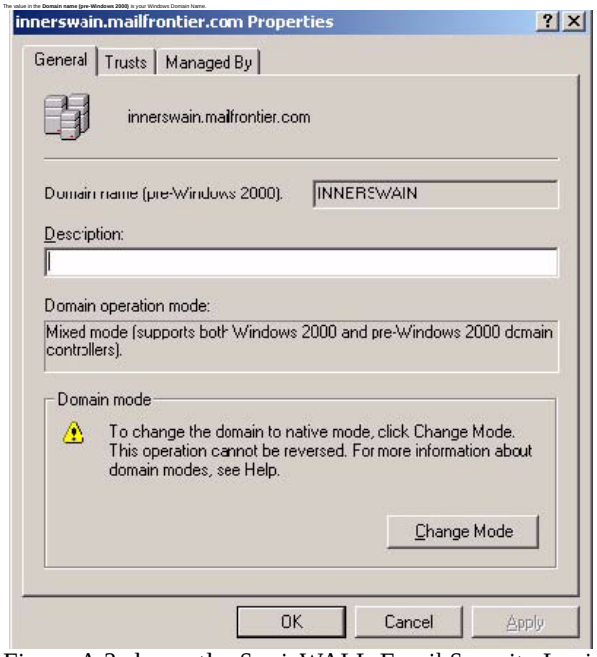
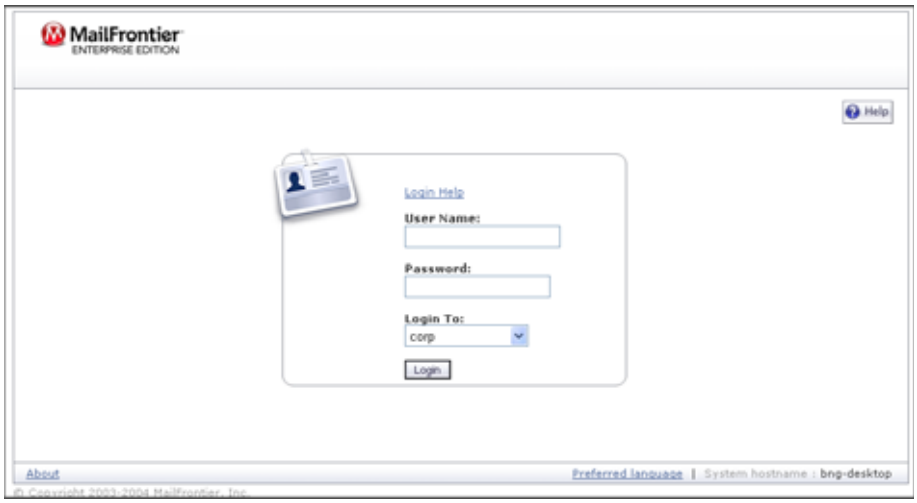


Figure A.3 shows the SonicWALL Email Security Login Window with the Windows Domain.

Figure A.3 SonicWALL Email Security Login Window with Windows Domain



Login to SonicWALL Email Security Gateway

To login into SonicWALL Email Security Gateway, users enter their Active Directory username and their password and selects the Windows Domain to which they belong. This list of domains is populated by the entries you made in **Server Configuration > LDAP Configuration**. If the password matches the Active Directory password, the user is logged in.

Multiple Domain Trees in One Forest

If you have more than one domain tree in one Active Directory forest, for example, `mycorp.com` and `mycorp.org`, you must make some minor changes to include users from all the domain trees:

1. Under **LDAP Server**, choose a **Global Catalog server** instead of a regular Active Directory Domain Controller.
2. Under **Port**, specify the **Global Catalog port:** 3268.
3. Under Directory Node, specify *all* the domain trees, separated by an ampersand (&). For example:

   `DC=mycorp,DC=com&DC=mycorp,DC=org`

Configuring Microsoft Exchange 5.5 LDAP

The Microsoft Exchange 5.5 LDAP service allows SonicWALL Email Security Gateway access to user login, email address and email aliases.

LDAP Server

Server Name (configuration parameter M): In this field, enter the IP address or DNS name of one of your Exchange 5.5 servers. Different Exchange servers replicate their information amongst each other. Any Exchange server should have all the data required by the SonicWALL Email Security Gateway, provided they are all within the same Exchange Organization.

Port (configuration parameter N): The default LDAP port is 389. Unless your Exchange server has been configured for another port (highly unlikely), use the default port number.

Note

By default, the LDAP service for Microsoft Exchange 5.5 is turned on. If your LDAP service is not enabled, launch Exchange Administrator, go to Configuration > Protocols > LDAP, and click the Enable check box.

Login Information

Anonymous Bind: Do not use this setting with Microsoft Exchange 5.5. Exchange 5.5 servers can be configured to allow for anonymous access. However, by default, the anonymous access setting does not provide enough directory information for SonicWALL Email Security Gateway.

Login (configuration parameter O): Specify a user login that has access to browse the Exchange 5.5 Directory. By default, Exchange 5.5 allows all users to browse the directory. However, if your Exchange server does not allow this, use a login name with administrative privileges.

The proper format for the login name is:

`cn=`*`Exchange username`*

For example, if your Exchange 5.5 user name is `bsmith`, the exact syntax would be: `cn=bsmith.`

LDAP Query

Directory Node To Search (configuration parameter Q).
Specify your Exchange Organization name using LDAP syntax. For example, if your Exchange Organization name is `MyCorp` the LDAP syntax is `o=MyCorp`.

NOTE: If you have more than one Directory Node that you intend to use, you can separate multiple nodes by separating them with an ampersand (**&**). For example:

```
DC=sales,DC=xyz,DC=com&DC=engr,DC=xyz,DC=com
```

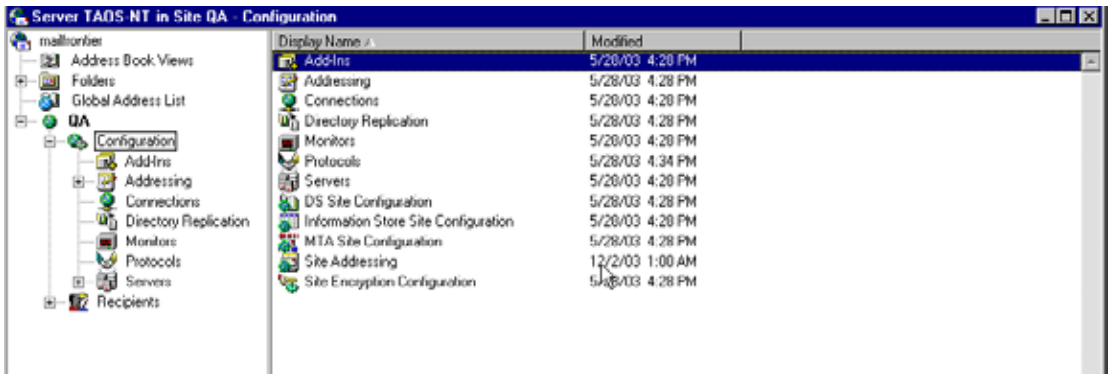
To discover your **Exchange Organization Name**, from an Exchange Server, go to **Start->Programs->Microsoft Exchange->Microsoft Exchange Administrator**. Your Microsoft Exchange Organization name is listed as the top element of the tree visible on the left-hand side of the Administrator tool.

In the example, the Exchange Organization name is SonicWALL Email Security, Inc. The LDAP syntax is:

```
o="MailFrontier, Inc."
```

NOTE: Quotation marks (“ “) are required if your Exchange Organization name has spaces, like the example shown.

Figure A.4 Microsoft Exchange Administrator



Filter: The Exchange 5.5 default filter is the following:

```
(&(|(objectClass=groupOfNames)(objectClass=person))(mail=*)(uid=*))
```

This filter will provide SonicWALL Email Security Gateway with all the necessary information for users and distribution lists. The default filter for getting groups is:

```
(objectClass=groupOfNames)
```

User Login Name Attribute: The Exchange 5.5 default user login attribute is the following:

```
uid
```

Email Alias Attributes: The Exchange 5.5 default email alias attributes are:

```
distinguishedName, otherMailbox, rfc822Mailbox
```

Group Name Attribute: The Exchange 5.5 default group name attribute is:

```
cn
```

Group Member Attribute: The Exchange 5.5 default attribute that contains the members of a group is:

```
member
```

Attribute to indicate groups that users belong to: The Exchange 5.5 default attribute that contains the groups a user belong to is:

```
memberOf
```

Windows Domains (configuration parameter R)

User authentication requires the use of Windows NT/NetBIOS Domain Names. Just like the Windows 2000 login screen, the SonicWALL Email Security Gateway login screen has three elements, the User name, Password and Domain. SonicWALL Email Security Gateway uses a convention that should be familiar to users. Enter each of your Windows Domains into the Domain List.

Login to SonicWALL Email Security Gateway

To login into SonicWALL Email Security Gateway, a user enters their Exchange 5.5 username and their password and then selects the Windows Domain to which they belong. This list of domains is populated by the entries you made in **Server Configuration > LDAP Configuration.** If the password matches the Exchange 5.5 password, the user is logged in.

Configuring Lotus Domino R5 LDAP

The Lotus Domino R5 LDAP service allows SonicWALL Email Security Gateway access to user login, email address and email aliases.

NOTE: The SonicWALL Email Security Gateway queries your LDAP server for all the email addresses under the directory node you specified. By default, your Lotus server is configured to return all the entries requested; however, you may have changed the configuration to limit the number of entries returned per query. If the LDAP Configuration page warns you about not able to get the complete list of users, or if you notice users missing from the User Management page, change your Domino Server LDAP Configuration to increase the maximum limit.

LDAP Server

Server Name (configuration parameter M): In this field, enter the IP address or DNS name of one of your Lotus Domino servers. Different Domino servers replicate their information amongst each other. Any Domino server should have all the data required by the SonicWALL Email Security Gateway.

Port (configuration parameter N): The default LDAP port is 389. Unless your Domino server has been configured for another port (highly unlikely), use the default port number.

NOTE: By default, the LDAP service for Lotus Domino R5 is turned off. If your LDAP service is not enabled, run the LDAP Server task from the **Domino Administrator->Server** console. For more information about the LDAP Server, please refer to the Lotus Domino R5 documentation.

Login Information

Anonymous Bind: Do not use this setting with Lotus Domino R5. Domino R5 servers can be configured to allow for anonymous access. However, by default, the anonymous access setting does not provide enough directory information for SonicWALL Email Security Gateway.

Login (configuration parameter O): Specify a user login that has access to browse the Domino Directory. By default, Domino allows all users to browse the directory. However, if your Domino server does not allow this, use a login name with administrative privileges.

```
shortname
```

For example, if your Domino short name is `bsmith`, the exact syntax would be `bsmith.`

NOTE: To successfully connect to the Domino Server, your Domino ID must have an Internet Password.

LDAP Query

Directory Node to Search (configuration parameter Q):
Specify your Lotus Domino Domain name using LDAP syntax. For example, if your Lotus Domino Domain name is *MyCorp*, the LDAP syntax is

```
o=MyCorp.
```

NOTE: If you intend to use more than one Directory Node, you can separate multiple nodes by separating them with an ampersand (&), for example:

```
DC=sales,DC=xyz,DC=com&DC=engr,DC=xyz,DC=com
```

Filter: The Lotus Domino R5 default filter can be configured in two ways, depending on whether your users will want to connect via their short name (that is, `bsmith`) or common name (that is, `Bob Smith`). If you would like to use the short name, use the following filter:

```
(&(objectClass=person)(mail=*)(shortname=*))
```

If you would like to use the common name, use this filter:

```
(&(objectClass=person)(mail=*)(cn=*))
```

Either of these filters will provide SonicWALL Email Security Gateway with all the necessary information for users. The default filter for getting groups is:

```
(objectClass=dominoGroup)
```

User Login Name Attribute: If you would like the users to connect via their short name, use the following:

```
shortname
```

If you would like the users to connect via their common name, use the following:

```
cn
```

Email Alias Attributes: The Lotus Domino default email alias attribute is:

```
shortname
```

Note

Lotus Domino R5 allows SMTP aliases to be defined in the short name or user name fields. However, SonicWALL Email Security Gateway only supports SMTP aliases defined in the short name field. The user name is not exposed via LDAP.

Group Name Attribute: The Lotus Domino default group name attribute is:

```
cn
```

Group Member Attribute: The Lotus Domino default attribute that contains the members of a group is:

```
member
```

Attribute to indicate groups that users belong to: There is no Lotus Domino default for this attribute

Windows Domains (configuration parameter R) Windows Domains are not needed for Lotus Domino R5.

Login to SonicWALL Email Security Gateway

To login into SonicWALL Email Security Gateway, a user enters either their Lotus Domino short name or common name, depending on how you configured LDAP, and their password. If the password matches the Lotus Domino internet password, they are allowed to login.

Note SonicWALL Email Security Gateway depends on a person document having an internet password defined. If an Internet password is not defined, SonicWALL Email Security Gateway will not be able to authenticate the password provided by the user.

Configuring SunOne/iPlanet Messaging Server

SunOne/iPlanet Messaging Server uses SunOne/iPlanet Directory for user login, email address and email aliases.

LDAP Server

Server Name (configuration parameter M): In this field, enter the IP address or DNS name of your SunOne/iPlanet Directory server.

Port (configuration parameter N): The default LDAP port is 389. Unless your Domino server has been configured for another port (highly unlikely), use the default port number.

Login Information

Anonymous Bind: Do not use this setting with SunOne/iPlanet Directory Server. SunOne/iPlanet Directory servers can be configured to allow for anonymous access. However, by default, the anonymous access setting does not provide enough directory information for SonicWALL Email Security Gateway.

Login (configuration parameter O): Specify a user login that has access to browse the SunOne/iPlanet Directory. By default, SunOne/iPlanet allows all users to browse the directory. However, if your SunOne/iPlanet server does not allow this, use a login name with administrative privileges.

The easiest ID to use is the Directory Manager. If you choose to use Directory Manager, use the following syntax:

```
cn=Directory Manager
```

Note You can use a specific user for binding purposes. However, you must know the full distinguished name for this user. For example:

```
uid=joe,ou=People,o=mycorp.com,o=internet
```

LDAP Query

Directory Node to Search (configuration parameter Q):

Specify your SunOne/iPlanet Messaging server User Directory Subtree using LDAP syntax. An example of a root level node is:

```
"o=mycorp, o=internet"
```

NOTE: If you have more than one Directory Node that you intend to use, you can separate multiple nodes by separating them with an ampersand (&); for example:

```
DC=sales,DC=xyz,DC=com&DC=engr,DC=xyz,DC=com
```

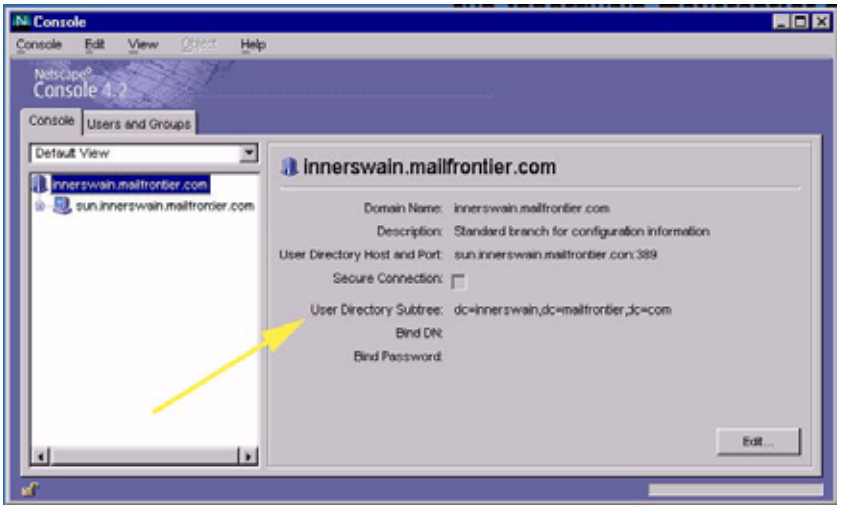
To discover your SunOne/iPlanet root node, start the SunOne/iPlanet Console.

NOTE: This is sometimes called the Netscape Console.

Your User Directory Subtree is listed on the main properties screen of the Console. In the example, the SunOne/iPlanet User Directory subtree name is:

```
dc=innerswain,dc=mailfrontier,dc=com"
```

Figure A.5 SunOne/iPlanet Console



Filter: The SunOne/iPlanet default filter is as follows:

```
(&(|(objectClass=inetMailGroup)(objectClass=person))(mail=*)(cn=*))
```

This default filter will provide SonicWALL Email Security Gateway with all the necessary information for users and distribution lists. The default filter for getting groups is:

```
(|(objectClass=inetMailGroup)(objectClass=groupOfUniqueNames))
```

User Login Name Attribute: The SunOne/iPlanet default user login attribute is the following:

```
cn
```

Email Alias Attributes: The SunOne/iPlanet default email alias attribute is:

```
mailalternateaddress
```

Group Name Attribute: The SunOne/iPlanet default group name attribute is:

```
cn
```

Group Member Attribute: The SunOne/iPlanet default attribute that contains the members of a group is:

```
uniquemember
```

Attribute to indicate groups that users belong to: The SunOne/iPlanet default attribute that contains the groups a user belong to is:

```
memberOf
```

NOTE: For large organizations, the default LDAP query window might be too small to retrieve all the users. If all the users in your organization do not appear in SonicWALL Email Security Gateway, you must increase the limit.

1. Open the **SunOne/iPlanet** console.
2. Double-click the **Directory Server** icon and select **Configuration->Database**.

3. Under the **Performance** tab, increase the **Look through limit** to a large enough number.

   For example, if you have 50,000 users and distribution lists in your organization, make this number 50,000.

Windows Domains (configuration parameter R): Windows Domains are not needed for SunOne/iPlanet Directory.

Login to SonicWALL Email Security Gateway

To login into SonicWALL Email Security Gateway, users enter either their SunOne/iPlanet common name (that is, Bob Smith) and their password. If the password matches the SunOne/iPlanet Directory password, they are allowed to login.

Appendix B

SonicWALL Email Security Gateway TCP Port Utilization

The SonicWALL Email Security Gateway uses a variety of TCP ports that it uses to communicate with other network services. Each of these ports needs special attention if your organization filters TCP traffic.

Note Generally, DMZ traffic is heavily filtered by multiple firewalls. Ensure that all the inbound and outbound ports SonicWALL Email Security Gateway requires are open for SonicWALL Email Security Gateway to communicate.

Inbound TCP Traffic

SMTP (configurable port, usually 25) SonicWALL Email Security Gateway is an SMTP proxy server. It receives email to be analyzed for characteristics of spam on SMTP port 25.

HTTP (configurable port, usually 80) or HTTPS, port 443 SonicWALL Email Security Gateway hosts a Web server, HTTP port 80, which is used to administer SonicWALL Email Security Gateway's Web interface. In addition, users log in to this Web server to view their personal Junk Box and configure their anti-junk settings.

Outbound TCP Traffic

HTTP (port 80) SonicWALL Email Security Gateway server installed in your organization communicates with SonicWALL Email Security Anti-Spam Lab's data center via HTTP port 80.
SonicWALL Email Security Anti-Spam Data Center is available on the Internet.

HTTP requests are made via port 80 to the data center requesting anti-spam updates. If an update is available, the HTTP response returns it.

LDAP (configurable port, usually port 389) or LDAPS, (configurable port 636)
SonicWALL Email Security Gateway server installed in your datacenter communicates with a LDAP server inside your organization on TCP port 389 or 636.

DNS, port 53 SonicWALL Email Security Gateway needs to communicate with DNS server to look up information if it is configured to check for senders SPF records. Port 53 is the default port used for DNS queries.

SMTP (configurable port, usually 25) If SonicWALL Email Security Gateway determines an email message is not spam, it needs to be delivered to the next mail server in your SMTP mail flow. SonicWALL Email Security Gateway sends these messages via SMTP port 25

Split Configuration TCP Port Utilization

Here are some additional changes that you must make if you are running Split Architecture.

Port 2599 SMTP configurable (Remote Analyzer to Control Center, bad mail routing) SonicWALL Email Security Remote Analyzer communicates with Control Center for routing quarantine email through port 2599.

Port 80 HTTP or port 443 HTTPS configurable (Control Center to Remote Analyzer communication) Control center keeps all Remote Analyzers up to date with latest configuration information by communicating via port 80 or 443.

<Xref_Color>Figure B.1 on page 181 illustrates these ports and protocols used between components of SonicWALL Email Security Gateway and other parts of the network.

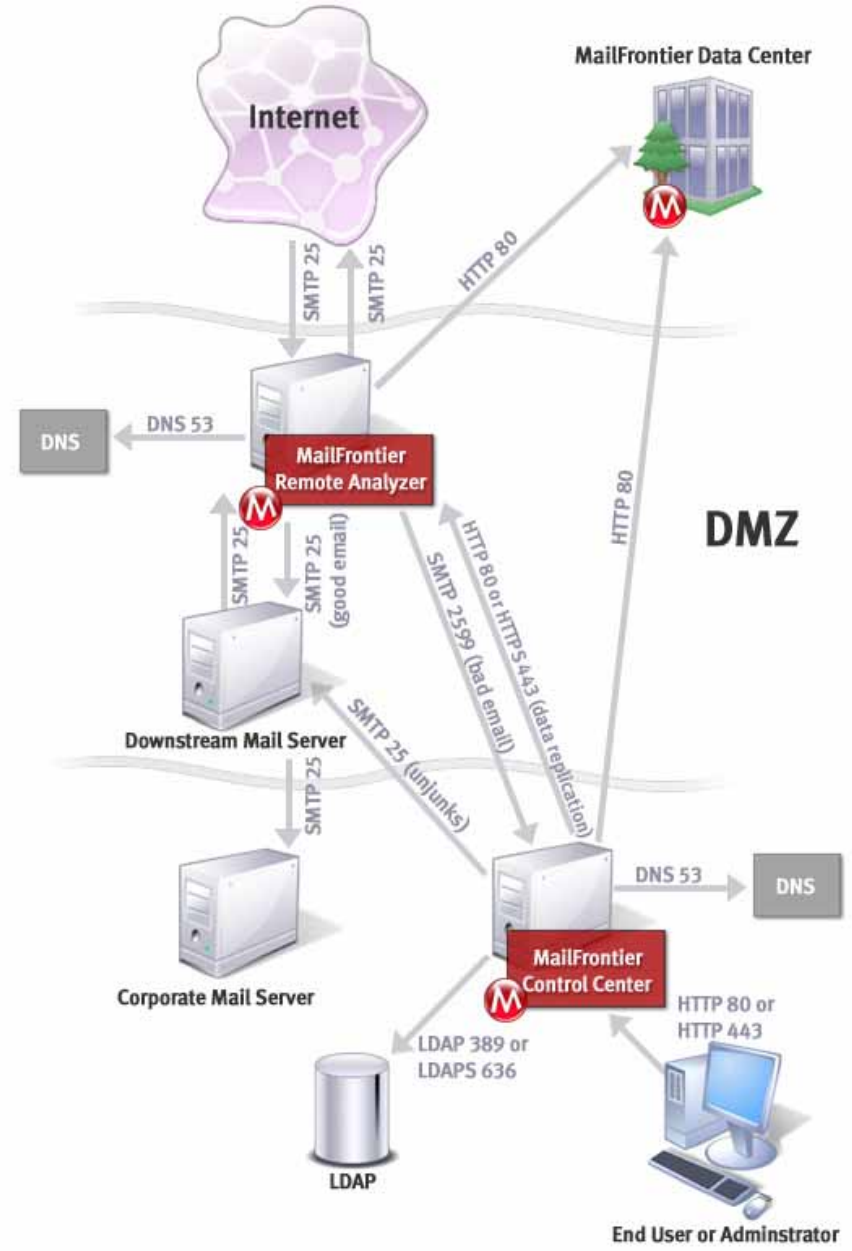


Figure B.1 Ports and Protocols used in SonicWALL Email Security Gateway Connections

Other TCP Port Usage

Port 3050 used by Firebird Database. SonicWALL Email Security Gateway uses Firebird database for reporting purposes. This database listens in on port 3050 locally. This port usage is local in the machine Firebird is running and hence no changes to the network elements (like firewall) needs to be made.

Appendix C

Secure Socket Layer

This Appendix explains how to configure a secure environment using Secure Socket Layer (SSL) between the following components:

- The LDAP server and SonicWALL Email Security Gateway's Tomcat Web server
- The Control Center and the Remote Analyzer

Overview

When a user logs into the SonicWALL Email Security Gateway, either as a System Administrator who wants to configure the system or as a user who wants to manage their Junk Box, the SonicWALL Email Security Gateway verifies via the LDAP protocol that the login (user ID and password) is valid. This communication between SonicWALL Email Security server and the LDAP server can be encrypted using SSL protocol. Also, if you configured the Split Network Architecture, you can use SSL between a Control Center and a Remote Analyzer to encrypt data between the two servers.

For general information about SSL, see the following Web sites:

http://jakarta.apache.org/tomcat/tomcat-4.0-doc/ssl-howto.html

http://java.sun.com/webservices/docs/1.0/tutorial/doc/WebAppSecurity6.html

SSL Signed Certificates and Certificate Authorities

An SSL trusted certificate is a digitally signed document authenticating the server. If the client accepts the certificate as valid, it proceeds with encrypted communication with the server. It is analogous to when you present your driver's license to an airline representative to collect your boarding pass for a flight.

The license provides assurance that you are who you say you are, and the airline representative accepts that and gives you your boarding pass. SSL certificates are signed by Certificate Authorities.

Similar to the DMV issuing driver licenses, a Certificate Authority is an organization that provides the assurance of identity. All SSL clients have a list of trusted Certificate Authorities.
SonicWALL Email Security recommends Verisign and Thawte as Certificate Authorities.

Use of Third-Party Vendors for Certificates

SonicWALL Email Security recommends you use third-party vendors Verisgn and Thawte to provide you with your certificates. If you use other third-party vendors, additional procedures might be required for the certificates to be accepted, which are not documented in this guide. See the documentation that shipped with the access to the Certificate Authority.

Setting up LDAP over SSL (LDAPS)

LDAPS between SonicWALL Email Security Gateway and the LDAP server involves three parts:

- Obtaining and importing a certificate from a certificate authority
- Configuring the LDAP server to use the certificate and accept an LDAPS connection
- Configuring SonicWALL Email Security Gateway to use an LDAPS connection

SonicWALL Email Security recommends you obtain and import your certificates from the third-party vendors Verisign or Thawte. It is easier to acquire and use third-party certificates from the system when they are from the same vendor. If you use an internal certificate server, see the section, “Generating a Self-Signed Certificate for LDAP over SSL” on page 189.

Environment Assumptions

The following instructions use Exchange 2000/Windows 2000 Server and Exchange 5.5/Windows NT 4.0 Server as examples.

Environment Assumptions for Exchange 2000 on Windows 2000 Server:

- Server #1: Windows 2000 Active Directory Domain Controller

  Service Pack 4 (previous versions of Service Pack also work)

  Internet Information Server (IIS) 5.0

  Server #2: Exchange 2000 running on a Windows 2000 member server in the same Active Directory domain as Server #1.

Environment Assumptions for Exchange 5.5 on Windows NT 4.0 Server:

- Server: NT4, Primary or Backup Domain Controller (PDC or BDC)

  Internet Information Server (IIS) 4.0

  Microsoft DNS server

  Option Pack 4

  Service Pack 6a

  Exchange 5.5

Obtaining and Importing A Certificate From A Certificate Authority (Exchange 2000/ Windows 2000)

1. Create a certificate request on the Active Directory Domain Controller.

If you do not have IIS already installed on your Active Directory Domain Controller, first create the certificate request on any IIS 5.0 server and then proceed with the steps below.

2. Go to Verisign or Thawte's Web site and follow their instructions on requesting and installing an SSL certificate.

Verisign:

To acquire the certificate:

`http://www.verisign.com/products/site/secure/index.html`

To generate the Customer Service Request and install the certificate:

`http://www.verisign.com/support/csr/index.html`

IIS 5.0-specific:

`- http://www.verisign.com/support/csr/microsoft/v05.html`

Thawte:

Main page at Thawte Support for various Web Servers

`http://www.thawte.com/html/SUPPORT/keygen/list.html`

Microsoft Internet Information Server 5 Key and CSR Generation Instructions

`http://www.thawte.com/html/SUPPORT/keygen/msiis5/msiis5.html`

Microsoft Internet Information Server 5 Certificate Installation

`http://www.thawte.com/html/SUPPORT/server/msiis5/msiis5_install.html`

IMPORTANT! As you follow the instructions on the Web site, ensure you follow these guidelines for the SSL certificate name; the Common Name in the Certificate request *must* match the Active Directory fully qualified domain name.

Example: `SSLTEST.DOMAIN.COM`

The internal DNS name must match the domain name of the Active Directory Domain.

Example:

URL: `ssltest.company.com`

Active Directory Domain Controller computer `name = ssltest`

Active Directory Domain `name = domain.com`

TCP/IP configuration: `Host = ssltest, Domain = domain.com`

Internal DNS server `domain = domain.com`

After you receive the certificate from the Certificate Authority, export the SSL certificate and its private key. Import the Certificate into the Certificate store on the Active Directory controller.

Obtaining and Importing a Certificate From a Certificate Authority (Exchange 5.5 / Windows NT 4.0 Server)

Access the following Web sites for general instructions:

- Verisign:

  http://www.verisign.com/products/site/secure/index.html

  To generate the Customer Service Request and install the certificate: http://www.verisign.com/support/csr/index.html.

- Thawte:

  http://www.thawte.com/support/keygen/index.html and select IIS4.

Caution As you follow the instructions on the Web site, ensure you follow these guidelines for the SSL certificate name:

- The Common Name in the Certificate request must match the Computer name and NT Domain name of the server where it will be installed.
- The internal DNS name must match the domain name of the NT Domain.

Example:

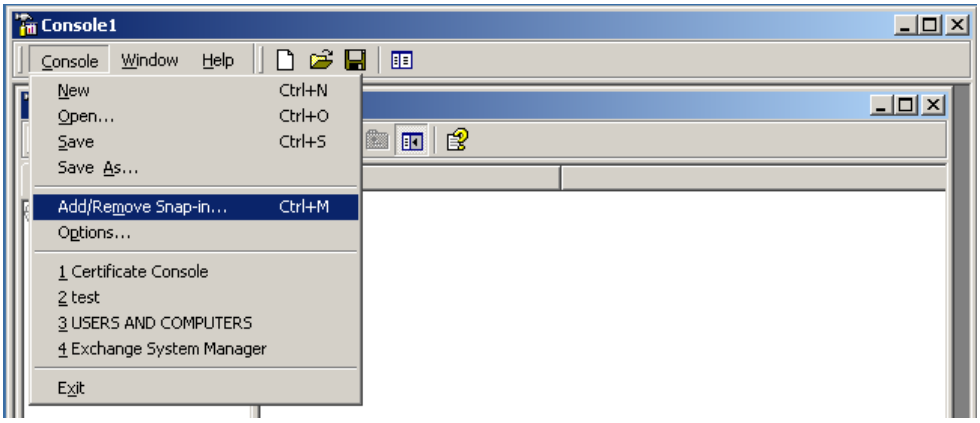
```
URL: ssltest.domain.com
Exchange/NT4 computer name = ssltest
NT4 Domain name = domain
TCP/IP configuration
Host = ssltest
Domain = domain.com
Internal DNS server domain = domain.com
```

Configure the LDAP Server to Use the Certificate and Accept an LDAPS Connection (Exchange 2000)

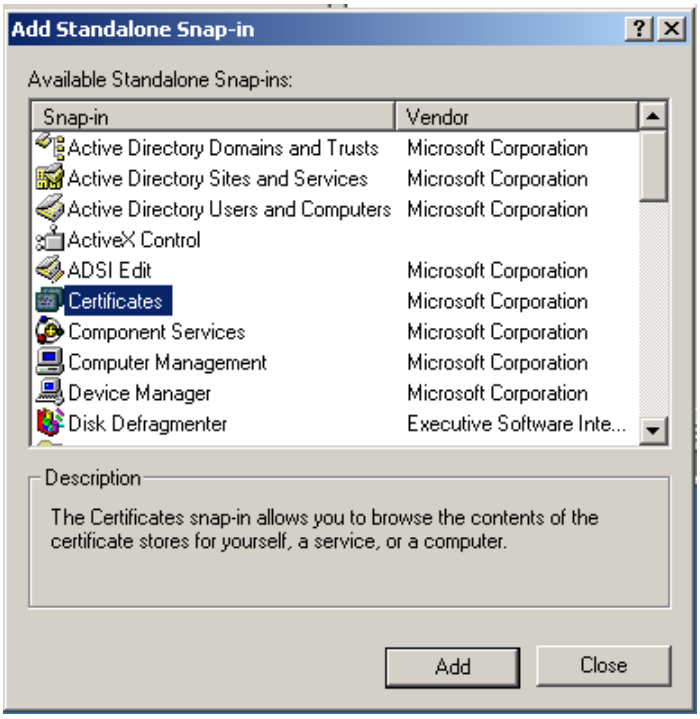
Configuring the LDAP server to use the certificate and accept an LDAP Over SSL (LDAPS) connection involves creating a Certificate Console. The Certificate Console allows you to manage your SSL Certificates and verify they are configured correctly. It is a Microsoft Management Console (MMC) Plug-in, and not available by default.

Configure the Certificate Console:

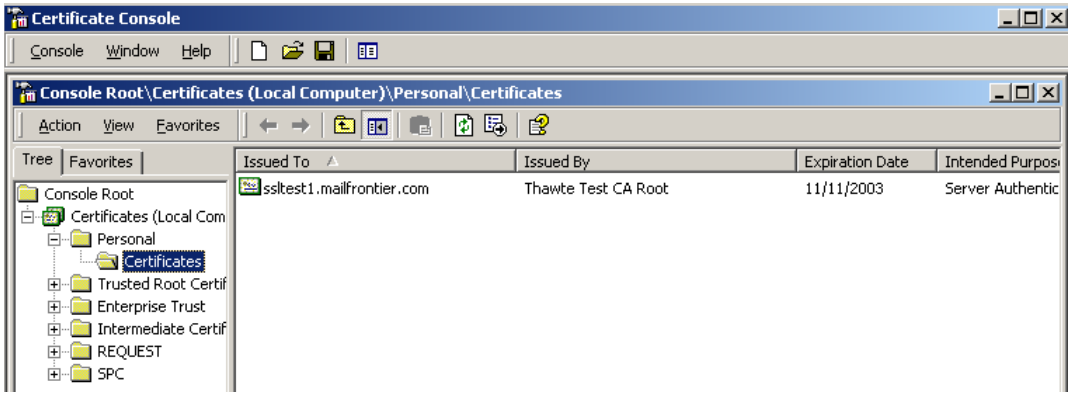
1. Click **Start > Run > MMC**.
   The Console1 screen appears.
2. Click **Console**.
3. Select **Add/Remove Snap-In**.



4. Click **Add**, and select certificates from the list of Snap-in modules on the **Add Standalone Snap-in** screen that appears.
5. Click **Add**.



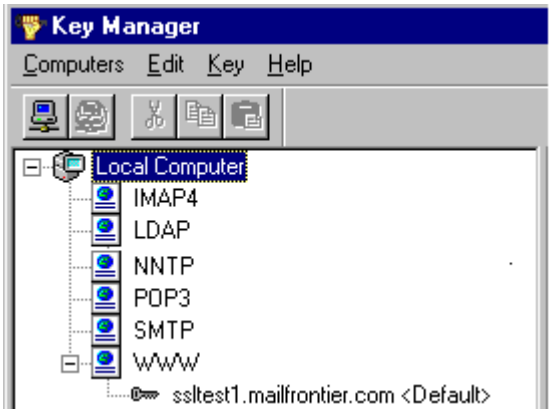
6. Select **Computer Account** on the next screen and click **Next**.
7. Leave the default of **Local Computer** on the next screen and click **Finish**.
8. Click **Close** and click **OK** to return to the Certificate Console.
9. Click **Console > Save As**, and enter **Certificate Console**, then click **Save**.
   This adds the Console to **Administrative Tools** for future use.
10. Verify the SSL certificate is in the Local Computer's Personal certificate store. Click **Start > Program Files > Administrative Tools > Certificate Console.**



LDAP communication to the Active Directory controller is now enabled over SSL.

Configure the LDAP Server to Use the Certificate and Accept an LDAPS Connection (Exchange 5.5)

1. Click **Start > Run**.
2. Enter the keyring.
   The Key Manager screen appears.



3. Highlight the installed SSL certificate under **WWW**.
4. Click **Key>Export Key> Backup File**, and enter a name, for example: **`Sslkey.`**
5. Enter a password to protect the SSL key, for example: **`my*password`**.
6. Highlight **LDAP**.
7. Click **Key> Import Key> Backup File**.
8. Select the SSL certificate you exported in step 3, (for example, `SSLkey.key`. T.
   The system automatically appends the second `key`).
9. Enter the password, for example: **`my*password.`**
10. When prompted for **Server Connection** information, click **IP Address**, and enter the IP address of your Exchange server.
11. Click **OK**.
    The SSL certificate is now usable for secure LDAP communication.

Configuring SonicWALL Email Security Gateway to use an LDAPS connection

1. In SonicWALL Email Security Gateway, go to the **Server Configuration>LDAP Configuration** screen.
2. Check the **This server requires a secured connection (SSL)** check box.
3. Change the port number to **636**.
4. Click on **Apply Changes**.


Caution

If Exchange 5.5 resides on a Windows 200x domain controller, the default port for LDAPS, 636, is already reserved by a Directory service on the Windows 200x domain controller. According to Microsoft, you must reconfigure the Exchange Server to use another port. See Microsoft Knowledge Base Article 232606.

Generating a Self-Signed Certificate for LDAP over SSL

Prerequisites

You must have a copy of OpenSSL to generate a CA certificate. Sun's KEYTOOL program does not support Certificate Authority-issuing functionality. OpenSSL can perform this task. A Win32 binary version can be downloaded at `www.slproweb.com`

OpenSSL is also a part of the Cygwin utilities distribution (`www.cygwin.com`), but it is not part of the default installation. You must manually select OpenSSL during the installation of Cygwin.

These instructions are based on the following environment:

- Exchange 5.5 and IIS 4.0 on Windows NT 4.0 SP6.
- SonicWALL Email Security Gateway Version 3 on Windows 2003 Server, originally configured to use LDAP/389
- Using Sun's Java Runtime Environment on Windows (installed as part of the Windows version of SonicWALL Email Security Gateway)

Caution: If Exchange 5.5 resides on a Windows 200x domain controller, the default port for LDAPS, 636, is already reserved by a Directory service on the Windows 200x domain controller. According to Microsoft Knowledge Base Article 232606, you must reconfigure the Exchange Server to use another port.

Setting up SSL between SonicWALL Email Security Gateway and the LDAP Server

Setting up SSL between SonicWALL Email Security Gateway's Tomcat Web Server and the LDAP Server consists of five parts:

1. Creating a private key and Certificate Authority (CA) certificate
2. Creating an Exchange Certificate Server Request (CSR)
3. Creating a Server Certificate with the private key and CA certificate
4. Installing a Server Certificate in Exchange
5. Installing a CA certificate in Tomcat

1. Creating a Private Key and a CA Certificate:

1. Install OpenSSL on any workstation.
2. Create a private key with OpenSSL. Type:

   `openssl genrsa -des3 -out` ***`privateKeyFileName`*** **`1024`**
3. When prompted, enter a password or pass phrase you can remember for this key.

Note the command line syntax is case-sensitive.

4. Create a Certificate Authority certificate using the private key created above. Type:

   `openssl req -new -key privateKeyFileName -x509 -days n -out <CACertFileName>`

   NOTE: The `-days n` parameter allows you to enter the number of days the CA certificate is valid from *n* days from today.

   Example:

   ```
   openssl req -new -key PrivateKey.key -x509 -days 10000 -out CACert.crt
   ```

5. When prompted for the pass phrase, enter the password you used in step 2 above and press **Enter**.

Caution As you follow the instructions to create a Certificate Authority, ensure the Common Name is the fully qualified domain name (FQDN) or the server name of the Exchange server.

2. Creating an Exchange Certificate Server Request (CSR)

1. On the server where Exchange and IIS are installed on, login as the administrator and run **keyring** from the command line.
2. In keyring, highlight the LDAP node and click **Key->Create New Key** to create a Certificate Server Request. On the dialog box where you are asked for the Common Name (CN), you must enter the fully qualified domain name (FQDN) of the Exchange server. If you do *not* enter a valid FQDN here, the authentication between Tomcat and Exchange will fail with the message:
   `trusted Certificate cannot be found`
3. When you type in the password for the CSR, it does not have to be same as the one used in "1. Creating a Private Key and a CA Certificate:" on page 189 but for consistency, use the password you created in "1. Creating a Private Key and a CA Certificate:" on page 189. Otherwise, you must remember the password for this step when you install the signed key certificate later).
4. Save the CSR to a file and copy it to the workstation where you are running OpenSSL.

3. Creating a Server Certificate with the Private Key and a CA Certificate

Type:

```
openssl x509 -req -days n -in CSR from Exchange -CA <CACertFileName> -CAkey
<privateKeyFileName> -CAcreateserial -out <ServerCertFileName>
```

Example:

```
openssl x509 -req -days 10000 -in NewKeyRq.txt -CA CACert.crt -CAkey PrivateKey.key -
CAcreateserial -out ServerCert.crt
```

4. Install the Server Certificate in Exchange

1. Take the `ServerCertFileName created in` "3. Creating a Server Certificate with the Private Key and a CA Certificate" on page 190 and copy it to the Exchange server.
2. On the Exchange server, run keyring, locate the LDAP node and the key you created in "2. Creating an Exchange Certificate Server Request (CSR)" on page 190, right click on the key and select **Install Key Certificate**.

3. When the **Open** dialog box appears, select the **ServerCertFileName** and click **Open**.
4. When prompted for a password, type in the password used in "2. Creating an Exchange Certificate Server Request (CSR)" on page 190.
5. When prompted for **Server Connection**, select **Default**.

5. Install the CA certificate in Tomcat

1. Take the CACertFileName created in "1. Creating a Private Key and a CA Certificate:" on page 189, step 3, and install it in Tomcat on SonicWALL Email Security Gateway using Sun's KEYTOOL program located in `C:\Program Files\Java\j2re1.4.2_03\bin`. Type:

   ```
   keytool -import -keystore C:\Program Files\Java\j2re1.4.2_03\lib\security\cacerts -
   file CACertFileName -alias CACertName
   ```

   Example:

   ```
   keytool -import -keystore C:\Program Files\Java\j2re1.4.2_03\lib\security\cacerts -
   file CACert.crt -alias CACert
   ```

2. Restart both the Exchange server and Tomcat. When the Exchange Server is restarted, look in the Event Viewer on the Exchange Box to verify that the `MSExchangeDS LDAP Interface` is started on both port 389 and 636.
3. Log in to SonicWALL Email Security Gateway as the administrator and change the LDAP Configuration to use port 636.
4. Check the **This server requires a secure connection (SSL)** check box.
5. Click Apply Changes.
6. Test the **LDAP Login** and the **LDAP Query** to verify LDAPS connectivity.

Setting Up SSL Between Control Center and a Remote Analyzer

Setting up SSL between the Control Center and a Remote Analyzer includes three steps:

- Generating a self-signed certificate
- Setting up Tomcat to accept an HTTPS connection
- Configuring a Remote analyzer as a secure server

Generating a Self-Signed Certificate Keystore

The keystore file contains your public and private keys. Each keytool command has a `–keystore` option for specifying the name and location of the persistent keystore file for the keystore managed by a keytool. The keystore is stored in a file named `.keystore` in the user's home directory, as determined by the `user.home` system property. On Solaris systems, `user.home` defaults to the user's home directory.

To generate and store keys in a keystore:

NOTE: <JAVA_HOME> is a variable that represents where the Java directory is installed.

1. On Windows 2000 and Windows 2003 Server, enter the following:

   `<JAVA_HOME>\bin\keytool –genkey –keyalg RSA –alias tomcat`

On Unix, enter the following:

```
<JAVA_HOME>/bin/keytool –genkey –alias tomcat -keyalg RSA –keystore~root/.keystore
```

Example:

```
<MailFrontierEG>/java/bin/keytool -genkey –alias tomcat - keyalg RSA
```

2. Respond to system prompts regarding general system information:

- **Password.** The default Tomcat password is **changeit** (all lower case).
- **First and last name.** Enter the name of the server you are using, for example, machine1234.XYZcorp.com.
- Name of your organizational unit.
  Example: Engineering.
- Name of your organization.
  Example: example_company
- Name of your city or locality.
  Example: San Francisco.
- Name of your State or Province.
  Example: California.
- 2-letter country code.
  Example: US

The system displays the information entered for review.

3. Enter **Yes** to approve the entries, or edit them as necessary.

   The system prompts you for the same password you entered earlier. The system displays **Return** if it uses the same password as .keystore password, but you must type the password again.

The .keystore file is now created.

Setting Up Tomcat to Accept an HTTPS Connection

To modify Tomcat to use your certificate store, open Tomcat's server.xml file in a text editor. This file is located in *YOUR_TOMCAT_INSTALL_DIR*/conf.

1. Scroll down to find the following text:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<!--
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"
useURIValidationHack="false" disableUploadTimeout="true">
<Factory ClassName="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" />
</Connector>
-->
```

2. Remove the comment notation from this connector; remove the <!-- and --> around the connector tag. After you remove the comments, the text should look as follows:

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->
<Connector className="org.apache.coyote.tomcat4.CoyoteConnector"
port="8443" minProcessors="5" maxProcessors="75"
enableLookups="true"
acceptCount="100" debug="0" scheme="https" secure="true"
useURIValidationHack="false" disableUploadTimeout="true">
<Factory className="org.apache.coyote.tomcat4.CoyoteServerSocketFactory"
clientAuth="false" protocol="TLS" />
  </Connector>
```

3. Find and replace all references in the code to port 8443 to 443 in the Tomcat's `server.xml` file.
4. Restart the Tomcat service or reboot the server. After the server has rebooted, you can navigate to `https://your_server_name/` or `http://your_server_name`.

Configuring a Remote Analyzer as a Secure Server

To configure a Remote Analyzer as a secure server:

1. Access **Server Configuration** on SonicWALL Email Security Gateway.
2. Check the **Remote Analyzer** check box that you want to make a secure server.
3. Click **Edit**.
   An Edit screen appears.
4. Change the **port number** for the secure connection to 443.
5. Check the box that enables a **Secure SSL connection for this Remote Analyzer**.
6. Use the **Test** buttons to verify that SSL connectivity is working.

Importing New Verisign Certificates into the Keystore

To import a new Verisign certificate:

1. Type:

   ```
   $ ./keytool -certreq -alias tomcat -keyalg RSA -file /export/spare/kris/cr.txt
   ```

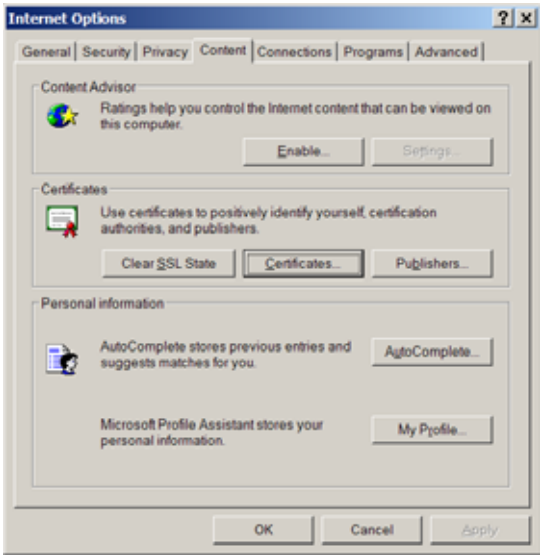
2. Enter the `.keystore` password:

   ```
   changeit
   $
   ```

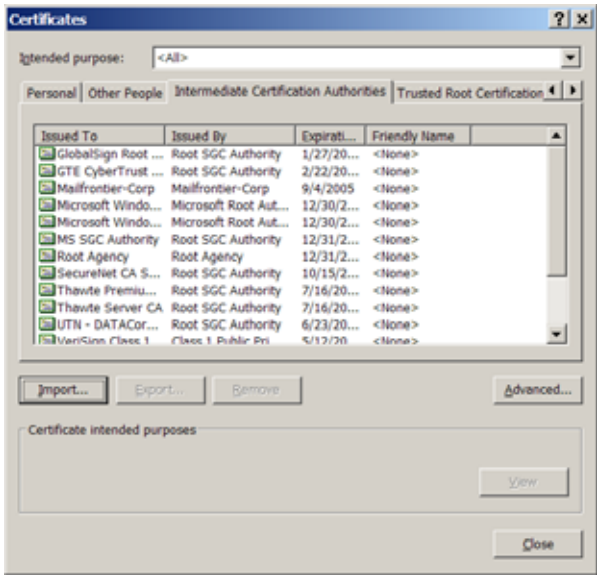
   Verisign creates a certificate that is automatically downloaded.

   NOTE: If you purchase a Global Secure Site Pro Certificate (128 bit), there are additional steps involved in the installation. The Global Secure Site Pro Certificate requires an intermediate certificate to complete the authentication chain of trust. The existing Intermediate Certificate expired on 1/7/2004. Therefore, you must include the new Intermediate Certificate when doing the import into Tomcat.

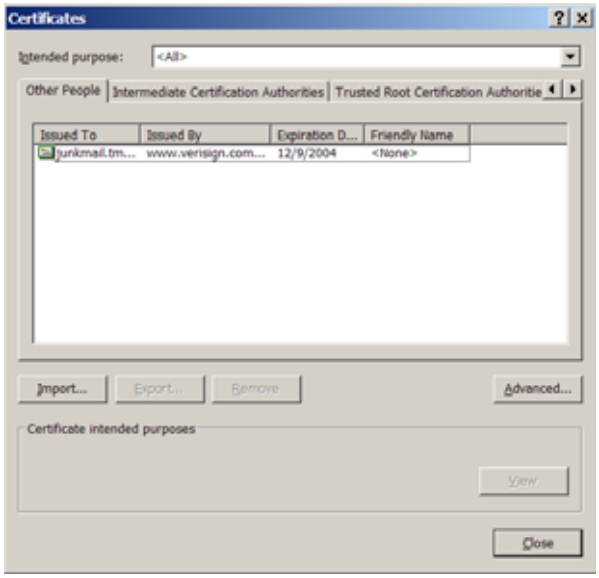
3. Download the certificate that was purchased from Verisign, and save it as a text file.
4. Download the Intermediate certificate from this location `https://www.verisign.com/support/site/caReplacement.html` and save it as a text file.
5. Import the Intermediate Certificate into the Internet Explorer browser.
6. In your browser, go to **Tools > Internet Options > Content Tab**.
7. Click the **Certificates** button.



8. Select the **Intermediate Certification Authorities Tab.**

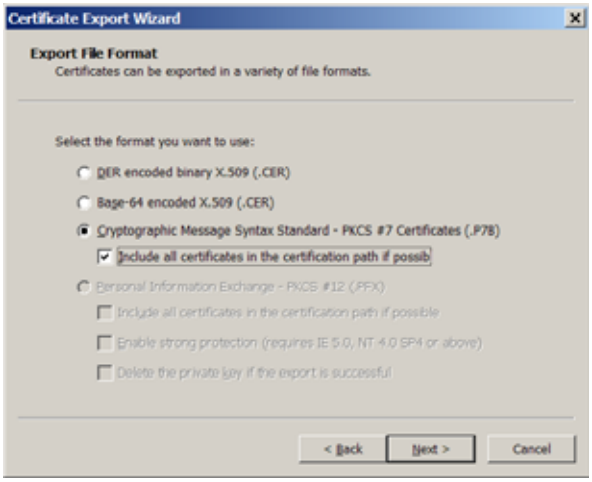


9. Click the **Import…** button and follow the steps in the Certificate Import wizard to import your certificate. This imports the Intermediate Certificate into the Internet Explorer keystore.
10. Import the certificate that was received from Verisign using the same procedure.
11. Highlight the **Other People Tab**.
12. Press the **Import…** button.
13. Follow the steps in the Certificate Import wizard to import your certificate.



The certificate is displayed in the list of Other People Certificates.

14. Highlight the certificate and press the **Export…** button.
15. Follow the steps in the Certificate Export Wizard.
16. For the export File Format, select `Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)`
17. Check the **Include All Certificates In The Certification Path** if possible.



18. Save this file with a `.p7b` extension.
    This creates a file with the complete certification chain of your certificate and includes the new Verisign Intermediate certificate plus the Verisign Root certificate.
19. Import this into your keystore file. Type:

    ```
    $ ./keytool -import -keyalg RSA -trustcacerts -alias tomcat -file /yourfile.p7b
    ```

20. Enter keystore password:

    ```
    changeit
    ```

The top-level certificate appears:

```
Owner: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
```

```
Issuer: OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
Serial number: 70bae41d10d92934b638ca7b03ccbabf
Valid from: Sun Jan 28 16:00:00 PST 1996 until: Tue Aug 01 16:59:59 PDT 2028
Certificate fingerprints:
         MD5:  10:FC:63:5D:F6:26:3E:0D:F3:25:BE:5F:79:CD:67:67
         SHA1: 74:2C:31:92:E6:07:E4:24:EB:45:49:54:2B:E1:BB:C5:3E:61:74:E2

... is not trusted. Install reply anyway? [no]:  yes
Certificate reply was installed in keystore
```

Importing the LDAP Server's SSL Root Certificate to the SonicWALL Email Security Gateway Server

If the SSL certificate's root is not trusted by the LDAP client (SonicWALL Email Security Gateway server), attempts to establish an SSL connection fails. The only certificates that are trusted are those whose root certificates are present in the local Java Runtime Environment keystore. If the certificate used by the LDAP server was self-generated or generated by a Microsoft Certificate Server, then the root certificate is unknown to SonicWALL Email Security Gateway Tomcat server. You must import the root certificate into the Java Root Certificate Keystore.

To import a root Certificate Authority certificate — either self-signed or third-party signed —you must import it into the `cacerts` keystore.

1. Extract the root key from the Certificate Authority that created your SSL certificate for LDAP. Refer to the documentation that comes from the Certificate Authority on how to extract a root key. You receive a text file root certificate file that looks similar to this:

   ```
   -----BEGIN CERTIFICATE-----
   MIIDRzCCArCgAwIBAgIEO5kvRTANBgkqhkiG9w0BAQUFADBQMQswCQYDVQQGEwJV
   UzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25z
   dHJhdGlvbiBDZXJ0aWZpY2F0ZXMwHhcNMDEwOTA3MjAwNDEzWhcNMjEwOTA3MjAz
   NDEzWjBQMQswCQYDVQQGEwJVUzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMm
   RW50cnVzdCBQS0kgRGVtb25zdHJhdGlvbiBDZXJ0aWZpY2F0ZXMwgZ0wDQYJKoZI
   BENSTDEwKwYDVR0QBCQwIoAPMjAwMTA5MDcyMDA0MTNagQ8yMDIxMDkwNzIwMDQx
   M1owCwYDVR0PBAQDAgEGMB8GA1UdIwQYMBaAFHNSsvL8PTcMqhffaMAOOpbtViW6
   MB0GA1UdDgQWBBRzUrLy/D03DKoX32jADjqW7VYlujAMBgNVHRMEBTADAQH/MBkG
   CSqGSIb2fQdBAAQMMAobBFY0LjADAgSQMA0GCSqGSIb3DQEBBQUAA4GBAAx6b1uh
   0ZLLgvnc+ePagi1cK3oRL5XMNawXamiiub+WfHXxyl2A2L9Gg3T5JdEooGAo1v1n
   w4KN8Iz+E5BTly+vJkP7WCOcchXg8aDxI8kCySlkxqJ+hcX7/hdvOzEAPkkJRboz
   VonUPwEk+elHGXQDcr5nXllPwl9UzFkgrxBZ
   -----END CERTIFICATE-----
   ```

2. Locate the `cacerts` file for the Java installation used by SonicWALL Email Security Gateway's Tomcat.
   It should be located at

   ```
   C:\Program Files\Java\j2re1.4.1_01\lib\security\cacerts
   ```

3. Import the root key certificate from the `root_certificate_file`:
4. Navigate to `<%JAVAhome>`.
5. Type:

   ```
   \bin\keytool -import -keyalg RSA -alias tomcat -keystore
   ..\jre\lib\security\cacerts -file root_certificate_file
   ```

   a. The `keytool` prompts:

   ```
   Enter keystore password:
   ```

   b. Type the default password for the java `cacerts` key store: **`changeit`**.

Appendix D

SonicWALL Email Security Log Files

About SonicWALL Email Security Gateway Logs

SonicWALL Email Security Gateway provides several sets of log files available for tracing and diagnosing problems and for monitoring message tracking. Logs for a specific server are under the `logs` directory in SonicWALL Email Security Gateway installation path (for example, `C:\ProgramFiles\MailFrontierEG\logs)`.

Aggregate logs for across multiple servers can be found under the `commonlogs` directory (for example, `C:\ProgramFiles\MailFrontierEG\data\commonlogs`).

Message Tracking Log File

SonicWALL Email Security Gateway tracks all SMTP messages, so you can see what happened to each message and why it might have been flagged as spam. A new file is created every day based on Greenwich Mean Time (GMT), and is stored in the log folder of the SonicWALL Email Security installation directory. This system continually appends new data to the day's file. The log file is a tab-separated file, easily loaded into Excel or another spreadsheet for analysis. For inbound messages the file name `mfe<yyyymmdd>.log` and for outbound messages the file name is `mfe<yyyymmdd>_out.log` where, `yyyy` stands for the year, `mm` stands for the month, and `dd` stands for the day of the month.

Table 1 Log File Fields

Field	Meaning
Version	The format version of this log file line
DateTime	The date and time the message was received in GMT
MsgId	The SMTP message ID
SenderAddr	Sender's address (envelope's "MAIL FROM")
RecipAddr	Recipients' addresses (envelope's "RCPT TO")
NumRecip	Number of recipients
NumBytes	Size of the message in bytes
ClientIp	IP address of the sender
ClientName	Host name of the sender
ServerIp	IP address of the downstream SMTP server
ServerName	Host name of the downstream SMTP server
NumAttach	Number of attachments

ServerAction	Actions taken upon the message (none, quarantine, delete, tag, reject, redirect)
ServerReason	Reason for above action
Priority	Priority flag of the message
Subject	Subject line of the message
SenderDomain	Domain name of the sender
MessageThreat	Disposition of the message (spam, likely spam, or other types of junk)
Categories	Information about various email categories into which this email falls
DescriptiveName	Threat name (e.g. the name of the policy or virus)
OrigRcptIfRewritten	If email address rewriting is enabled and applied to this email, this is the original sender or recipient before the email was rewritten
UniqSmtpSessionId	A unique ID associated with each email. Used for troubleshooting.

Statistics Log

Hourly, daily, and monthly statistics are compiled into Comma Separated Value (CSV) files, which you can use to generate your own reports. You can load these into Excel or another spreadsheet for analysis. `MlfUpdater.exe` parses the message tracking logs every hour.

Files that do not end in `_display.cvs` are ongoing history of statistics for a particular server. The `_display.csv` files are truncated histories of statistics collected across the servers in an SonicWALL Email Security Gateway configuration. The exceptions to this are the address book statistics files because the source information for these is shared across servers. The `_spammer_` files are tallies of domains that were judged to be sources of spam. The table below displays each file name and a brief description of its contents.

File Name	Contents
`mlf_boundary_date.csv`	Timestamp for the previous log analysis, used to scan logs more efficiently
`mlf_addrbk_stats.csv`	Snapshot of the last change to the address book size statistics
`mlf_hourly_addrbk_display.csv`	History of hourly snapshots of address book size statistics
`mlf_daily_addrbk_display.csv`	History of daily snapshots of address book size statistics
`mlf_monthly_addrbk_display.csv`	History of monthly snapshots of address book size statistics
`mlf_hourly_stats.csv`	History of complete hourly SMTP log statistics for the local server
`mlf_hourly_stats_part.csv`	Incomplete (current) hourly SMTP log statistics for the local server
`mlf_hourly_stats_display.csv`	Rollup of the hourly SMTP log statistics for all servers
`mlf_hourly_spammer.csv`	History of complete hourly spammer statistics for the local server
`mlf_hourly_spammer_part.csv`	Incomplete (current) hourly spammer statistics for the local server
`mlf_hourly_spammer_display.csv`	Rollup of the hourly spammer statistics for all servers
`mlf_daily_stats.csv`	History of complete daily SMTP log statistics for the local server
`mlf_daily_stats_part.csv`	Incomplete (current) daily SMTP log statistics for the local server
`mlf_daily_stats_display.csv`	Rollup of the daily SMTP log statistics for all servers
`mlf_daily_spammer.csv`	History of complete daily spammer statistics for the local server
`mlf_daily_spammer_part.csv`	Incomplete (current) daily spammer statistics for the local server

File Name	Contents
mlf_daily_spammer_display.csv	Rollup of the daily spammer statistics for all servers
mlf_monthly_stats.csv	History of complete monthly SMTP log statistics for the local server
mlf_monthly_stats_part.csv	Incomplete (current) monthly SMTP log statistics for the local server
mlf_monthly_stats_display.csv	Rollup of the monthly SMTP log statistics for all servers
mlf_monthly_spammer.csv	History of complete monthly spammer statistics for the local server
mlf_monthly_spammer_part.csv	Incomplete (current) monthly spammer statistics for the local server
mlf_monthly_spammer_display.csv	Rollup of the monthly spammer statistics for all servers
mlf_running_total_stats.csv	Snapshot of total SMTP log statistics for the local server
mlf_running_total_stats_display.csv	Rollup of total SMTP log statistics for all servers

The `mlfupdater` utility gathers and aggregates the statistics every hour to ensure that all processing of the messages has been completed.

MLF Report Logs

SonicWALL Email Security Gateway adds the following log files to the logs directory on every machine on which it is runs, as shown in Table 2 on page 199. These logs assist in debugging log issues.

Table 2 MLF Report Logs

Log Name	Function
MlfMfeImportCopy.log	Logs information during a `-copylogs` operation, in which mfe logs are parsed and copied into hourly `mfe` logs for replication.
MlfMfeImportRead.log	Logs information during a `-importchangedlogs` operation, in which hourly `mfe` logs are imported into the database.
MlfMfeImportSetup.log	Logs information during the period before the program has parsed the arguments passed to it to determine which actions to perform. **Logs all information about creating the database and tables, the performance test option, and anything else not directly related to the other two log files.** Used at the beginning of every invocation of `mlfmfeimport.exe`.

Bookmark Files

Bookmark files are also stored in the logs directory of the server on which SonicWALL Email Security Gateway runs.

Table 3 Bookmark Files

File Name	Function
copybookmark.xml	Stores the offset of the mfe log from which we are copying data into hourly `mfe` logs. Used for inbound message processing.
copybookmark_out.xml	Stores the offset of the mfe log from which we are copying data into hourly `mfe` logs. Used for outbound message processing.

read bookmark-<hostname>.txt	Stores the offset into the hourly `mfe` log from which data is being imported into the database. There is one `readbookmark-<hostname>.txt` file for each machine that provides hourly mfe logs to the reports directory. Used for inbound message processing.
read bookmark-<hostname>_out.txt	Stores the offset into the hourly `mfe` log from which data is being imported into the database. There is one `readbookmark-<hostname>_out.txt` file for each machine that provides hourly mfe logs to the reports directory. Used for inbound message processing.

These bookmark files are to be created and modified only by `mlfmfeimport`. If they are deleted or modified by any other means, data could be lost or bad data could be written to the database.

Login File

For security reasons, you can check who has logged in to SonicWALL Email Security Gateway. This information is logged with a separate file for each day (01, 02, and so on). The files roll over each month. The log displays the date and time of login, hostname, the logged in user, the ID used to log in, and the permissions of the ID, for example:

20031001113414 turlock - Logged in user with email=asgmonitoring@mailfrontier.com, ID=admin, and permission of Account Admin

The files are stored under `data\commonlogs\activities`.

Event Logging

You can set event logging from level 1, for maximum logging, to level 6, for minimum logging. By default, logging is enabled at level 3.

Note Do *not* adjust the log level unless you are troubleshooting a specific problem with the help of SonicWALL Email Security's Technical Support staff.

Glossary

Term	Definition
All-in-One Architecture	An architecture for the SonicWALL Email Security Gateway where one server manages all email protection that receives all enterprise email. See also *Split Architecture* on page 203.
Allowed List (Whitelist)	Lists of users, domains, and mailing lists that are allowed to send email to users in your organization.
Anti-Virus	Software that detects viruses in email message bodies and attachments.
Blocked List (also known as Black Lists)	Lists of users, domains, or mailing lists from whom you or your users do not want to receive email.
Collaborative Settings	SonicWALL Email Security Gateway administers its own content-based email signature network with a collaborative community of users and junk mailboxes worldwide. You can select collaborative settings to customize the level of influence community input has on enterprise spam blocking.
Control Center	Manages all data files; it controls and communicates with one or more of the remote analyzers. It stores or quarantines mail it receives from the remote analyzer, and queries LDAP servers to ensure valid users can log in to the SonicWALL Email Security Gateway.
Dashboard	A high level overview of the system statistics.
Cluster	A group of SonicWALL Email Security Gateway servers that act like a single system and enable high availability and, in some cases, load balancing and parallel processing.
Directory Harvest Attack (DHA)	Spammers stage Directory Harvest Attacks (DHA) to get lists of all users in an organization's directory. DHA makes organizations vulnerable to increased attacks, spam, and fraudulent messages.
DMZ	The logical space between two firewalls where an email gateway typically resides. This term was derived from De-Militarized Zone, an area between two warring countries where tanks were not permitted.
Envelope	Information in RFC-821 format, which includes the address from which the mail came and the receipt-to address.

Term	Definition (continued)
Honeypot	A specially equipped system deployed by security professionals to lure hackers and track their every move.
Internet Message Access Protocol (IMAP)	A method of accessing electronic mail messages that are kept on a mail server. IMAP permits a client email program to access remote message stores as if they were local.
Keystore	The keystore file contains your public and private keys.
Junk Box	A Web page interface that displays all quarantined email.
Junk Box Summary	A daily email sent to users summarizing email messages that have been quarantined because they contained spam, viruses, or other undesired mail content.
Lightweight Directory Access Protocol (LDAP)	An Internet protocol that email programs use to look up contact information from a server.
LDAP Groups	Allow you to assign roles to user groups and set spam-blocking options for user groups. This is an optional configuration that enables you to fine-tune user access by group.
LDAPS	LDAP run over SSL provides a secure LDAP connection
Master Account	The initial account you log in to when configuring SonicWALL Email Security Gateway. This is also the master administrative account.
Mail Transfer Agent (MTA)	Email software that runs on an outward-facing server that delivers mail to an organization.
Phishing	Sending email or creating a replica of an existing Web page to fool a user into submitting personal, financial, or password data. In the enterprise, phishers seek enterprise passwords and sensitive information. Phishers might use enterprise email to send fraudulent information to customers and business partners.
Post Office Protocol Version 3 (POP3)	A protocol used to retrieve email from a server.
Policy Management	A customizable module that enables the administrator to filter the content of email messages and attachments that enter SonicWALL Email Security Gateway.
Profiler	A software component that collects users' outgoing email addresses, which can optionally be stored as known good addresses. The Profiler can be configured to work with each supported email client.
Probe Account	Similar to a Honeypot, an account that is established on the Internet for the sole purpose of collecting spam and tracking hackers.
Quarantine	A means of containing suspect email messages in a Junk Box.
Realtime Blackhole List. (RBL)	A list of Internet TCP/IP addresses known to send spam, or by hosts considered friendly to spam.

Term	Definition (continued)
Remote Analyzer	An SMTP proxy placed in the email flow, and performs a spam analysis to determine whether email is good or junk. It sends junk mail to the control center where it is quarantined, and routes good mail to its destination server.
Privilege Roles	Users can be assigned privileges so that they can administer all email, log in as another person or for a helpdesk role, can view SonicWALL Email Security Gateway reports, or view their own Junk Box.
Sender ID	A mechanism that determines whether the alleged domain address of each email is authentic, which is one factor SonicWALL Email Security Gateway uses to determine whether the message is junk.
Simple Mail Transfer Protocol (SMTP)	A protocol designed to transfer mail reliably and efficiently.
Secure Socket Layer (SSL)	A protocol for transmitting private documents via the Internet. SSL uses a private key to encrypt data that is transferred over the SSL connection.
Spam	Any unsolicited commercial email that a user does not want. Spam frequently contains false advertising, get-rich-quick schemes, and other offensive material.
Split Architecture	Architecture for networks with multiple physical data centers, the functions of SonicWALL Email Security Gateway can be split across different servers in different locations.
STARTTLS	The keyword used to initiate a secure SMTP connection between two servers using Transport Layer Security (TLS).
Tarpitting	Protects your enterprise from spammers trying to spam your mail server accounts through Directory Harvest attacks (DHA).
Time Zero Virus	A term for the first hours that a virus is released, when major anti-virus companies have not yet modified their virus definitions to catch it.
Thumbprint	Checksums that uniquely identify email from junk messages. The thumbprint contains absolutely no readable information. Thumbprints are sent the collaborative community to block new types of junk.
Transport Layer Security (TLS)	TLS is the successor to the Secure Sockets Layer (SSL) protocol. The terms SSL and TLS are often used interchangeably since they are very similar protocols.
Usermap	A local cache of the LDAP Server containing the list of email aliases per user.
User Profile	An optional program that creates per-user allowed lists based on the information in address books and sent items, and then uses the HTTP protocol to post these allowed lists in an XML format to the SonicWALL Email Security Gateway.
Unjunk	Removing messages from the Junk Box as enabled by the administrator.
Virus	Message content that contains malicious and self-replicating code. A virus in email can infect the user's computer and then use email to propagate itself to other computers.

Index

Q

R

S

T

U

V

W

X

SonicWALL,Inc.
1143 Borregas Avenue
Sunnyvale,CA 94089-1306

T: 408.745.9600
F: 408.745.9300

www.sonicwall.com

P/N 232-000042-00
Rev A 04/06