SonicWall® Email Security 9.1

Administration

Contents

Part 1. Introduction

Introduction to Email Security . . . 8
Description of Email Security . . . 8
Available Module Licenses . . . 9
Email Security Deployment Architecture for Appliances . . . 9
All in One Architecture . . . 10
Split Network Architecture . . . 10
Selecting an Architecture . . . 11
Other Planning Considerations for Email Security Appliances . . . 11
Email Security as the First-Touch/Last-Touch Server . . . 12
Proxy versus MTA . . . 12
Inbound and Outbound Email Flow . . . 13
Hosted Email Security Overview . . . 13
Activating the Hosted Email Security Service . . . 14
Adding MX records . . . 14
Logging into the HES Console . . . 15

Part 2. Monitor

Dashboard . . . 17
Using the Reports . . . 17
Customizing the Display . . . 17
Configuring Chart Formats . . . 18
Filtering Chart Data . . . 19
Managing Table Formats . . . 19
Dashboard . . . 20
Event Summaries . . . 21
All Event Connections . . . 22
Anti-Spam . . . 22
Anti-Phishing . . . 23
Anti-Virus . . . 23
Anti-Spoof . . . 23
Directory Harvest . . . 23
Capture ATP . . . 24
Policy and Compliance . . . 24
Policy . . . 24
Compliance . . . 25
Encryption . . . 25
Appliance Health . . . 25
Live Monitor . . . 26
Performance Metrics . . . 26
LDAP Users . . . 27

Current Status 28
System Status 28
MTA Status 29

Part 3. Investigate

INVESTIGATE | Junk Box 32
Using the Junk Box 32
Simple Searching for Data 32
Filtering Table Data 33
Customizing the Display 33
Managing Junk Box Messages 33

Email Continuity 35
Managing the Email Tables 35
Simple Search for Data 36
Filtering Table Data 36
Customizing the Display 36
Inbox 36
Outbox 37
Sent 38

Logs 39
Message Logs 39
Simple Searching for Data 39
Filtering Table Data 40
Customizing the Display 40
Sharing Data 40
Connection Logs 41
Capture ATP Logs 42

Tools 44
Run DMARC Reports 44
Generating the Report 45
Defining New Filters 46
Audit Trail 46
Diagnostics 48

Part 4. Manage

Basic Administration 51
License Management 51
Firmware Update 52
Backup/Restore 53
Manage Backups 53
Schedule Backup 53
FTP Profiles 56
Downloads 57

Policy & Compliance 58
Policy Management and Mail Threats 58
Filters 59
Preconfigured Inbound Filters 59
Preconfigured Outbound Filters 60
Adding Filters 61
Language Support 65
Managing Filters 65
Advanced Filtering 66
Policy Groups 69
Adding a New Policy Group 69
Removing a Policy Group 69
Listing Members 70
Compliance 70
Dictionaries 71
Approval Boxes 73
Encryption 75
Record ID Definitions 75
Archiving 77

System Setup | Server 78
Administration 78
Email Security Master Account 78
User Interface Preference 79
Password Policy 79
Invalid Login Policy 79
Login Custom Text 80
Allow Admin Access from Specific IPs 80
Quick Configuration 80
LDAP Configuration 81
Configuring LDAP 81
Server Configuration 82
Global Configurations 82
LDAP Query Panel 83
Add LDAP Mappings 84
Updates 86
Monitoring 87
Configure System Monitoring 87
Alert Suppression Schedule 88
Miscellaneous 89
Monitor Configure 90
Host Configuration 91
Hostname 91
HTTPS Settings 91
Date & Time Settings 91
Network Settings 92
CIFS Mount Settings 94

Advanced . . . 95
General Settings . . . 95
Miscellaneous Settings . . . 96
Reset Settings . . . 97

System Setup | Customization and Certificates . . . 98
Customization . . . 98
User View Setup . . . 98
Branding . . . 100
Quick Settings . . . 100
Packages . . . 101
Certificates . . . 102
Generate/Import . . . 102
Generate CSR . . . 102
Configure . . . 103

Users, Groups & Organizations . . . 104
Users . . . 104
User View Setup . . . 104
Locked Users . . . 108
Groups . . . 108
Assigning Roles to Groups Found in LDAP . . . 108
Set Junk Blocking Options for Groups Found in LDAP . . . 110
Organizations . . . 119
Organizations Overview . . . 120
Adding an Organization . . . 120
Signing In as an OU Admin . . . 121
Configuring OU Settings . . . 121
Removing an Organization . . . 121
Users and Groups in Multiple LDAP . . . 121
Users . . . 121
Groups . . . 123

System Setup | Network and Junkbox Commands . . . 125
Network . . . 125
Server Configuration . . . 125
MTA Configuration . . . 138
Email Address Rewriting . . . 140
Trusted Networks . . . 141
Junk Box . . . 142
Message Management . . . 142
Summary Notifications . . . 143

Anti-Spam . . . 147
Spam Management . . . 147
Address Books . . . 149
Using the Search Field . . . 149
Adding People, Companies, Lists, or IPs . . . 150

Deleting People, Companies, Lists, or IPs . . . 150
Importing and Exporting the Address Book . . . 150
Anti-Spam Aggressiveness . . . 151
Configuring Grid Network Aggressiveness . . . 151
Configuring Adversarial Bayesian Aggressiveness . . . 152
Unjunking spam . . . 152
Category settings . . . 152
Languages . . . 153
Black List Services . . . 153
Adding to the Black List . . . 153
Email from Sources on the Black Lists Services . . . 153
Spam Submissions . . . 153
Managing Spam Submissions . . . 154
Probe Accounts . . . 154
Managing Mis-Categorized Messages . . . 154
Forwarding Mis-Categorized Email . . . 155
Configuring Submit-Junk and Submit-Good email accounts . . . 155

Anti-Spoofing . . . 156
Inbound SPF Settings . . . 156
Inbound DKIM Settings . . . 158
Inbound DMARC Settings . . . 159
Inbound DMARC Report Settings . . . 160
Outbound DKIM Settings . . . 160
Generating DNS Record . . . 161
Managing Outbound DKIM Settings . . . 162

Anti-Phishing and Anti-Virus . . . 163
Anti-Phishing . . . 163
Phishing Overview . . . 163
Configuring Phishing Protection . . . 164
Anti-Virus . . . 165
Inbound Anti-Virus Protection . . . 165
Outbound Anti-Virus Protection . . . 166

Capture, Encryption and Connections . . . 170
Capture ATP . . . 170
Basic Setup Checklist . . . 171
Blocking Behavior . . . 171
Exception Management . . . 171
Encryption Service . . . 172
Encryption Service Overview . . . 172
Licensing Email Encryption Service . . . 173
Enabling the Secure Mail Policy . . . 174
Configuring Encryption Service . . . 174

Connection Management 182
Intrusion Prevention 182
Quality of Service 185
Manually Edit IP Address Lists 189

Reporting 191
Configure Known Networks 191
Scheduled Reports 193

Part 5. Appendixes

Interface Map 196

SonicWall Support 200
About This Document 201

Part 1

Introduction

- Introduction to Email Security

Introduction to Email Security

Welcome to the *SonicWall Email Security 9.1 Administration Guide*. This guide provides information about configuring and using the different features for all facets of the SonicWall Email Security product including on-premise appliances, virtual appliances, and hosted appliances. Differences between each are noted where applicable.

The SonicWall® Email Security can help you safeguard your data and meet compliance requirements. It can help protect your organization from outside attacks with effective virus, zombie, phishing and spam blocker by leveraging multiple-threat detection techniques. It can also help you better understand email usage, archive for compliance, efficiently perform e-discovery, and audit all mailboxes and access controls to prevent violations.

More information is provided in the following sections:

Topics	Applies to Appliance Solutions	Applies to Hosted Solutions
Description of Email Security	X	X
Available Module Licenses	X	X
Email Security Deployment Architecture for Appliances	X	
Other Planning Considerations for Email Security Appliances	X	
Hosted Email Security Overview		X
Activating the Hosted Email Security Service		X

Description of Email Security

Email-based communications are fundamental to effectively conducting business. Given the volume of worldwide emails and the continued growth each year, email continues to be a popular vector for a variety of threats. It offers hackers a vehicle to deliver a variety of vulnerabilities. These threat require a new set of features for detection and protection. SonicWall Email Security deploys a multi-layer solution dedicated to combatting emerging threats.

Advanced Threat Protection
Helps protect against ransomware and unknown malware that requires a sandbox to detect and protect against attacks.

Known Threat Protection
Screens malicious inbound emails using known anti-virus signatures and prevents your employees from sending viruses with outbound email. Using multiple virus-detection engines can improve coverage.

Phishing Protection
Incorporates advanced content analysis and dymanic blacklists to filter emails with malicious links.

Fraud Protection
Takes advantage of mail configurations such as SPF, DKIM and DMARC—along with pattern recognition and content analysis—to enforce validation of incoming messages.

Spam Protection	Uses multiple methods like allowed and blocked lists, pattern recognition and the ability to enable third-party blocked lists.
Data Loss Prevention	Allows encryption of sensitive emails and attachments for protection.

Email Security is supported on multiple platforms, including SonicWall Email Security appliances, as a software installation on Windows Server systems, and as a virtual appliance on VMware ESX® or VMware ESXI™ platforms. The system requirements for the various platforms are listed in the *SonicWall Email Security 9.1 Release Notes*.

ⓘ **NOTE:** Email Securityrequires that certain ports be left open to operate correctly. Refer to the *SonicWall Email Security 9.1 Release Notes* for the most recent list.

Available Module Licenses

Several modules are available for Email Security that must be licensed separately. For maximum effectiveness, all modules are recommended. The following licenses are available:

Email Protection (Anti-Spam and Anti-Phishing)	Protects against email spam and phishing attacks.
Email Anti-Virus (McAfee and SonicWall Time Zero)	Provides updates for McAfee anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
Email Anti-Virus (Kaspersky and SonicWall Time Zero)	Provides updates for Kaspersky anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
Email Anti-Virus (SonicWall Grid A/V and SonicWall Time Zero)	Provides updates for SonicWall Grid anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
Email Anti-Virus Cyren	Provides updates for Cyren anti-virus definitions and SonicWall Time Zero technology for immediate protection from new virus outbreaks.
Email Encryption Service	Features enabling the secure exchange of sensitive and confidential information. It includes predefined dictionaries to ensure proper protection.
Email Compliance Subscription	Provide license for compliance features. It includes predefined polices for easy compliance, allows multiple governance policies, identifies email for compliance policy enforcement, and provides compliance reporting and monitoring.
Capture for Email Security	Provides analysis of threats by examining their behavior in a managed environment (sandbox).

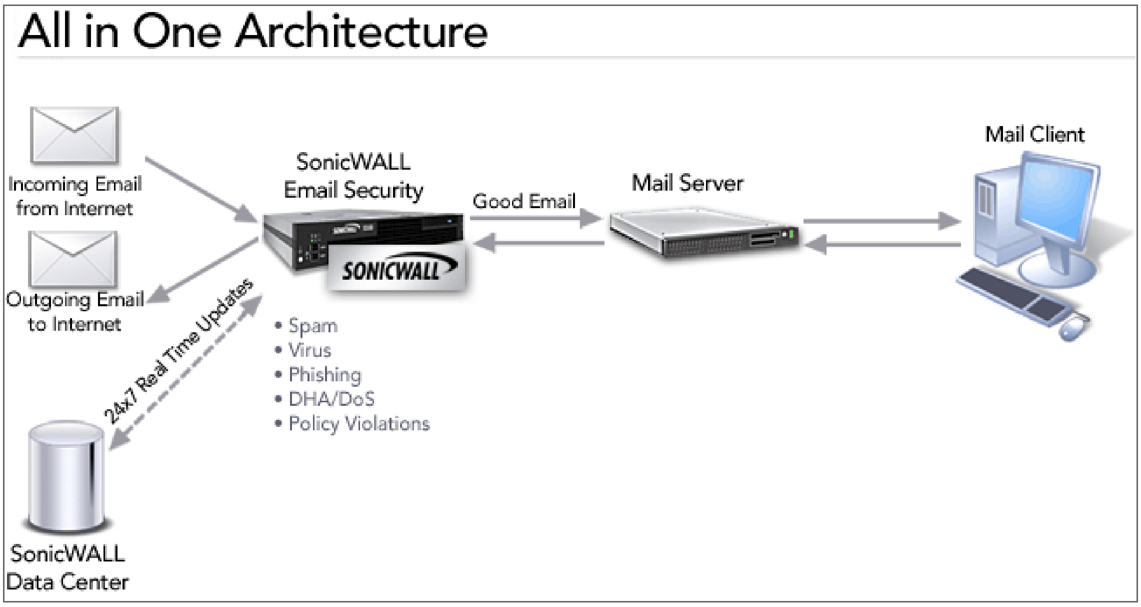
ⓘ **NOTE:** Email Continuity is automatically activated with the subscription for Hosted Email Security.

Email Security Deployment Architecture for Appliances

When planing an appliance-based deployment, Email Security can be configured in two ways: and *All in One* architecture or a *Split Network* architecture. Select the architecture before installation to avoid issues later.

All in One Architecture

In the All in One configuration, all machines running SonicWall Email Security analyze email, quarantine junk mail, and allow for management of administrator and user settings.

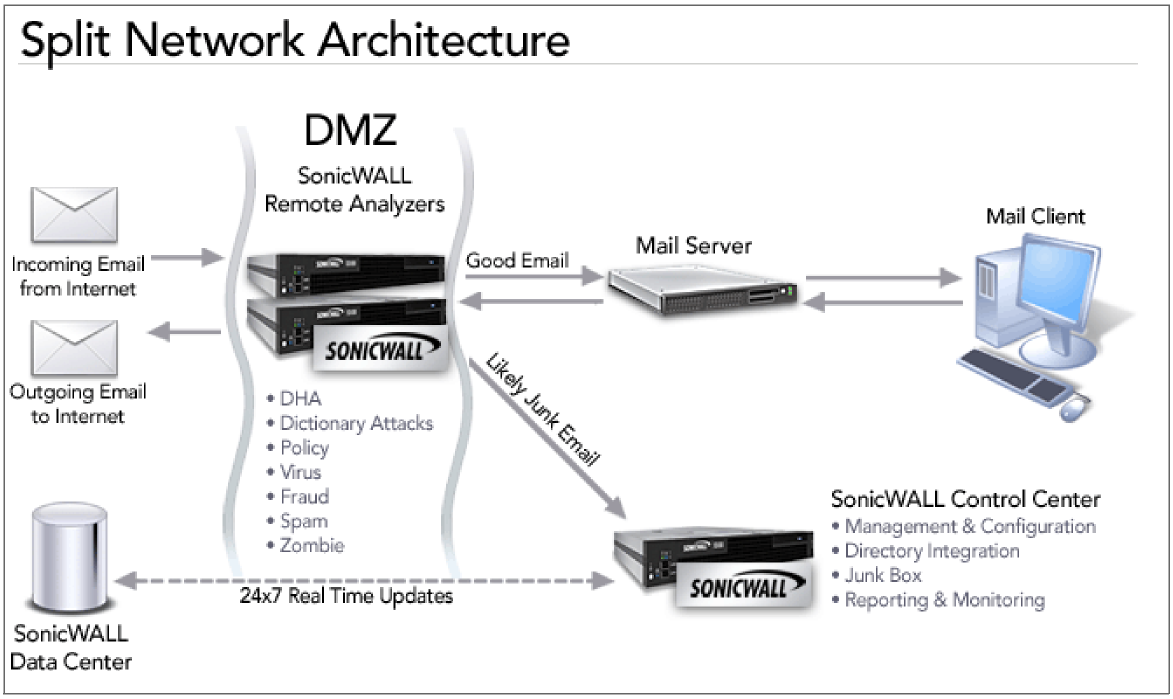


In an All in One configuration, you can also deploy multiple Email Security servers in a cluster setup wherein all of the gateways share the same configuration and data files. To set up such a cluster, begin by creating a shared directory, on either one of the SonicWall Email Security servers or on another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

Split Network Architecture

A Split Network configuration is comprised of two kinds of servers: Control Centers and Remote Analyzers. Typically, this configuration has one Control Center and multiple Remote Analyzers, but Control Center functions can be distributed between several Control Centers, where each device performs a specific job, like main control center functions, searching, or reporting. This allows the work to be balanced between the Control Centers and is sometimes refers to as a *cluster*. The Split configuration is designed for organizations with remote physical data centers.

The Split configuration allows you to manage SonicWall Email Security so that email messages are filtered in multiple remote locations through Remote Analyzers at those locations. The entire setup is centrally managed through the Control Center at a single location.



The Control Center controls, monitors, and communicates with all Remote Analyzers, in addition to storing or quarantining the junk email it receives from the Remote Analyzers. It manages all the data files, which 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 also queries LDAP servers to ensure valid users are logging in to SonicWall Email Security. 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 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.

Selecting an Architecture

SonicWall recommends the All in One configuration whenever possible because of its simplicity. Choose a Split Network configuration to support multiple physical data centers that can be centrally managed from a single location.

IMPORTANT: Make the deployment architecture decision before installing Email Security on the device. If you change the setup from a Control Center to a Remote Analyzer or vice versa, some data may be lost in the transition. There are no obvious advantages to changing a device.

Other Planning Considerations for Email Security Appliances

When planning an appliance-based solution, you need to consider other features:

- Email Security as the First-Touch/Last-Touch Server
- Proxy versus MTA
- Inbound and Outbound Email Flow

Email Security as the First-Touch/Last-Touch Server

In a deployment where Email Security is the first-touch and last-touch server in the DMZ, change your MX records to point to the SonicWall Email Security setup. Also, all the inbound and outbound connections for SonicWall Email Security (typically port 25) must be properly configured in your firewalls.

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

To configure Email Security as the first-touch/last-touch server:

1. Configure Email Security server with a static IP address on your DMZ.
2. In your firewall, add the private IP address for an inbound NAT Rule to an Internet-addressable IP address for TCP port 25 (SMTP).
3. In the public DNS server on the Internet, create an A record, mapping a name such as smtp.my_domain.com to the Internet-addressable IP address you assigned in step 2.
4. Update your email domain's MX record to point to the new record. You need to deploy the SonicWall Email Security for each MX record.

NOTE: SonicWall does not recommend a network topology where Email Security is not the first-touch and last-touch SMTP server because security mechanisms such as SPF and Connection Management cannot be used. If you opt for this topology, Email Security can be configured to be either an MTA or a proxy.

Proxy versus MTA

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

The SMTP proxy operates by connecting to a destination SMTP server before accepting messages from a sending SMTP server. Note that SMTP proxies can only send email to one server. Benefits of the SMTP proxy include:

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

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

- Routing messages to different domains based on MX records or LDAP mapping
- Queuing messages by temporarily storing messages on disk and retrying delivery later in case the receiving server is not ready
- Allowing Email Security to be the last touch mail gateway for outbound traffic

Inbound and Outbound Email Flow

Email Security can process both inbound and outbound email on the same machine. In an All in One configuration, each Email Security instance can support both inbound and outbound email. In a Split configuration, each Remote Analyzer can support both inbound and outbound email.

For inbound email flow, DNS configuration and firewall rules need to be set to direct email traffic to SonicWall Email Security. Whereas, for outbound email flow, the downstream email server must be configured to send all email to SonicWall Email Security (Smart Host Configuration).

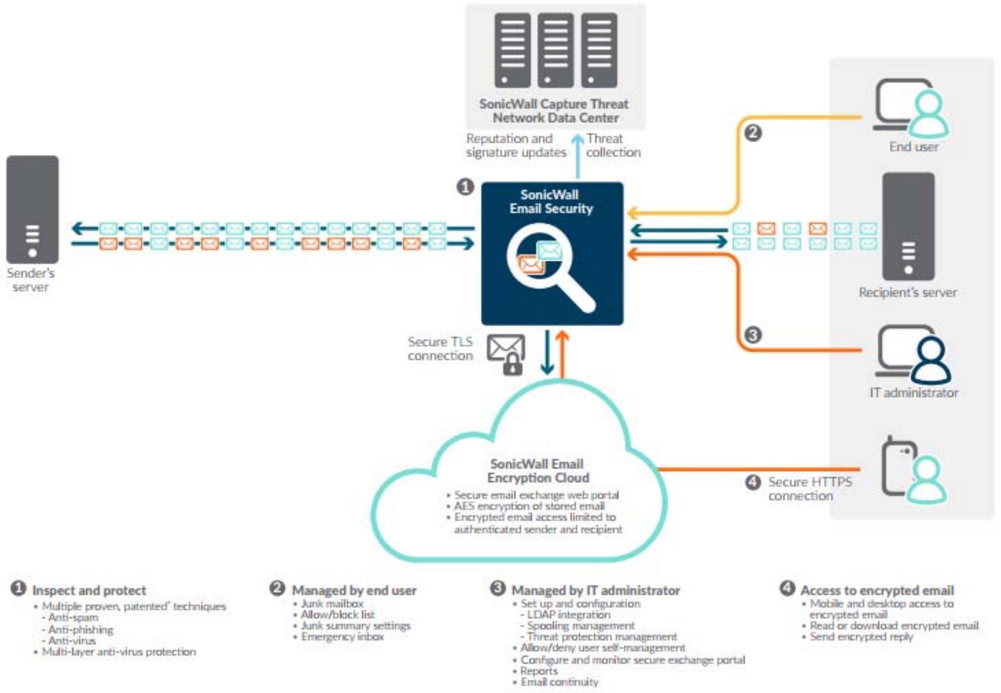
Hosted Email Security Overview

SonicWall Hosted Email Security (HES) offers superior, cloud-based protection from inbound and outbound threats, including ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses, at an affordable, predictable and flexible subscription price. At the same time, it minimizes upfront deployment time and costs, as well as ongoing administration expenses.

SonicWall Hosted Email Security includes advanced compliance scanning, management and, optionally, email encryption to prevent confidential data leaks, regulatory violations and to ensure the secure exchange of sensitive data. Policies may be configured at the organizational level, to scan outbound email content and attachments for sensitive data and route email for approval or encryption. Encrypted email can be tracked to confirm the time of receipt and time opened. A notification email is delivered to the recipient’s inbox with instructions to simply log into a secure portal to read or securely download the email.

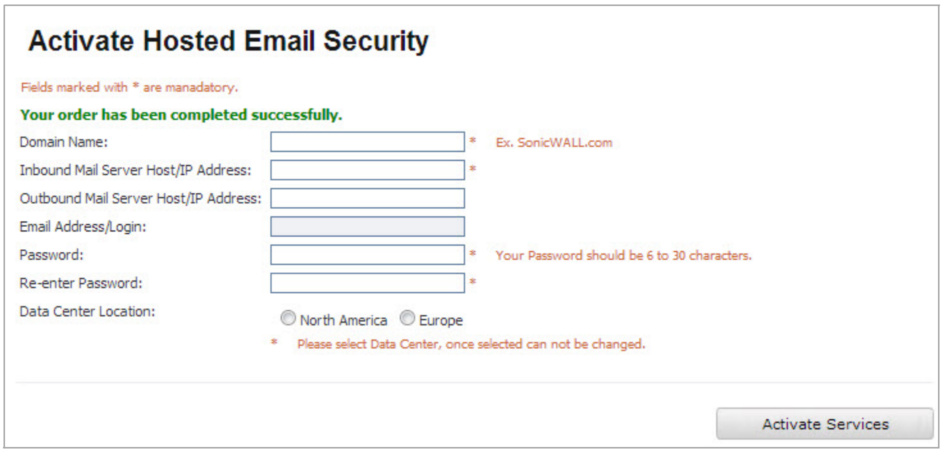
Other features include integration with Capture Advanced Threat Protection (ATP) and Email Continuity. Capture ATP gives you an effective and responsive defense against ransomware and zero-day attacks. Email Continuity provides cost-effective protection against planned or unplanned downtime events, whether your email servers are on-premises, hybrid environments or in the cloud.

The HES is cloud-based, with no additional client software necessary. Unlike competitive solutions, the encrypted email may be accessed and read from mobile devices or laptops.


SonicWall Capture Threat Network Data Center
Reputation and signature updates
Threat collection
1
SonicWall Email Security
Sender's server
2
End user
Recipient's server
3
IT administrator
Secure TLS connection
SonicWall Email Encryption Cloud
• Secure email exchange web portal
• AES encryption of stored email
• Encrypted email access limited to authenticated sender and recipient
4 Secure HTTPS connection
1 Inspect and protect
• Multiple proven, patented' techniques
- Anti-spam
- Anti-phishing
- Anti-virus
• Multi-layer anti-virus protection
2 Managed by end user
• Junk mailbox
• Allow/block list
• Junk summary settings
• Emergency inbox
3 Managed by IT administrator
• Set up and configuration
- LDAP integration
- Spooling management
- Threat protection management
• Allow/deny user self-management
• Configure and monitor secure exchange portal
• Reports
• Email continuity
4 Access to encrypted email
• Mobile and desktop access to encrypted email
• Read or download encrypted email
• Send encrypted reply

Activating the Hosted Email Security Service

After purchasing the hosted SonicWall Email Security service, you are directed to the activation screen.



Activate Hosted Email Security

Fields marked with * are manadatory.

Your order has been completed successfully.

Domain Name:	*	Ex. SonicWALL.com
Inbound Mail Server Host/IP Address:	*	
Outbound Mail Server Host/IP Address:		
Email Address/Login:		
Password:	*	Your Password should be 6 to 30 characters.
Re-enter Password:	*	
Data Center Location:	○ North America ○ Europe * Please select Data Center, once selected can not be changed.	

Specify the following fields, then click **Activate Services**:

- **Domain Name**—The primary domain name that is associated with your SonicWall SonicWall Email Security solution.
- **Inbound Mail Server Host / IP Address**—The IP address of the mail server hosting your user mailbox(es) for inbound messages.
- **Outbound Mail Server Host / IP Address**—The IP address provided during the provisioning stage of your Hosted Email Security solution. For example, if you registered the domain name soniclab.us.snwlhosted.com, then the Outbound Mail Server Host will be soniclab.outbound.snwlhosted.com.

- **Email Address / Login**—The email address or login name associated with your SonicWall Email Security account.
- **Password**—The password associated with your SonicWall Email Security account.
- **Re-enter Password**—The password you entered in the previous field.
- **Data Center Location**—Select the location of your data center. You are not able to change this option once it has been specified.

A message displays confirming successful activation and product registration. Click **Go to HES Console**.

Adding MX records

After activating your Hosted Email Security service, you may receive a message to replace your current MX records settings for inbound email messages.

Mail eXchange (MX) records specify the delivery route for email messages sent to your newly specified SonicWall Email Security domain name. The SonicWall Data Center can then create an internal MX record so mail is correctly routed to the specified domain.

Multiple MX records are assigned to your domain name. Each MX record designates a priority to organize the way your domain's mail servers receive incoming email messages; the lower the number, the higher the priority. You should always set back-up priority numbers in case the primary mail server fails or is down.

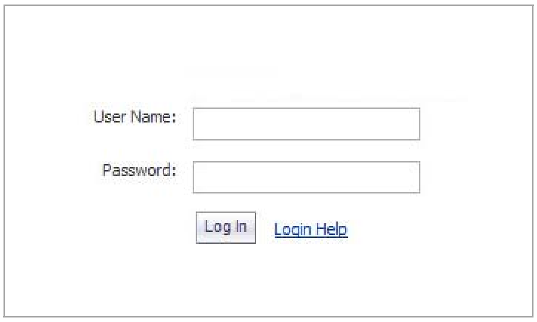
For example, a customer wishes to activate the domain name *example.com*. Since the SonicWall Data Center hosts *snwlhosted.com*, the domain then becomes *example.com.snwlhosted.com*. After an MX record is created, where the customer publishes example.com MX *example.com.snwlhosted.com*, SonicWall then publishes an A-record: *example.com.snwlhosted.com A 173.240.21.100*, where *173.240.21.100* is the IP address that SonicWall's hosted analyzers use to route emails sent to the jumbo.com domain. SonicWall publishes an A-record for outbound messages: *example.com.outbound.snwlhosted.com A 173.240.21.200.*

For outbound email messages, you need to configure the mail server hosting your user mailboxes for outbound messages to route all outbound emails to *example.com.outbound.snwlhosted.com*.

For more information regarding MX records, contact your ISP or refer to the Knowledge Base Article "How to set up your MX record after you activated Email Security Hosted Solution (SW9670)" located at: https://support.sonicwall.com/sonicwall-hosted-email-security/kb/sw9670.

Logging into the HES Console

After completing the activation process, click the **Go to HES Console** button to be directed to the Hosted Email Security console. You can also open a new Web browser and navigate to: https://www.snwlhosted.com. Enter the User Name and Password you configured during the Activation process, then click **Log In**.



NOTE: Because many of the screens are pop-up windows, configure your Web browser's pop-up blockers to allow pop-ups from your organization's server before using Hosted Email Security.

Part 2

Monitor

- Dashboard

2

Dashboard

On the default **MONITOR** view, the **Dashboard** summarizes Email Security at a glance. These charts are updated hourly and display the statistics for the last 24 hours and the views for each report can be customized.

Topics:

- Using the Reports
- Dashboard
- Event Summaries
- Policy and Compliance
- Appliance Health
- Current Status

Using the Reports

The reports shown on the **MONITOR** view can be managed and customized in a similar way across all the options.

Topics:

- Customizing the Display
- Configuring Chart Formats
- Filtering Chart Data

Customizing the Display

Several buttons are provided so you can customize what reports are shown for each of the options.

Button	Function
Add Charts	Allows you to add charts to be displayed. Click on the down arrow to select the report category, and then click on the report name you want to add.
Save View	Saves the view after you configured or made adjustments to your settings.
Reset to Default View	Resets the report view to the default settings.

Button	Function
Customize	Opens **Custom Reports** page so you can define the parameters for any report displayed. 1 Select the report to customize 2 Specify the date range for the report. 3 Select the units for how you want to list results: by the hour, day, week or month. 4 Enter the domains in the text field for **Report shows email sent to these domains**. Separate multiple domains with a comma, if left blank the report shows email sent to all domains. 5 Select delivery method. Choose **Display** to show data on the dashboard. Choose **Email to** to send the report to someone and provide the email address for the report recipient. 6 If you selected **Email to**, provide the following information in the text fields: • Name from which report is sent • Email address from which report is sent • Subject 7 Select **Generate This Report**.
Refresh Reports	Refreshes the data in the charts.

ⓘ **NOTE:** The **Appliance Health | Live Monitor** and either of the **Current Status** options are not customizable so these buttons don't appear in those tables.

Configuring Chart Formats

Each of the charts can be moved up and down or left and right in the display. Simply drag-and-drop the chart wherever you want it. You can also customize the data displayed in the charts by using the options provided. Select the tabs across the top of a chart to set the format and contents as described below:

To set the data style:	Select the data format you want: • Some data can be presented in **Stacked Chart**, **Line Chart**, or **Table** form. • Some data can only be presented in **Bar Chart** or **Table** form.
To set the time style:	Select one of the following: • **Hourly** • **Daily** • **Monthly**
To zoom:	Use the mouse to draw a box around the segment you want to zoom in on and the display adjusts to show only that portion of the data.
To undo zoom:	Click the **Undo Zoom** button to reset the view in that chart to the default setting. You might have to click the right-arrow to scroll over and make the **Undo Zoom** button visible.
To download data:	Click the download arrow allow you to download the chart in **PDF**, **JPEG**, or **CSV** formats.

To minimize or open the chart:	Use the double arrow head to minimize the chart when arrows are pointing up and opens the chart when the arrows are pointing down.
To close a chart and remove it from the view:	Click the close (X) button.

Filtering Chart Data

Since some charts display several types of data in a single view, you can customize what data shows in the charts. Click on an item listed in the legend. That item becomes grayed out and the data is removed from the display. To restore that item to the chart or table, click on the grayed out item and the data is returned.

Managing Table Formats

If you choose to show a table instead of a chart, use the following options to customize how the data is displayed, sorted or filtered.

Topics:

- Customizing Data Table Formats
- Sorting
- Search Filters

Customizing Data Table Formats

Most of the tables in the **MONITOR** view be customized by selecting which columns of data to show and what columns to omit.

To define the columns of data to display:

1 Go to any heading in a table and click on the down arrow to see the drop box.

2 Navigate to **Columns** to see what columns of data are available for that table.

3 Check the box by those columns you want to appear and uncheck the boxes you want to hide. The table reconfigures itself in response to each action.

Sorting

The columns in the data table can be sorted in sorted in ascending or descending order.

To sort a column:

1 Click in a the column you want to sort. A small arrowhead appears in the column. The arrowhead points up to indicate ascending order and down to indicate descending order.

2 Click in the column again to change the direction of the arrowhead. The data refreshes immediately to reflect the choice you made.

In the drop down menus for the column headings, you can also chose **Sort Ascending** or **Sort Descending**.

Search Filters

Search filters have been integrated into the reporting tool so you can show just part of the data. Filters can be applied to multiple columns, but not all columns have the option to be filtered. The filtering is performed directly on the data that's displayed.

To filter data in a column:

1. Select the down arrow next to the column title.
2. Highlight the **Filter** option.
3. Depending on the options provided, do one of the following:
   - Type in a string of text to filter on.
   - Choose one or more filters from a list of pre-populated options.

   The results of any filtering are immediately shown in the data table.

Dashboard

The **Dashboard** displays a series of reports that shows at a glance what Email Security is doing. You can customize the **Dashboard** view by adding or deleting charts or by customizing how the data is displayed. The predefined reports belonging to the **Dashboard** category are described in the following table.

ⓘ | **NOTE:** You can add reports from any of the other categories to the **Dashboard** view.

Dashboard Reports

Report Name	Description
Inbound Good vs. Junk	Displays the number of good messages versus junk messages received in an hour in inbound email traffic. Junk is comprised of spam, likely spam, phishing, likely phishing, viruses, likely viruses, policy events, directory harvest attacks (DHA), and rejected connections (CM). Rejected connections are those deliberately dropped by Email Security because of greylisting, IP reputation, and other features provided on the Connection Management page.
Outbound Good vs. Junk	Displays the total number of outbound messages processed by Email Security along with the total number of junk messages and good messages.
Junk Email Breakdown	Displays Junk email broken down into the following categories: • Spam (Spam and Likely Spam) • Phishing (Phishing and Likely Phishing) • Virus (Virus and Likely Virus) • Policy • Directory Harvest Attacks (DHA) • Connection Management (CM) **NOTE:** The Junk Email Breakdown chart displays only those categories of junk email that are filtered by your organization.
Top Spam Recipients	Displays the volume of spam received by the top 12 recipients in your organization.

Dashboard Reports

Report Name	Description
Spam Caught	Displays the number of email messages that are definitely Spam compared to the number that are Likely Spam.
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.
Top Outbound Email Senders	Displays what percentage of the processor is used, as sampled every fifteen minutes. This chart increments in processor percentage. Use this chart to judge whether you have sufficient processor power for your needs. If you are viewing a Remote Analyzer, this is one of the available charts.
Top Connecting IP Addresses	Displays what percentage of the processor is used, as sampled every fifteen minutes. This chart increments in processor percentage. Use this chart to judge whether you have sufficient processor power for your needs. If you are viewing a Remote Analyzer, this is one of the available charts.
System Load Average (15 min)	Displays the system load as sampled every fifteen minutes. This chart increments in thousands of messages. Use this chart to judge your peak system load, and your loads through the day. If you are viewing a Remote Analyzer, this is one of the available charts.
System % Processor Time (15 min)	Displays what percentage of the processor is used, as sampled every fifteen minutes. This chart increments in processor percentage. Use this chart to judge whether you have sufficient processor power for your needs. If you are viewing a Remote Analyzer, this is one of the available charts.
Total Files Scanned	Shows the total number of files scanned each hour.

Event Summaries

Event Summaries provides several predefined groupings. Each of these groupings can be customized to suit your needs as described in Using the Reports.

Topics:

- All Event Connections
- Anti-Spam
- Anti-Phishing
- Anti-Virus
- Anti-Spoof
- Directory Harvest
- Capture ATP

All Event Connections

Email Security provides connection management to reduce the traffic your system must analyze and automatically rejects connections from bad IP addresses. The pre-configured reports grouped in **All Event Connections** shows comparisons of the data processed through the connection management features.

Reports for All Event Connections

Report Name	Description
Allowed vs. Blocked Connections	Reports the number of SMTP connections that were allowed versus those that were blocked, deferred, or throttled as a result of the Connection Management settings. The default is the Daily view.
Blocked Connections Breakdown	Categorizes the SMTP connections that have been acted upon as a result of the Connection Management settings. The categories are: • REPTN (Grid Network IP Reputation) • Blocked • Deferred • Greylisted • TCNXN (throttled based on connection) • TMSGS (throttled based on message) • TRCPT (throttled based on recipient commands) The default is Daily view.
Greylisted Connections	Displays the number of SMTP connections that were blocked due to the Greylisting component of your Connection Management settings versus the number of connections that were later retired and allowed. The default is Daily view.
Top Spam Countries	Lists the countries that the most spam comes from and the volume of connections for each.

Anti-Spam

Email Security provides the following reports specific to the **Anti-Spam** function:

Anti-Spam Reports

Report Name	Description
Spam Caught	The Spam Caught report displays the number of messages filtered by SonicWall Email Security that are definitely Spam compared to the amount that are Likely Spam. This report also gives a percentage breakdown.
Top Spam Domains	The Top Spam Domains report presents the domains or IP addresses that send the most spam to your organization. **NOTE:** This report only contains useful information if your Email Security server is running as “first touch.” If your server is not first touch, the IP addresses displayed are those of the server that routes mail to the Email Security server.
Top Spam Recipients	The Top Spam Recipients report lists the email addresses in your organization that receive the most spam.

Anti-Phishing

Phishing messages are an especially pernicious form of fraud that use email with fraudulent content to steal consumers' personal identity data and financial account credentials. This report displays the number of messages that were identified as Phishing Attacks and Likely Phishing Attacks.

Anti-Virus

The Anti-Virus reports allows you to view the number of viruses detected by the SonicWall Email Security.

Anti-Virus Reports

Report Name	Description
Inbound Viruses Caught	The Inbound Viruses Caught report displays the number of viruses caught in inbound email traffic. The default is the Daily view.
Top Inbound Viruses	The Top Inbound Viruses report lists the names of the viruses that have been detected most often in inbound email traffic sent through Email Security and the amount of times each virus has been detected. The default is the Monthly view
Outbound Viruses Caught	The Outbound Viruses Caught report displays the number of viruses caught in outbound email traffic. The default is he Daily view.
Top Outbound Viruses	The Top Outbound Viruses report lists the names of the viruses that have been detected most often in outbound email traffic sent through Email Security and the amount of times each virus has been detected. The default is the Monthly view.

Anti-Spoof

The Anti-Spoof reports provide summary and detailed reports on the types of anti-spoof messages detected.

Anti-Spoof Reports

Report Name	Description
Likely Spoof Messages	Displays the total number of Likely Spoof messages caught in inbound email traffic.
Likely Spoof Message Breakdown	Shows the breakdown of the Likely Spoof messages according the categories used to detected them in the inbound email traffic.
SPF Breakdown	Shows the breakdown of Likely Spoof message that were detected using SPF parameters.
DKIM Breakdown	Shows the breakdown of Likely Spoof message that were detected using DKIM parameters.
DMARC Breakdown	Shows the breakdown of Likely Spoof message that were detected using SPF and DMARC parameters.

Directory Harvest

SonicWall Email Security provides protection against directory attacks. The directory protection reports give more information on the directory attacks targeted towards your organization.

Directory Protection Reports

Report Name	Description
Number of Directory Harvest Attacks	Displays the number of messages with invalid email addresses that were sent to your organization. If this number is large, your organization may be experiencing one or more Directory Harvest Attacks in which spammers try to harvest a list of all your email addresses. The default is the Daily view.
Top DHA Sending Domains	Shows the IP addresses from which the most frequent Directory Harvest Attacks originate and the number of invalid recipient addresses in those attacks. The default is the Monthly view.

Capture ATP

The Capture ATP reports provides about the quantity and types of files scanned.

Capture ATP Reports

Report Name	Descriptions
Total Files Scanned	Shows the total number of files scanned each hour.
File Type Scanned	Shows how many of each type of file was scanned. Data is either shown in a pie chart or a table.
Malicious File Type	Shows how many of each kind of malicious file was scanned. Data is either shown in a pie chart or a table.

Policy and Compliance

The pre-configured reports grouped in **Policy and Compliance** shows comparisons of the data processed through policies and encryption.

Topics:

- Policy
- Compliance
- Encryption

Policy

The **Policy** group includes the reports that are relevant to policy filters in Email Security.

Policy Management Reports

Report Name	Description
Inbound Policies Filtered	Displays the total number of inbound email messages that Email Security has filtered based on your configured policies.
Top Inbound Policies	Displays the policy filter names that are triggered most often in inbound email traffic.

Policy Management Reports

Report Name	Description
Outbound Policies Filtered	Displays the total number of outbound messages that Email Security has filtered based on your configured policies.
Top Outbound Policies	Displays the policy filter names that are triggered most often in outbound email traffic.

Compliance

The **Compliance** option groups various reports that are relevant to compliance in Email Security.

Compliance Reports

Report Name	Description
Inbound Messages Decrypted	Displays the number of inbound messages decrypted relative to time.
Inbound Messages Archived	Displays the total number of inbound messages that were archived relative to time.
Top Inbound Approval Boxes	Lists the approval boxes in which inbound email messages sent through Email Security are stored most often. This report also displays the amount of messages that are stored in each approval box.
Outbound Messages Encrypted	Displays the number of outbound messages encrypted relative to time.
Outbound Messages Archived	Displays the total number of outbound messages that were archived relative to time.
Top Outbound Approval Boxes	Lists the approval boxes in which outbound email messages sent through Email Security are stored most often. This report also displays the amount of messages that are stored in each approval box.

Encryption

The **Encryption** option shows only one report: **Outbound vs. Encrypted Email**. This report displays the total number of outbound messages as compared to the number of messages sent as [SECURE] through the encryption service.

Appliance Health

The reports grouped under Appliance Health are specific to the Email Security appliance.

Topics:

- Live Monitor
- Performance Metrics
- LDAP Users

Live Monitor

The **Live Monitor** provides real-time information on the flow of email passing through the SonicWall Email Security system. **Message Throughput History** shows the number of emails processed by this server per second. **Message Bandwidth History** shows the total bandwidth used for email in bytes per second. The bandwidth is the sum of the sizes of all the messages passing through this SonicWall Email Security server per second.

ⓘ **NOTE:** The Live Monitor charts are not available for Control Centers in a split configuration.

Performance Metrics

The **Performance Metrics** page provides real-time system information on the SonicWall Email Security system. Performance monitoring allows administrators to monitor various metrics over a selectable period of time (Last Hour, 1 Day, or 7 Days). The charts and data can be downloaded for sharing.

Performance Metrics Reports

Report Name	Description
% Processor Time	The percentage of elapsed time that all process threads used to execute instructions.
Handle Count	The total number of handles this process currently has open. This number is the sum of the handles currently open by each thread in this process.
Private Bytes (kB)	Private Bytes is the current size, in kilobytes, of memory that this process has allocated which cannot be shared with other processes.
Thread Count	The number of threads currently active in this process. Every running process has at least one thread.
Virtual Bytes (kB)	The current size, in kilobytes, of the virtual address space the process is using. Use of virtual address space does not imply corresponding use of either disk or main memory pages. Virtual space is finite, and the process can limit its ability to load libraries.
% Disk Time	The percentage of elapsed time that the selected disk drive was busy servicing read or write requests.
% IO Wait Time	The percentage of elapsed time that all processes are in a wait state before starting the next action.
% Idle Time	The percentage of elapsed time that all processes are sitting in a state of idle and experiencing no amount of performance load.
Available Byte (kB)	The amount of physical memory available to processes running on the computer. This is calculated by adding the amount of space on the Zeroed, Free, and Standby memory lists.
Avg Load 1 min	The average system load, over time, measured in 1 minute intervals.
Avg Load 15 min	The average system load, over time, measured in 15 minute intervals.
Avg Load 5 min	The average system load, over time, measured in 5 minute intervals.
Avg Disk Bytes/Transfer	The time, in seconds, of the average disk transfer. The default is shown as a stacked line chart over time.
Avg Disk Queue Length	The average number of read and write requests queued for the selected disk during the sample interval. The default is shown as a stacked line chart over time.
Buffer Bytes (kB)	The amount of memory available for buffering before data transfer.

Performance Metrics Reports

Report Name	Description
Cache Bytes (kB)	The sum of the Memory\\System Cache Resident Bytes, Memory\\System Driver Resident Bytes, Memory\\System Code Resident Bytes, and Memory\\Pool Paged Resident Bytes counters. The default is shown as a stacked line chart over time.
Committed Bytes (kB)	The amount of committed virtual memory. Committed memory is the physical memory which has space reserved on the disk paging file(s). Each physical drive can have one or more paging files.
Connection Failures	The number of times TCP connections have made a direct transition to the CLOSED state from the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Connections Established	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Connections Reset	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Install Dir Free Space	The amount of free space available in the Install directory.
Segment Retransmitted/sec	The rate at which segments are retransmitted, that is, segments transmitted containing one or more previously transmitted bytes.
Segments/sec	The rate at which TCP segments are sent or received using the TCP protocol.
Swap Available Bytes (kB)	The amount of space that is available for swap space.
Queue Size	The number of message waiting in MTA queue. For this statistic to have a value, Email Security should have been set up in MTA (i.e., SmartHost) mode.

ⓘ **NOTE:** Some report names are only available on appliance-based solutions: % IO Wait Time, Buffer Bytes (kB), Install Dir Free Space, and Swap Available Bytes (kB).

LDAP Users

The LDAP Users provides statistics as a function of the number of users per domain or organization. With it, you can determine if all these users are license compliant. The following views are available for selection:

- Domain Person vs. Group Email Addresses
- Domain Primary vs. Alias Email Addresses
- Organization Person vs. Group Email Addresses
- Organization Primary vs. Alias Emails Addresses

Current Status

Current Status shows system and MTA status of the Email Security appliance.

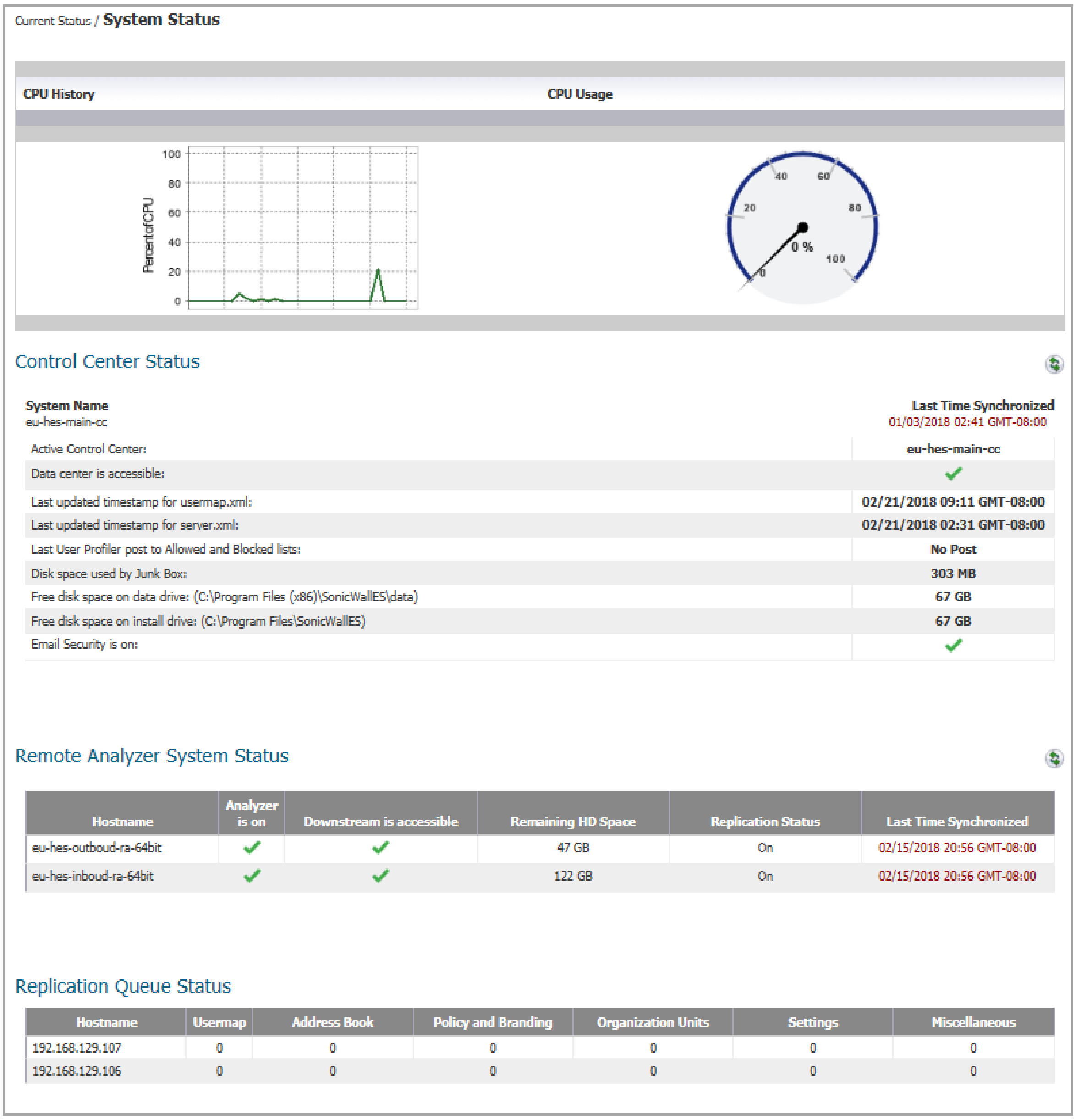
Topics:

- System Status
- MTA Status

System Status

The **Current Status | System Status** window shows the live status of the Email Security system, including Remote Analyzers if you have a Split configuration. It also shows the status of connections with other systems that Email Security needs to communicate with. A green check icon indicates the system is functioning as expected, while a red X icon indicates the system is not. Click on the refresh button at anytime to refresh the data.

The lower part of the System Status table (the Control Center Status and Remote Analyzer System Status tables in a Split configuration) shows system statistics, including the disk space used by the Junk Box, free disk space on the data drive, and free disk space on the install drive. Replication Queue Status is also shown at the bottom of the window.



Current Status / **System Status**

Control Center Status

System Name eu-hes-main-cc	**Last Time Synchronized** 01/03/2018 02:41 GMT-08:00
Active Control Center:	eu-hes-main-cc
Data center is accessible:	✓
Last updated timestamp for usermap.xml:	02/21/2018 09:11 GMT-08:00
Last updated timestamp for server.xml:	02/21/2018 02:31 GMT-08:00
Last User Profiler post to Allowed and Blocked lists:	No Post
Disk space used by Junk Box:	303 MB
Free disk space on data drive: (C:\Program Files (x86)\SonicWallES\data)	67 GB
Free disk space on install drive: (C:\Program Files\SonicWallES)	67 GB
Email Security is on:	✓

Remote Analyzer System Status

Hostname	Analyzer is on	Downstream is accessible	Remaining HD Space	Replication Status	Last Time Synchronized
eu-hes-outboud-ra-64bit	✓	✓	47 GB	On	02/15/2018 20:56 GMT-08:00
eu-hes-inboud-ra-64bit	✓	✓	122 GB	On	02/15/2018 20:56 GMT-08:00

Replication Queue Status

Hostname	Usermap	Address Book	Policy and Branding	Organization Units	Settings	Miscellaneous
192.168.129.107	0	0	0	0	0	0
192.168.129.106	0	0	0	0	0	0

In a Split configuration, a subset of system status data is shown for the Remote Analyzers. You can see remaining hard disk space, replication status, replication queue size, and last time synchronized.

NOTE: The System Status view cannot be customized or reconfigured.

MTA Status

The **Current Status | MTA Status** page displays detailed status of the mail transfer agent (MTA) if any paths have been configured to act as MTAs. At the top of the page, the **Total Messages in MTA Queues** is shown as a link.

To see MTA Queue Detailed Info:

1 Click on the link for **Total Message in MTA Queues**. The MTA Queue Detailed Info displays.

2 Click on the **Deliver All Queued Messages** button if you want the MTA to attempt delivery right away.

This attempt may take a minute or so to complete, and it may not succeed for all messages. A delivery attempt temporarily empties the message queue, and undeliverable messages eventually reappear in the queue.

3 Click the **Refresh** button if you want to see updated status.

The contents of the message queues change continually as messages pass through the MTA. The email messages displayed in this window represent the contents of the queue at a moment in time. Clicking the Refresh button cause the window to take another snapshot of the message queue. Refreshing the contents of the window does not affect mail flow.

MTA Totals by Host

The **MTA Totals by Host** section displays additional information about message totals sorted by host.

Host	This column shows the host names.
Service Status	MTA service on this device is on (green check icon) or off (red X icon)
Messages delivered in last hour	This column shows the number of messages delivered by the MTA in the last hour.
Messages in all queues	This column shows the sum of the messages in the queues of all the MTAs. If service status is off, it shows N/A.
Message recipients in all queues	This column shows the number of messages recipients in the queues of all the MTAs. Click on Show Detail to go to the MTA queue Detailed Info page. If service status is off, it shows N/A.

MTA Status on Inbound/Outbound Paths

If one or more paths are configured to act as MTAs, these two sections provide additional information about these paths. The columns and the values they represent are the same for each table:

Host	This column shows the host names.
(src/listen/dest))	*src* is the source IP contacting path; the IP address of a machine that is allowed to connect to and relay email through this path. *listen* is the IP address and port on which this path listens for connections. *dest* is the destination to which this path routes email.
Number of message recipients in queue	This column lists the number of messages in the queue if the path is an MTA. If it is a proxy, messages are not queued and this column will indicate N/A.

To see details about the messages in a queue, click the Show Details link for that queue. To see details for messages on a particular server, you must log in to the SonicWall appliance on that server.

Part 3

Investigate

- INVESTIGATE | Junk Box
- Email Continuity (for Hosted Email Security only)
- Logs
- Tools

3

INVESTIGATE | Junk Box

The default on the **INVESTIGATE** view is the inbound Junk Box data table. You can review and process email messages that have been quarantined in the Junk Box. Through analysis, these emails have been flagged as spam, virus-infected, policy violations, or phishing attempts. After review you can unjunk a falsely identified message. When you or the recipient unjunks an incoming message, Email Security adds the sender of the message to the recipient's Allowed list and delivers the email to the recipient.

To configure the Junk Box, go to the **MANAGE** view and select **System Setup | Junk Box > Message Management**. To set up email notifications about email quarantined in the Junk Box, go to the **MANAGE** view and select **System Setup | Junk Box > Summary Notifications**. Refer to Junk Box for more information.

Topics:

- Using the Junk Box
- Managing Junk Box Messages

Using the Junk Box

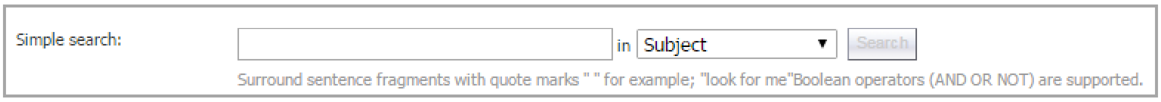
The information in the Junk Box table can be managed and customized much like other tables in Email Security.

Topics:

- Simple Searching for Data
- Filtering Table Data
- Customizing the Display

Simple Searching for Data

At the top of the page, a simple search tool is offered to search for specific strings or sentence fragments. The search parameters are applied directly on the data in the table. Surround sentence fragments with quotes (for example: "look for me"). Boolean operators AND, OR, and NOT are also supported.



Simple search: in Subject

Surround sentence fragments with quote marks " " for example; "look for me"Boolean operators (AND OR NOT) are supported.

To perform a simple search:

1. Enter the text you want to search for in the **Simple search** field.
2. Select the field to search on from the drop-down menu. Choose from **Subject**, **To**, **From**, or **Unique Message ID**.

3 Click on **Search**. The results are displayed in the data table.

4 Click **Clear Filters** to see all the data.

Filtering Table Data

Advanced search filters are performed directly on the data that's displayed. Select the down arrow next to the column title to filter the data. Some columns are searchable by typing in a string of text to search on. Other columns allow you to choose one or more filters from a list of pre-populated options. You can also filter more than one column at a time. The results of any filtering are immediately shown in the data table.

Click the **Clear Filters** button to see all the data in the table.

Customizing the Display

Several button are provided so you can customize what data is shown in the Junk Box table. The options are the same for both **Inbound** and **Outbound** tables.

Button name	Definition
Add Columns	Select Add Columns to get the drop down menu. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filers	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns.
Reset to Default View	Resets the data table back to the default view.
Settings	Takes you to **System Setup | Junk Box > Message Management** on the **MANAGE** view to customize the setting that defines what appears in the Junk Box.

Managing Junk Box Messages

The default view displays inbound messages. Click on the **Outbound** button to see the outbound messages. Click the **Inbound** button to return to the inbound view. The messages you see in the Junk Box are based on the options selected in **System Setup | Junk Box | Message Management** in the **MANAGE** view.

Inbound message management detects messages sent to users in your organization from people outside of your organization. Outbound message management detects messages sent by users in your organization that contain viruses, likely viruses, and message that trigger policy alerts. Outbound message management also quarantines outbound spam and phishing.

ⓘ **NOTE:** Messages stored in the Outbound Junk Box cannot be reviewed by users. They cannot see their messages in their Junk Box Summary notifications. Only administrators can review and process messages quarantined in the Outbound Junk Box.

You can take several actions after reviewing the messages in the Junk Box. See the table below for a description of the buttons at the top left of the data table.

Button name	Definition
Delete	Deletes the selected messages. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want. Then click on **Delete**.
Unjunk	Allows you to remove a valid email message from the Junk Box. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want and click on the **Unjunk** button.
Send Copy To	Sends selected messages to a specific recipient. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want.
Refresh	Refreshes the data in the table.

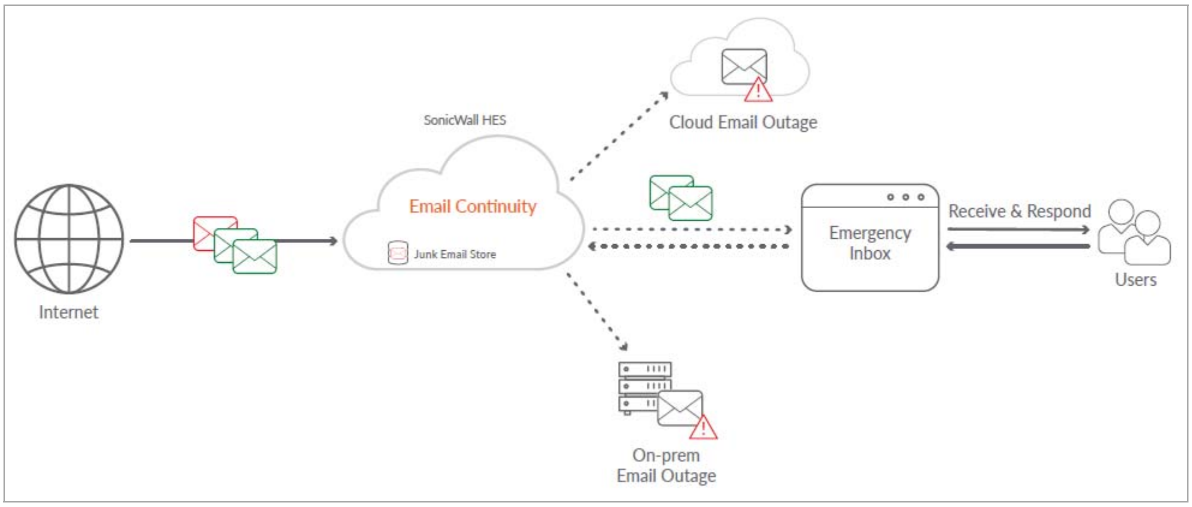
The size of the junk box can grow rapidly. By default, the messages are stored in the junk box for 30 days and deleted after that. You may need to customize this setting, depending on your organization’s policies and the storage capacity on the shared data directory where messages are stored.

4

Email Continuity

SonicWall Hosted Email Security delivers Email Continuity against planned or unplanned downtime events, whether your email servers are on-premises, hybrid environments or in the cloud. Continuity service is an add-on subscription that delivers email to end users.

> **NOTE:** Email Continuity is only offered on hosted solutions at this time. It is not available on appliance-based solutions.



Email Continuity is automatically activated with the subscription. When an email outage occurs, the administrator is notified and users can access emails through the emergency inbox. During an outage SonicWall HES acts as the email server. All suspicious emails are quarantined and only safe email is delivered.

Once the primary email server is back online, the Email Continuity servers automatically reconnects and synchronizes all email sent or received during the outage.

Topics:

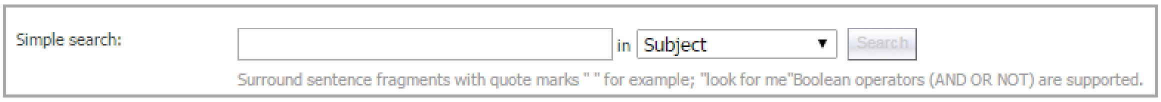
- Managing the Email Tables
- Inbox
- Outbox
- Sent

Managing the Email Tables

The Email Continuity tables are much like any other data table in Email Security. You can search, filter, or change the table appearance.

Simple Search for Data

At the top of each data table, a simple search tool is offered to search for specific strings or sentence fragments. The search parameters are applied directly on the data in the table. Surround sentence fragments with quotes (for example: “look for me”). Boolean operators AND, OR, and NOT are also supported.



Surround sentence fragments with quote marks " " for example; "look for me"Boolean operators (AND OR NOT) are supported.

To perform a simple search:

1. Enter the text you want to search for in the **Simple search** field.
2. Select the field to search on from the drop-down menu. Choose from **Subject**, **To**, **From**, or **Unique Message ID**.
3. Click on **Search**. The results are displayed in the data table.
4. Click **Clear Filters** to see all the available data again.

Filtering Table Data

Advanced search filters are performed directly on the data that's displayed. Select the down arrow next to the column title to filter the data. Some columns are searchable by typing in a string of text to search on. Other columns allow you to choose one or more filters from a list of pre-populated options. You can also filter more than one column at a time. The results of any filtering are immediately shown in the data table.

Click the **Clear Filters** button to display all the available data again.

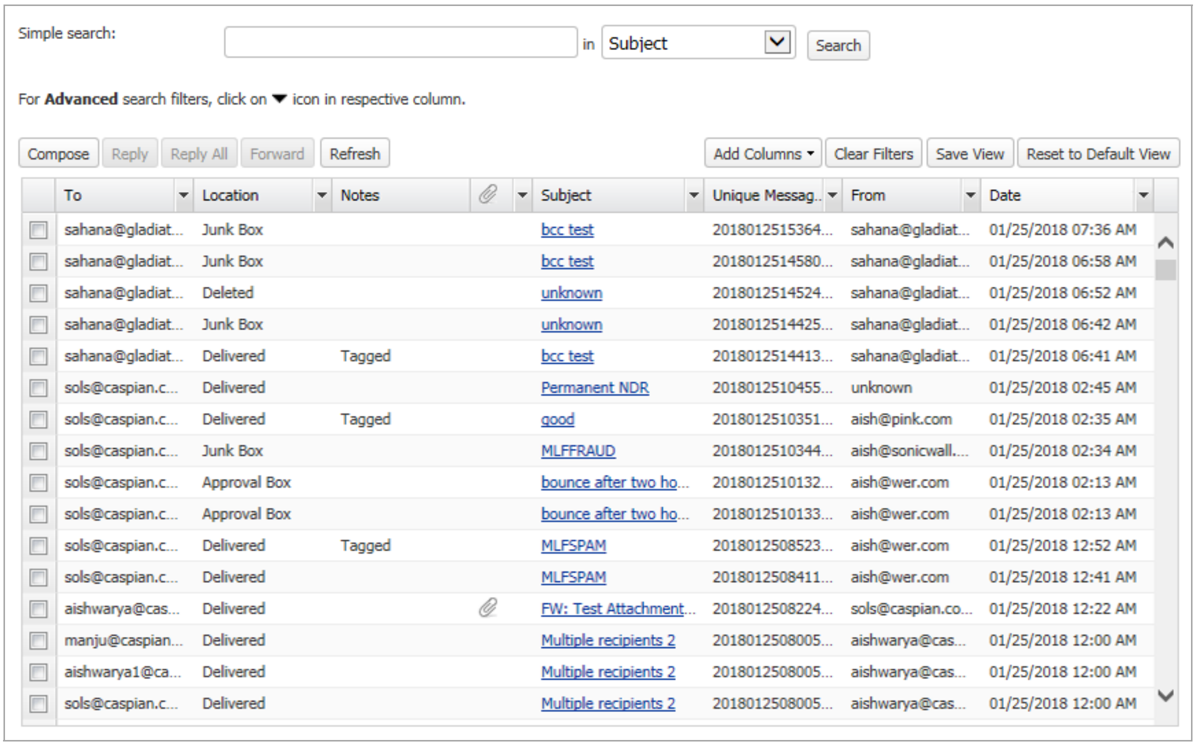
Customizing the Display

Several button are provided so you can customize what data is shown in the Email Continuity tables. The options are the same for **Inbox**, **Outbox** ,and tables.

Button name	Definition
Add Columns	Select **Add Columns** to see the drop down list. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filters	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns or setting filters.
Reset to Default View	Resets the data table back to the default view.
Settings	Opens a window you can set the number of days the email is retained for continuity. (This is also referred to as the time before the an email ages out of the system.) Confirmation is provided if the update is successful.

Inbox

Email Continuity | Inbox displays all the good messages received on the inbound path prior to the interruption on the primary email server. These represent all good email messages for the past 7 days.



Simple search: in Subject

For **Advanced** search filters, click on ▼ icon in respective column.

□	To	Location	Notes	📎	Subject	Unique Messag..	From	Date
□	sahana@gladiat...	Junk Box			bcc test	2018012515364...	sahana@gladiat...	01/25/2018 07:36 AM
□	sahana@gladiat...	Junk Box			bcc test	2018012514580...	sahana@gladiat...	01/25/2018 06:58 AM
□	sahana@gladiat...	Deleted			unknown	2018012514524...	sahana@gladiat...	01/25/2018 06:52 AM
□	sahana@gladiat...	Junk Box			unknown	2018012514425...	sahana@gladiat...	01/25/2018 06:42 AM
□	sahana@gladiat...	Delivered	Tagged		bcc test	2018012514413...	sahana@gladiat...	01/25/2018 06:41 AM
□	sols@caspian.c...	Delivered			Permanent NDR	2018012510455...	unknown	01/25/2018 02:45 AM
□	sols@caspian.c...	Delivered	Tagged		good	2018012510351...	aish@pink.com	01/25/2018 02:35 AM
□	sols@caspian.c...	Junk Box			MLFFRAUD	2018012510344...	aish@sonicwall....	01/25/2018 02:34 AM
□	sols@caspian.c...	Approval Box			bounce after two ho...	2018012510132...	aish@wer.com	01/25/2018 02:13 AM
□	sols@caspian.c...	Approval Box			bounce after two ho...	2018012510133...	aish@wer.com	01/25/2018 02:13 AM
□	sols@caspian.c...	Delivered	Tagged		MLFSPAM	2018012508523...	aish@wer.com	01/25/2018 12:52 AM
□	sols@caspian.c...	Delivered			MLFSPAM	2018012508411...	aish@wer.com	01/25/2018 12:41 AM
□	aishwarya@cas...	Delivered		📎	FW: Test Attachment...	2018012508224...	sols@caspian.co...	01/25/2018 12:22 AM
□	manju@caspian...	Delivered			Multiple recipients 2	2018012508005...	aishwarya@cas...	01/25/2018 12:00 AM
□	aishwarya1@ca...	Delivered			Multiple recipients 2	2018012508005...	aishwarya@cas...	01/25/2018 12:00 AM
□	sols@caspian.c...	Delivered			Multiple recipients 2	2018012508005...	aishwarya@cas...	01/25/2018 12:00 AM

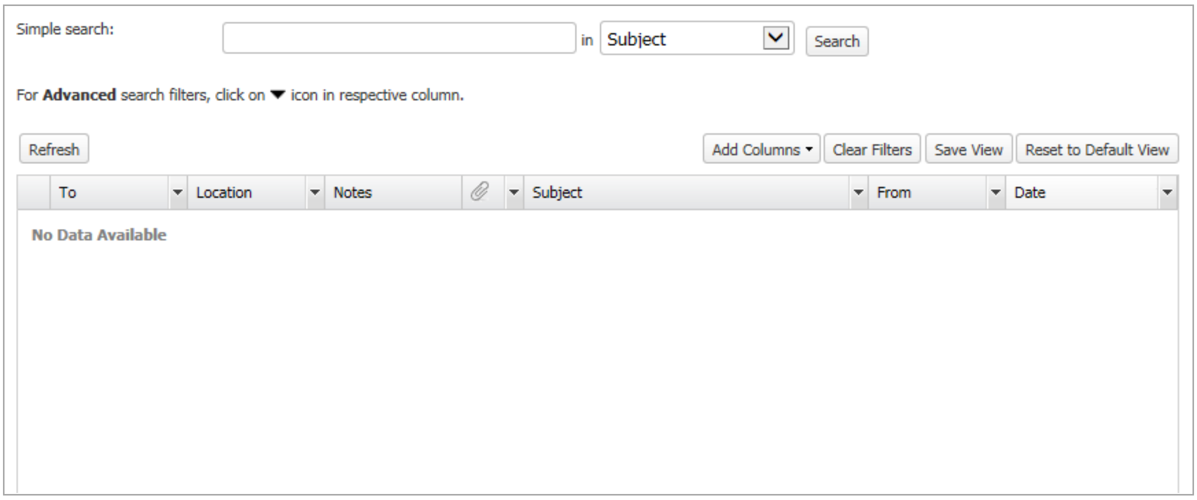
Use the buttons at the top of the table to manage the inbox:

Button	Definition
Compose	Click on the **Compose** button to send a new email. Click **Send** when email is ready.
Reply	Check the box by the email you want to respond to and click **Reply**. Type the message and click **Send** when email is ready.
Reply All	Check the box by the email where you want to respond to everyone and click **Reply All**. Type the message and click **Send** when email is ready.
Forward	Check the box by the email where you want to forward to another user and click **Forward**. Type the message and click **Send** when email is ready.
Refresh	Click Refresh to update the data in the inbox.

Refer to Managing the Email Tables for information on how to customize the table views.

Outbox

Email Continuity | Outbox displays all the messages that are currently in the queue, waiting to be delivered. Use the **Refresh** button to update the data in the outbox.



For **Advanced** search filters, click on ▼ icon in respective column.

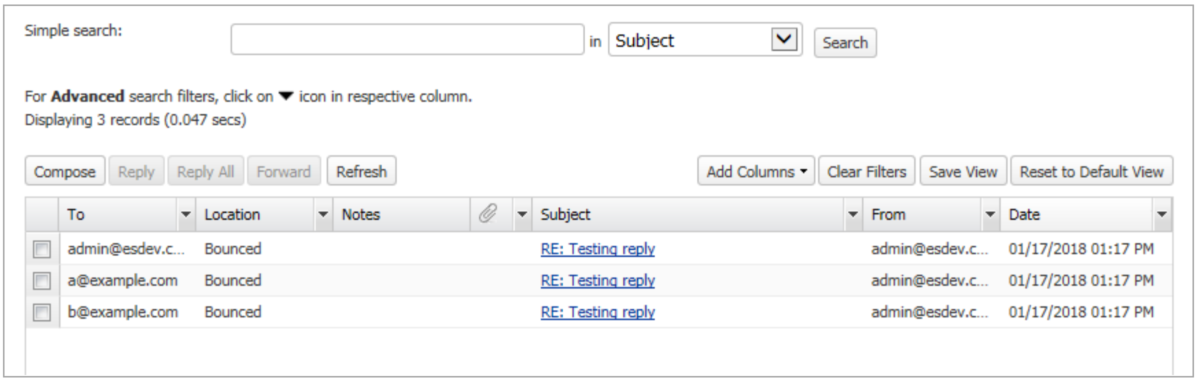
	To	Location	Notes	📎	Subject	From	Date

No Data Available

Refer to Managing the Email Tables for information on how to customize the table views.

Sent

Email Continuity | Sent displays all the messages sent on the outbound path. These represent messages that have been delivered in the past 7 days.



For **Advanced** search filters, click on ▼ icon in respective column.
Displaying 3 records (0.047 secs)

	To	Location	Notes	📎	Subject	From	Date
□	admin@esdev.c...	Bounced			RE: Testing reply	admin@esdev.c...	01/17/2018 01:17 PM
□	a@example.com	Bounced			RE: Testing reply	admin@esdev.c...	01/17/2018 01:17 PM
□	b@example.com	Bounced			RE: Testing reply	admin@esdev.c...	01/17/2018 01:17 PM

Use the buttons at the top of the table to manage the email in the **Sent** table:

Button	Definition
Compose	Click on the **Compose** button to send a new email. Click **Send** when email is ready.
Reply	Check the box by the email you want to respond to and click **Reply**. Type the message and click **Send** when email is ready.
Reply All	Check the box by the email where you want to respond to everyone and click **Reply All**. Type the message and click **Send** when email is ready.
Forward	Check the box by the email where you want to forward to another user and click **Forward**. Type the message and click **Send** when email is ready.
Refresh	Click Refresh to update the data in the inbox.

Refer to Managing the Email Tables for information on how to customize the table views.

5

Logs

Topics:

- Message Logs
- Connection Logs
- Capture ATP Logs

Message Logs

Message Logs displays messages captured in the auditing database. The messages selected are based on the auditing parameters you set. Select **Inbound** to see to see the inbound messages and select **Outbound** to see the outbound messages. Click the link in the Subject field to see the details about the message.

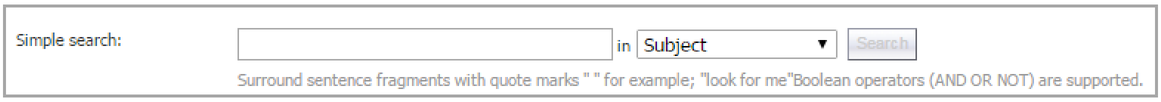
ⓘ **NOTE:** You can be in either the **Inbound** or the **Outbound** view when setting the auditing parameters. The **Settings** option is the same in either view.

Topics:

- Simple Searching for Data
- Filtering Table Data
- Customizing the Display
- Sharing Data

Simple Searching for Data

At the top of the page, a simple search tool is offered to search for specific strings or sentence fragments. The search parameters are applied directly on the data in the table. Surround sentence fragments with quotes (for example: “look for me”). Boolean operators AND, OR, and NOT are also supported.



Surround sentence fragments with quote marks " " for example; "look for me"Boolean operators (AND OR NOT) are supported.

To perform a simple search:

1 Enter the text you want to search for in the **Simple search** field.

2 Select the field to search on from the drop-down menu. Choose from **Subject**, **To**, **From**, or **Unique Message ID**.

3 Click on **Search**. The results are displayed in the data table.

4 Click **Clear Filters** to see all the available data again.

Filtering Table Data

Advanced search filters are performed directly on the data that's displayed. Select the down arrow next to the column title to filter the data. Some columns are searchable by typing in a string of text to search on. Other columns allow you to choose one or more filters from a list of pre-populated options. You can also filter more than one column at a time. The results of any filtering are immediately shown in the data table.

Click the **Clear Filters** button to display all the available data again.

Customizing the Display

Several button are provided so you can customize what data is shown in the Message Log table. The options are the same for both **Inbound** and **Outbound** tables.

Button name	Definition
Add Columns	Select **Add Columns** to get the drop down menu. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filters	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns.
Reset to Default View	Resets the data table back to the default view.
Settings	Opens a window you can customize the settings for Auditing. 1 Select on or off to enable the following: • Auditing for inbound email • Auditing for outbound email • Enable Judgment Details logging • Auditing for connections **NOTE:** Enabling **Auditing for connections** can generate five to ten times more data than not enabling it. To more effectively manage your storage space, you may wish to keep connection data for less time than you keep the email auditing files. 2 Specify how long you want to keep the auditing files by selecting one of the preset times for: • Keep Email auditing files for • Keep connection auditing files for 3 Click **Apply**.

Sharing Data

Data from the Message Logs table can be shared in many ways.

Button Name	Definition
Send Copy to	Sends selected messages to a specific recipient. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want.
Download	Sends the selected messages to the downloads file in zip format.
Release from Capture Box	Releases the email in the Capture Box without waiting for it to finish processing.

Button Name	Definition
Export to csv	Exports the displayed data to a file in CSV format.
Refresh	Refreshes the data in the table.

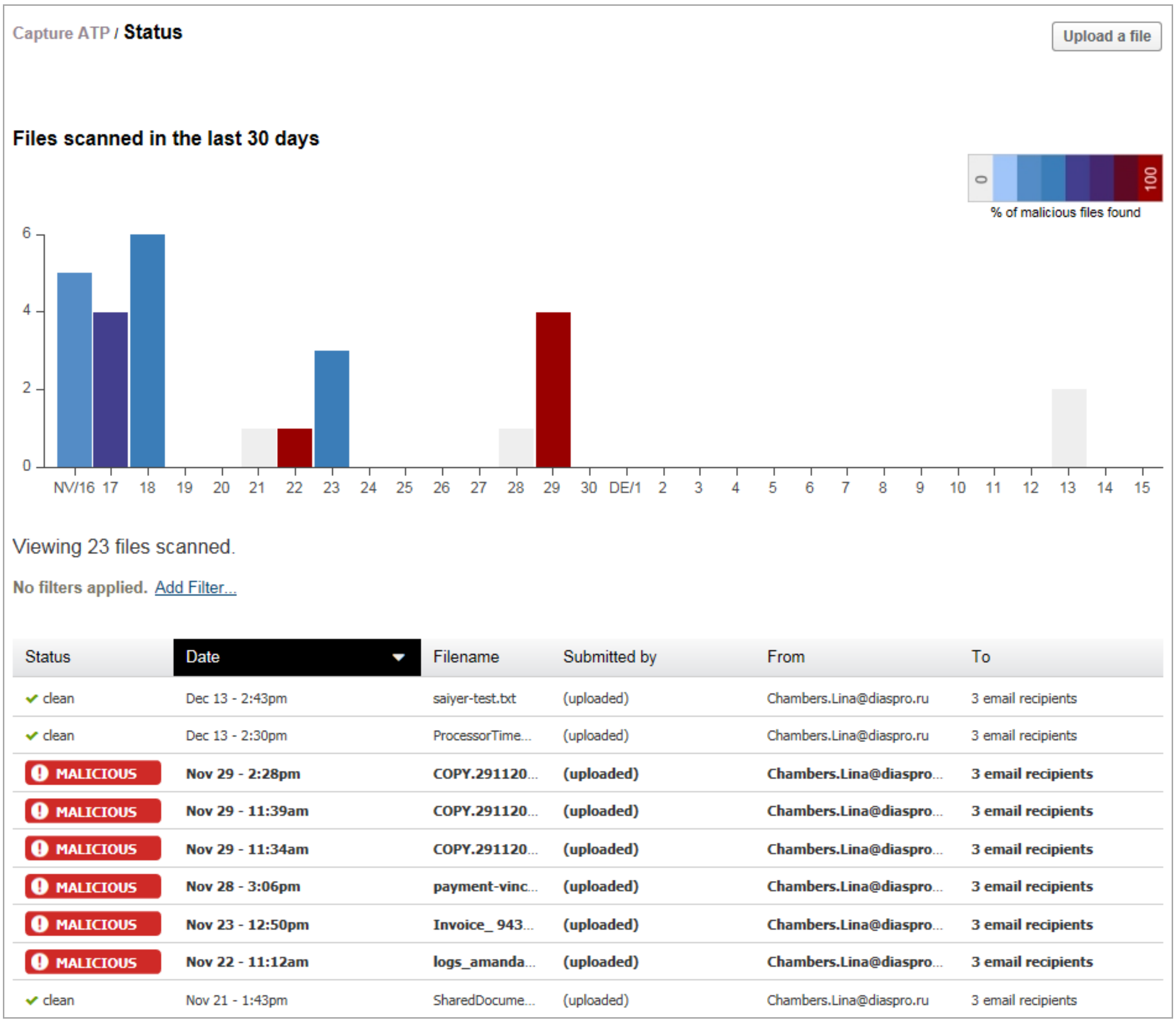
Connection Logs

You can use the **Connections** page to track the actions performed on every server that connects and delivers email to your Email Security server. Managing data is the Connections Logs table is very much like managing data in the Message Logs table. Refer to the following sections for details:

Function	Details
Simple search	Refer to Simple Searching for Data for details on how to perform a simple search.
Data filtering in the table	Refer to Filtering Table Data for details on how to use the built-in filtering capability.
Display customization	Refer to Customizing the Display for details on how to customize the table view.
Sharing data	Click on **Export to csv** to export the displayed data to a file in CSV format and click on **Refresh** to refresh the table in the data.

Capture ATP Logs

The Capture ATP logs provide a summary of Capture ATP activity in the last 30 days. It displays a bar graph showing how many files were scanned each day and a table listing the scanned files.

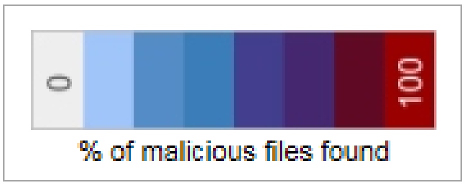


Files scanned in the last 30 days

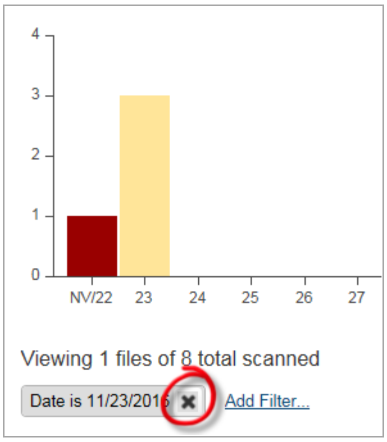
Viewing 23 files scanned.

Status	Date	Filename	Submitted by	From	To
✓ clean	Dec 13 - 2:43pm	saiyer-test.txt	(uploaded)	Chambers.Lina@diaspro.ru	3 email recipients
✓ clean	Dec 13 - 2:30pm	ProcessorTime...	(uploaded)	Chambers.Lina@diaspro.ru	3 email recipients
MALICIOUS	Nov 29 - 2:28pm	COPY.291120...	(uploaded)	Chambers.Lina@diaspro...	3 email recipients
MALICIOUS	Nov 29 - 11:39am	COPY.291120...	(uploaded)	Chambers.Lina@diaspro...	3 email recipients
MALICIOUS	Nov 29 - 11:34am	COPY.291120...	(uploaded)	Chambers.Lina@diaspro...	3 email recipients
MALICIOUS	Nov 28 - 3:06pm	payment-vinc...	(uploaded)	Chambers.Lina@diaspro...	3 email recipients
MALICIOUS	Nov 23 - 12:50pm	Invoice_ 943...	(uploaded)	Chambers.Lina@diaspro...	3 email recipients
MALICIOUS	Nov 22 - 11:12am	logs_amanda...	(uploaded)	Chambers.Lina@diaspro...	3 email recipients
✓ clean	Nov 21 - 1:43pm	SharedDocume...	(uploaded)	Chambers.Lina@diaspro.ru	3 email recipients

Additional data is available by dragging the cursor over the bars in the graph; a window pops up showing how many files were scanned that day and what percentage of them were malicious. The colors of the bars also indicate what percentage of the files were malicious. A white bar indicates that none were malicious. A red bar indicates 100% of them were malicious, and various shades of blue and purple represent different percentages in between, as shown in the legend on the graph.



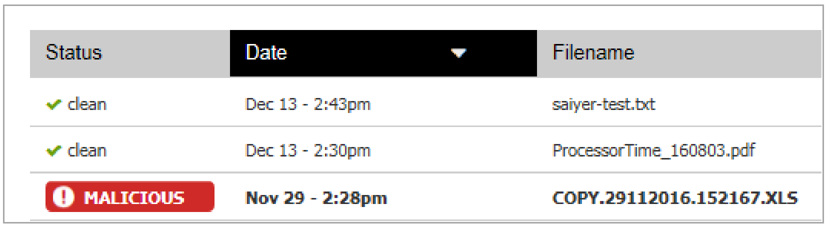
If you click on a bar in the graph, the data in the table below the graph is filtered to show only the files scanned on that day. The bar changes to yellow to show that it was selected for filtering. A date appears below the graph; click on the X next to the date to remove the filtering.



Viewing 1 files of 8 total scanned

Date is 11/23/2016 ✖ Add Filter...

Data in the table can also be sorted. Click in one of the headings to change the order of the data. The small arrow next to the heading indicates whether the data is listed in ascending or descending order as shown in the figure below:



Status	Date ▼	Filename
✓ clean	Dec 13 - 2:43pm	saiyer-test.txt
✓ clean	Dec 13 - 2:30pm	ProcessorTime_160803.pdf
! MALICIOUS	**Nov 29 - 2:28pm**	**COPY.29112016.152167.XLS**

To upload a specific file for scanning:

1 Select **Upload a File** to select a file for scanning.

2 Browse your disk to find and select the file.

3 Select **Upload** to start the scan.

ⓘ **NOTE:** The following file types are supported for scanning:

- EXE
- MSI
- ZIP
- APK applications
- PE

ⓘ **IMPORTANT:** The maximum file size allowed is 10 MB.

6

Tools

Topics:

- Run DMARC Reports
- Audit Trail
- Diagnostics

Run DMARC Reports

When the Email Security Mail Server plays the role as email sender and RUA receiver, it extracts and aggregates daily RUA files from the email receiver and from RUA providers, such as Google, Yahoo, etc. The DMARC Reporting Scheduler then imports the RUA files hourly into its database.

Based on date range and data filter, you can obtain five different types of reports. One report is a graphic chart; the others are tables. The reports include:

- DMARC Statistic Report (Graphic Chart)
- DMARC Master Detail Report
- Source IP Aggregation Report
- Source IP and Known Network Aggregation Report
- Provider Aggregation Report
- Source IP and Provider Aggregation Report

Users with an Admin Role or an OU Admin Role are allowed to access the DMARC reports. Admin role users can access all policy domains data, while OU Admin role users can only access the data in the domains assigned in **System Setup | Users, Groups & Organizations** on the **MANAGE** view.

> ⓘ **NOTE:** To receive reports, configure RUA address on the **MANAGE** view, under **Security Services | Anti-Spoofing**. Refer to Anti-Spoofing for more information.

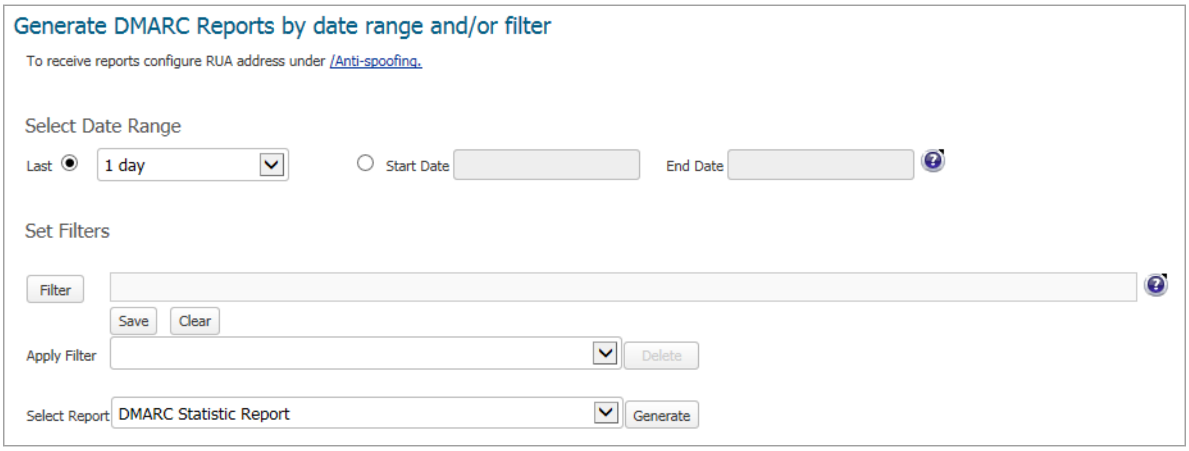
Topics:

- Generating the Report
- Defining New Filters

Generating the Report

To generate a DMARC report:

1 Navigate to **Investigate | Tools | Run DMARC Reports.**



Generate DMARC Reports by date range and/or filter

To receive reports configure RUA address under /Anti-spoofing.

Select Date Range

Last ● 1 day ○ Start Date End Date

Set Filters

Apply Filter

Select Report DMARC Statistic Report

2 Choose a Date Range using one of the following methods:

- Select **Last** and choose a pre-defined option from the drop down menu. Choices range from 1 to 21 days.
- Select **Start Date** and enter a **Start date** and **End date** from the pop up calendars.

3 Choose the filters for the report. You can select available filters from the **Apply Filters** drop down menu or you can build a new filter by selecting the **Filter** button. Refer to Defining New Filters for more information about building a new filter.

4 Select the report type from the **Select Report** drop down list. The options include:

- DMARC Statistic Report (Graphic Chart)
- DMARC Master Detail Report
- Source IP Aggregation Report
- Source IP and Known Network Aggregation Report
- Provider Aggregation Report
- Source IP and Provider Aggregation Report

5 Click on the **Generate** button to generate the report. Reports are shown in a window below the 'Set Filters' section.

6 Click **Download PDF** to download a PDF report once the HTML report is generated. The PDF report name includes the Report Name and a time stamp.

All reports can be rendered in HTML format and downloadable PDF file. (HTML reports allow you to mouse over 'Alignment' value to see alignment reason description.)

The statistics report displays either horizontally or vertically, depending on the date range. If days of selected date range are less than 15 days, three (3) bar charts will be horizontally display. If the date range is greater than 15 days, the bar charts display vertically. For tabulated reports, scrolling the mouse over the 'Alignment' value displays the Alignment Reason. For example, if the 'Alignment' is 'No', moving the mouse over this 'No' makes the Title Box show: “No DKIM and SPF is passed, On SPF Relaxed, SPF Organization Domain(sina.com) Not Matched From Header Domain(sonicwall.com)” This informational message can be useful for DMARC troubleshooting.

Defining New Filters

You can define a new filter to use for the DMARC reports. This filter then becomes an option for filtering the DMARC Report database.

To build a new filter:

1. Navigate to the **INVESTIGATE** view and select **Tools | Run DMARC Reports**.
2. Click on the **Filter** button to create a new filter. (If a filter already exists, clicking this button allows you to edit the filter.) The **Set Filter** page opens.
3. Define the parameters of the filters using the conditions provided.
   a. Select one of the **Condition Names** from the left.
   b. Select the operator for how the data is acted upon. For example, you might chose between **include** and **exclude** or mathematical operators like == (equals) and != (not equals).
   c. In the right column, **Select or Input Values**. Values are automatically provided for some Condition Names, but you need to type in the values you want if none are provided.
   d. Click **OK** to exit the Set Filter pages.
4. Click **Save** to save the newly configured settings.

Other buttons are available to help you manage the filters. They include:

Clear	Clears all settings of the current filter.
Delete	Deletes a selected filter.
Bullet icons	Represents a filter condition. Click the icon to open the Set Filter dialog box, or click the small 'x' icon to delete the condition from the filter.

Audit Trail

The Audit Trail feature is a set of destination and source records that tracks the actions performed on every email message that passes through Email Security. This feature logs all the activity performed by users, and the Global Administrator can view and search these activities.

The Audit Trail feature includes information of any fields that may have been added, edited, or deleted; search queries in the Junkbox and Auditing pages; and all View, Unjunk, Delete, Sent Copy to, Download actions performed on messages in the Junkbox and Auditing pages.

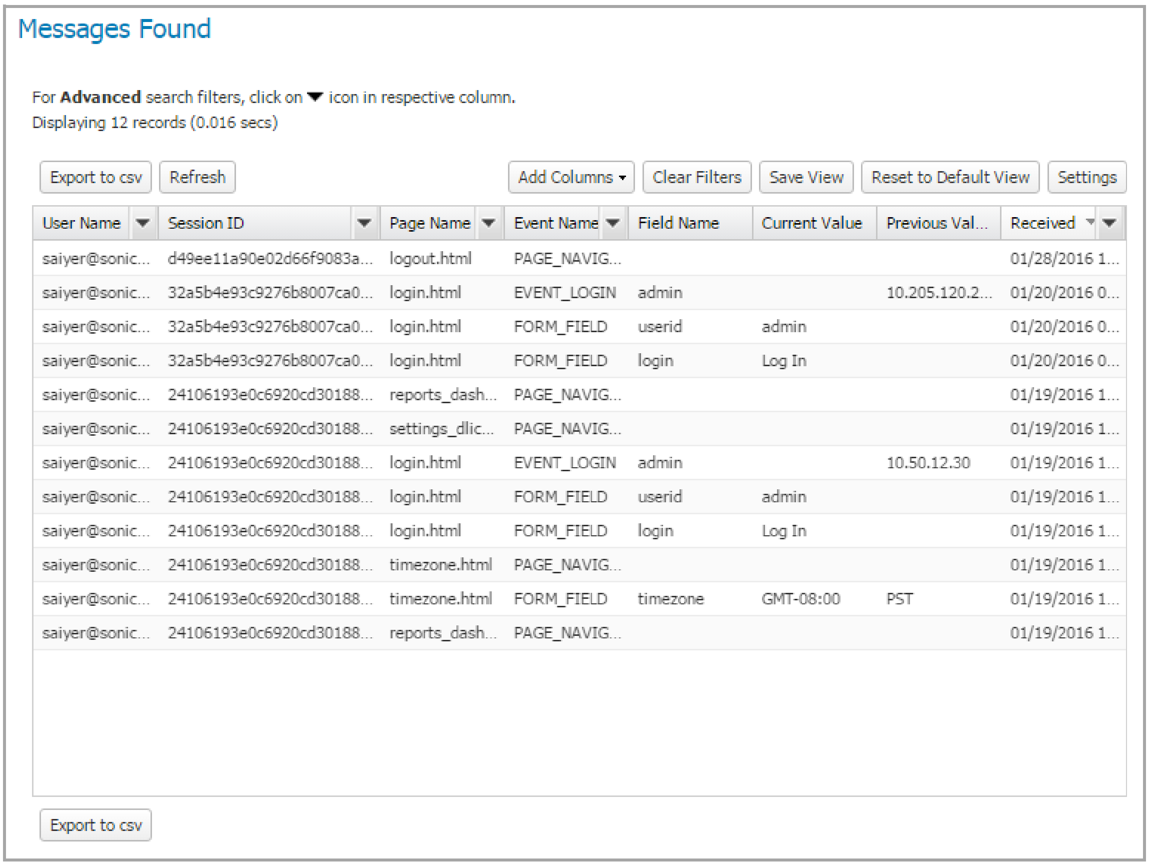
The audit messages are displayed in a table on the Audit Trail page. You can configure the data display and manipulate the data through filters and sorts.

To enable the Audit Trail:

1. Navigate to **Tools | Audit Trail** on the **INVESTIGATE** view.
2. Select **on** to enable the Audit Trail.
3. From the drop-down list, choose how long you want to deep the email auditing files. Options range from 1 day to 1 year.
4. Click **Apply** to save the settings.

To configure the data:

1. Click the **Add Columns** button.The drop down menu shows all the fields that can be displayed in the data table.
2. Check the box for the fields you want to appear
3. Uncheck the box for the fields you want to hide.
4. Click on **Save View** if you want to have that view displayed all the time.
5. Click on **Reset to Default View** if you want to return to the default view.



Messages Found

For **Advanced** search filters, click on ▼ icon in respective column.
Displaying 12 records (0.016 secs)

User Name	Session ID	Page Name	Event Name	Field Name	Current Value	Previous Val...	Received
saiyer@sonic...	d49ee11a90e02d66f9083a...	logout.html	PAGE_NAVIG...				01/28/2016 1...
saiyer@sonic...	32a5b4e93c9276b8007ca0...	login.html	EVENT_LOGIN	admin		10.205.120.2...	01/20/2016 0...
saiyer@sonic...	32a5b4e93c9276b8007ca0...	login.html	FORM_FIELD	userid	admin		01/20/2016 0...
saiyer@sonic...	32a5b4e93c9276b8007ca0...	login.html	FORM_FIELD	login	Log In		01/20/2016 0...
saiyer@sonic...	24106193e0c6920cd30188...	reports_dash...	PAGE_NAVIG...				01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	settings_dlic...	PAGE_NAVIG...				01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	login.html	EVENT_LOGIN	admin		10.50.12.30	01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	login.html	FORM_FIELD	userid	admin		01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	login.html	FORM_FIELD	login	Log In		01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	timezone.html	PAGE_NAVIG...				01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	timezone.html	FORM_FIELD	timezone	GMT-08:00	PST	01/19/2016 1...
saiyer@sonic...	24106193e0c6920cd30188...	reports_dash...	PAGE_NAVIG...				01/19/2016 1...

To set or clear filters:

1. Select the field to search on.
2. Click on the drop down menu and select Filters.
3. Type the search string in the field. The data immediately begins filtering based on what you typed in.
4. Add filters to other fields if you want to further refine your search.
5. Click on **Clear Filters** to view all the data again.

To sort:

1. Place the cursor in the heading of a the data column you want to sort.
2. Click in the column heading and an arrow indicator appears.
   - An arrow pointing down indicates data is sorted in descending order.
   - An arrow pointing up indicates data is sorted in ascending order.

3 Click in the column heading again to change directions.

To refresh the data:

1 Click the **Refresh** button.

To save the data:

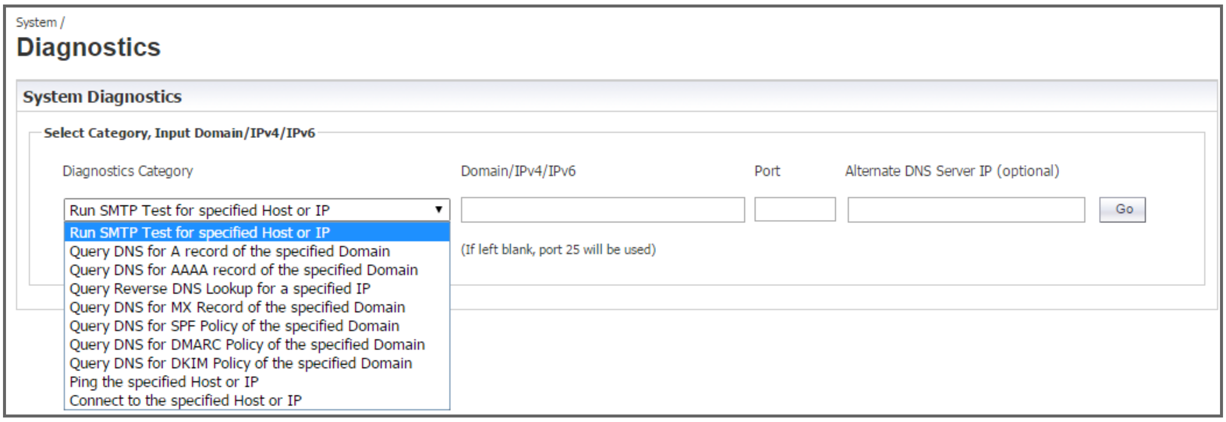
1 Click on the **Export to csv** button. An excel download file appears at the bottom of the window.

2 Double-click on the files to open it.

3 View or save as needed.

Diagnostics

The **Tools |Diagnostics** page on the **INVESTIGATE** view allows the Administrator to run different diagnostic tests on a specific SMTP Host or DNS Server.


System /
Diagnostics
System Diagnostics
Select Category, Input Domain/IPv4/IPv6
Diagnostics Category
Domain/IPv4/IPv6
Port
Alternate DNS Server IP (optional)
Run SMTP Test for specified Host or IP
Go
Run SMTP Test for specified Host or IP
Query DNS for A record of the specified Domain
Query DNS for AAAA record of the specified Domain
Query Reverse DNS Lookup for a specified IP
Query DNS for MX Record of the specified Domain
Query DNS for SPF Policy of the specified Domain
Query DNS for DMARC Policy of the specified Domain
Query DNS for DKIM Policy of the specified Domain
Ping the specified Host or IP
Connect to the specified Host or IP

(If left blank, port 25 will be used)

To run the diagnostics:

1 Select an option in **Diagnostics Category**. The various options are described below.

Run SMTP Test for specified Host or IP Run an SMTP test for the Input Domain/IPv4/IPv6 specified in the respective field. Optionally, you may specify the Alternate DNS Server IP.

Query DNS for A record of the specified Domain Specify the Input Domain/IPv4/IPv6 and select this option to query the DNS server for the A record. Optionally, you may specify the Alternate DNS Server IP.

Query DNS for AAAA record of the specified Domain Specify the Input Domain/IPv4/IPv6 and select this option to query the DNS server for the AAAA record. Optionally, you may specify the Alternate DNS Server IP.

Query Reverse DNS Lookup for a specified IP Specify the Input Domain/IPv4/IPv6 and select this option to query reverse the DNS lookup server for the specified IP. Optionally, you may specify the Alternate DNS Server IP.

Query DNS for MX Record of the specified Domain Specify the Input Domain/IPv4/IPv6 and select this option to query the DNS server for the MX Record. Optionally, you may specify the Alternate DNS Server IP.

Query DNS for SPF Policy of the specified Domain Specify the Input Domain/IPv4/IPv6 and select this option to query the DNS server for the SPF Policy. Optionally, you may specify the Alternate DNS Server IP.

Query DNS for DMARC Policy of the specified Domain	Specify the Input Domain/IPv4/IPv6 and select this option to query the DNS server for the DMARC Policy. Optionally, you may specify the Alternate DNS Server IP.
Query DNS for DKIM Policy of the specified Domain	Specify the Input Domain/IPv4/IPv6 and select this option to query the DNS server for the DKIM Policy. Optionally, you may specify the Alternate DNS Server IP.
Ping the mentioned Host or IP	Ping the Host or IP specified in the Input Domain/IPv4/IPv6 field.
Connect to the specified Host or IP	Select this option to connect to the Host or IP specified in the Input Domain/IPv4/IPv6 field.

2 Enter the data for the remaining fields. Different fields show depending on choice made in Step 1.

3 Enter the **Alternate DNS Server IP**, if needed.

4 Click the **Go** button.

Part 4

Manage

- Basic Administration
- Policy & Compliance
- System Setup | Server
- System Setup | Customization and Certificates
- Users, Groups & Organizations
- System Setup | Network and Junkbox Commands
- Anti-Spam
- Anti-Spoofing
- Anti-Phishing and Anti-Virus
- Capture, Encryption and Connections
- Reporting

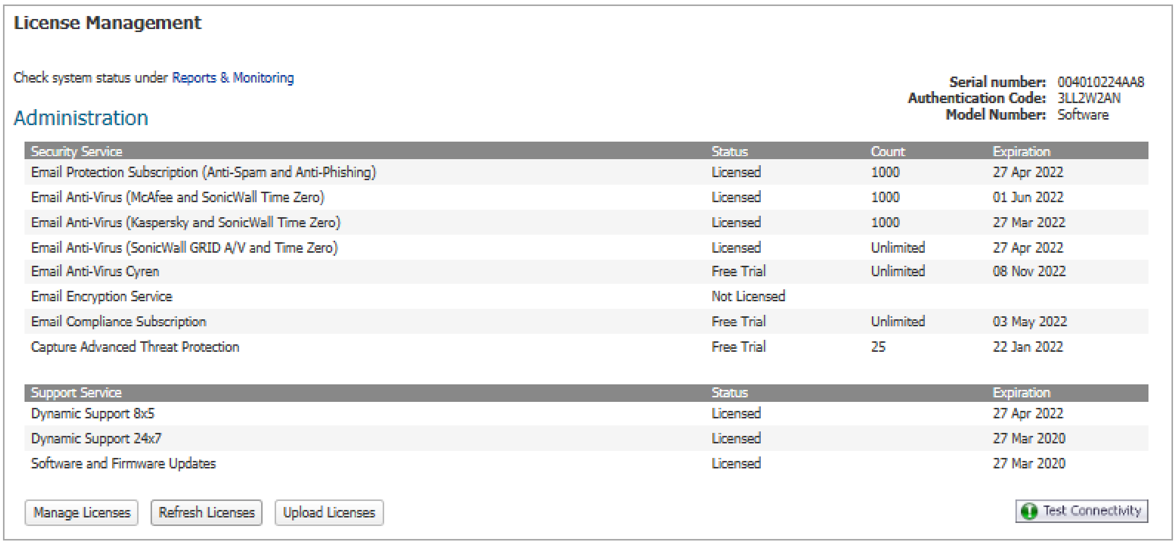
Basic Administration

The basic administration tasks for an Email Security instance are grouped at the top of menu. They include things you do more often, like:

- License Management
- Firmware Update
- Backup/Restore
- Downloads.

License Management

The **License Management** option allows you to view and manage current Security Service and Support Service for your Email Security solution.



License Management

Check system status under Reports & Monitoring

Serial number: 004010224AA8
Authentication Code: 3LL2W2AN
Model Number: Software

Administration

Security Service	Status	Count	Expiration
Email Protection Subscription (Anti-Spam and Anti-Phishing)	Licensed	1000	27 Apr 2022
Email Anti-Virus (McAfee and SonicWall Time Zero)	Licensed	1000	01 Jun 2022
Email Anti-Virus (Kaspersky and SonicWall Time Zero)	Licensed	1000	27 Mar 2022
Email Anti-Virus (SonicWall GRID A/V and Time Zero)	Licensed	Unlimited	27 Apr 2022
Email Anti-Virus Cyren	Free Trial	Unlimited	08 Nov 2022
Email Encryption Service	Not Licensed		
Email Compliance Subscription	Free Trial	Unlimited	03 May 2022
Capture Advanced Threat Protection	Free Trial	25	22 Jan 2022

Support Service	Status	Expiration
Dynamic Support 8x5	Licensed	27 Apr 2022
Dynamic Support 24x7	Licensed	27 Mar 2020
Software and Firmware Updates	Licensed	27 Mar 2020

Key information for your Email Security solution is provided in the upper right corner:

- **Serial Number**—The serial number of your SonicWall Email Security appliance/software.
- **Authentication Code**—The code you entered upon purchasing/activating the SonicWall Email Security solution.
- **Model Number**—The model number of the SonicWall Email Security appliance. If you are using the SonicWall Email Security software, the model number is listed as Software.

The following buttons, located at the bottom of the page, allow you to perform certain licensing functions:

- **Manage Licenses**—Click this button to log in to your MySonicWall account to register appliances and manage all security services, upgrades, and changes.
- **Refresh Licenses**—Click this button to refresh the license status for Security and Support services.

- **Upload Licenses**—Click this button to manually update your licenses. This feature is useful in the event that you are unable to use the dynamic licensing feature for any reason. Before clicking this button, download a license file from MySonicWall. Then, click the **Choose File** button, select the license file you downloaded, and click the **Upload** button. Your product’s licenses updates based on the license file.
- **Test Connectivity**—Click this button to validate connectivity to the SonicWall License Manager.

ⓘ **NOTE:** The hourly license update synchronizes with the online license manager and overwrite licenses applied by the offline method.

SonicWall Email Security comes with several service modules that must be licensed separately. For maximum effectiveness, all services are recommended. Refer to Available Module Licenses for descriptions.

The Security Service table on the **License Management** page provides information on the status of the various offerings in your configuration.

Status The status for the Security or Support Service may be one of the following:

- **Licensed** Services have a regular valid license.
- **Free Trial** Services are using a 14-day free trial license.
- **Not licensed** Service has not been licensed.
- **Perpetual** The base Key license comes with the purchase of the product and is perpetual. Note that the Base Key is the only perpetual license.

Count The number of users to which the license applies.

Expiration Expiration date of the service. Either a specific expiration date is listed or **Never** is listed, indicating no expiration.

The Support Service table shows the kinds of service support agreements that have been licensed for your solution. It includes license status and expiration date.

Firmware Update

On the **Firmware Update** page, you can upload and apply the latest version of Email Security. The general process for an update includes:

1. Download the current version of Email Security to a local hard drive that’s accessible by the appliance or software instance.
2. Either schedule a backup or perform a **Backup Now** if you want to be able to restore the prior configuration. Refer to Backup/Restore for more information.
3. Navigate to **Firmware Update** on the **MANAGE** view.
4. Use the **Browse...** button to choose the file you want to upload and apply.
5. Click **Apply Patch**.

Backup/Restore

Backup/Restore has three options where you can configure the backup and restore settings for Email Security.

ⓘ **NOTE:** You are not required to use the backup and restore settings. Executing the backup and restore functions depend on the needs of your organization.

Topics:

- Manage Backups
- Schedule Backup
- FTP Profiles

Manage Backups

On the **Backup/Restore > Manage Backups** page, you can view and manage the following features:

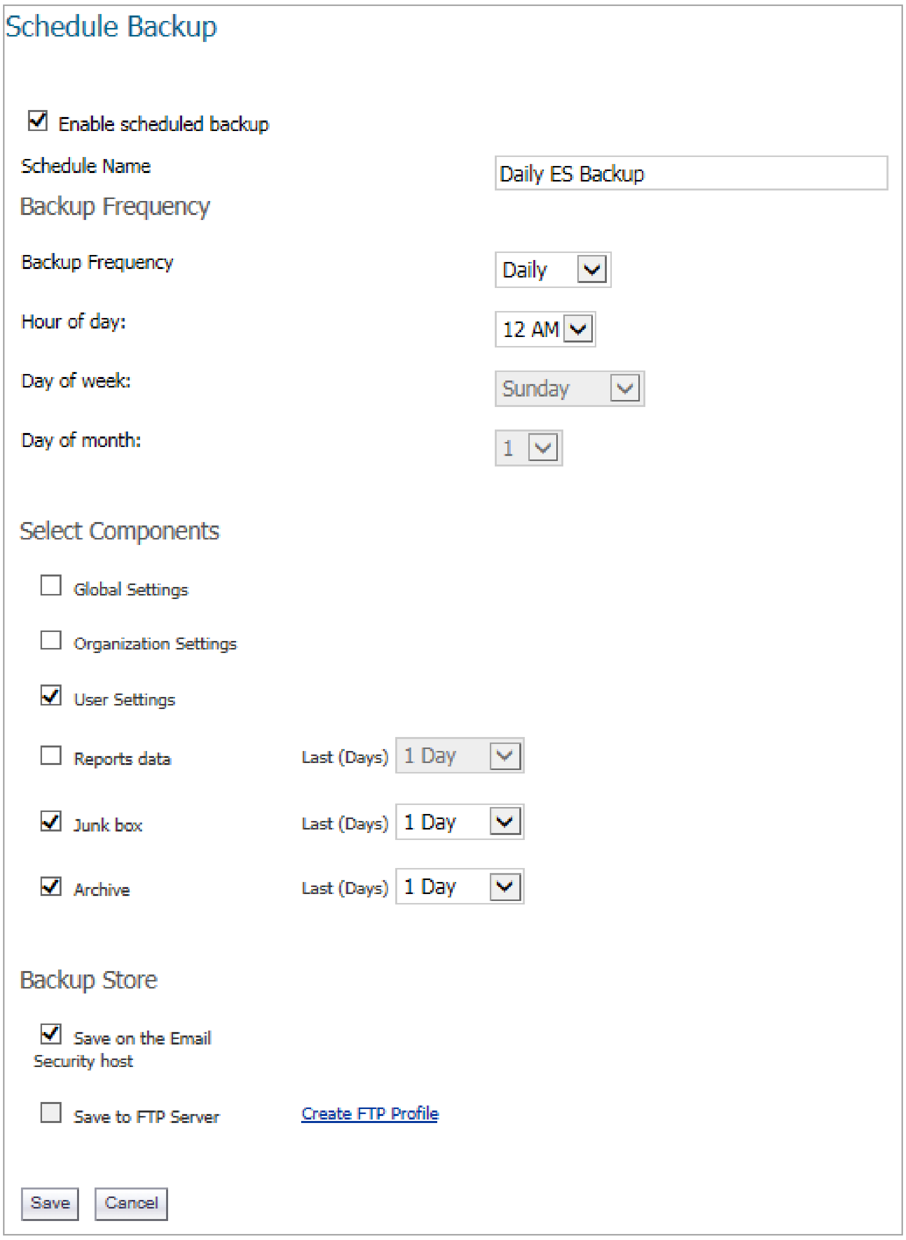
Backup Snapshots	Displays all of the backup snapshots that have been defined and saved. From that display you can restore, delete or download the data by selecting a specific snapshot and using the appropriate buttons at the far right. The total disk spaced used is also highlighted at the top of the table.
Restore from a snapshot file	Select **Browse...** and navigate to the snapshot file you wish to restore. Then click **Start Restoring Data** to begin the restore.
Settings	In the drop-down menu, select the length of time of keeping snapshot files. The choices are 1 day, 2 days, 3 days, 7 days, 14 days, 30 days, 60 days, 90 days, 180 days, or 1 year. Click **Apply Changes** to finalize your choice.
Backup and Restore History	Displays the backup and restore history. You can filter or sort the data by clicking on drop-down menu to the right of each title. Then chose the options you want.

Schedule Backup

On the **Backup/Restore > Schedule Backup** page, you can define all your scheduled backups and snapshots.

To define a scheduled backup:

1 Click on the **Add** button and the **Configure Schedule Backup** page opens.



Schedule Backup

☑ Enable scheduled backup

Schedule Name	Daily ES Backup

Backup Frequency

Backup Frequency	Daily
Hour of day:	12 AM
Day of week:	Sunday
Day of month:	1

Select Components

□ Global Settings		
□ Organization Settings		
☑ User Settings		
□ Reports data	Last (Days)	1 Day
☑ Junk box	Last (Days)	1 Day
☑ Archive	Last (Days)	1 Day

Backup Store

☑ Save on the Email Security host

□ Save to FTP Server   Create FTP Profile

2 Select the **Enable scheduled backup** check box to use this feature.

3 Enter a name for the backup in the **Schedule Name** field.

4 Then, configure the following settings:

- **Backup Frequency**—Specify how often you want the backups to occur: **Daily**, **Weekly** or **Monthly**.
- **Hour of day**—Choose the hour the backup begins.
- **Day of week**—Choose the day of the backup, if needed.
- **Day of month**—Choose the date of the backup, if needed.

5 Select which of the following components to include in the backup:

- **Global Settings**
- **Organization Settings**
- **User Settings**

- **Reports data**: select how many days of data to include
- **Junk box**: select how many days of data to include
- **Archive**: select how many days of data to include

6 Select one of the following storage options:

- **Save on the Email Security host** if you want to save the file locally.
- **Save to FTP Server** if you want to save and upload it to a remote server.

> ⓘ **NOTE:** If an FTP server hasn’t been defined yet, you can click on the link **Create FTP Profile** to set one up.

7 Click on **Save** to save the backup definition.

To initiate an immediate snapshot:

1 Click on the **Backup Now** button and the **Create Backup Snapshot** page opens.

2 Select the components to include in the backup:

- **Global Settings**
- **Organization Settings**
- **User Settings**
- **Reports data**: select how many days of data to include
- **Junk box**: select how many days of data to include
- **Archive**: select how many days of data to include

3 Select one of the following storage options:

- **Save on the Email Security host** if you want to save the file locally.
- **Save to FTP Server** if you want to save and upload it to a remote server.

> ⓘ **NOTE:** If an FTP server hasn’t been defined yet, you can click on the link **Create FTP Profile** to set one up.

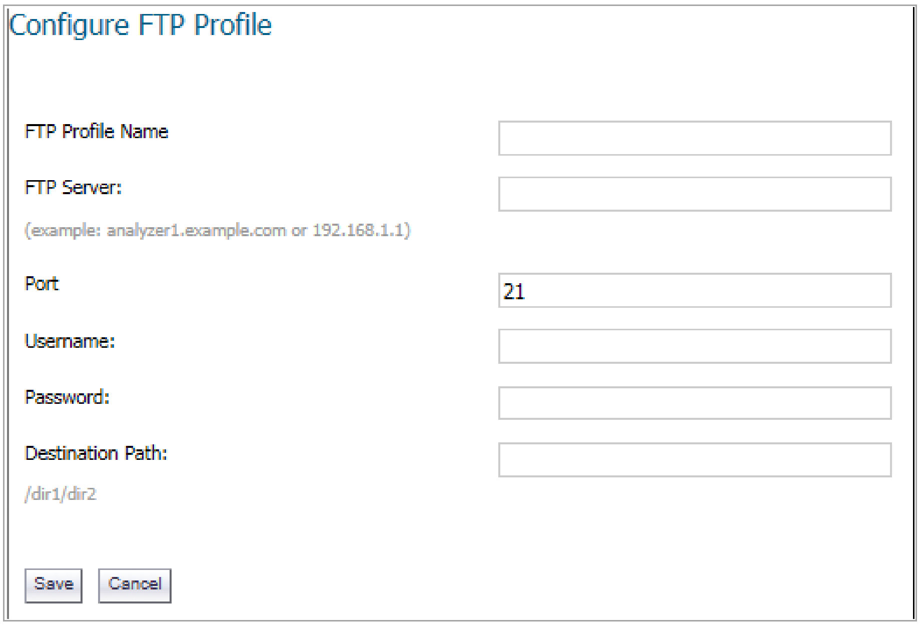
4 Click on **Start** to begin the snapshot.

FTP Profiles

On the **Backup/Restore > FTP Profile** page, you can configure FTP Profiles so that snapshots and scheduled backup files can be stored on your FTP server.

To configure an FTP profile:

1 Click on the **Add** button and the **Configure FTP Profile** page opens.



Configure FTP Profile

FTP Profile Name	
FTP Server: (example: analyzer1.example.com or 192.168.1.1)	
Port	21
Username:	
Password:	
Destination Path: /dir1/dir2	

2 Type in the **FTP Profile Name**.

3 Input the domain name or IP address of the **FTP Server**.

4 List the **Port** number.

5 Add the **Username** and **Password** in their respective fields.

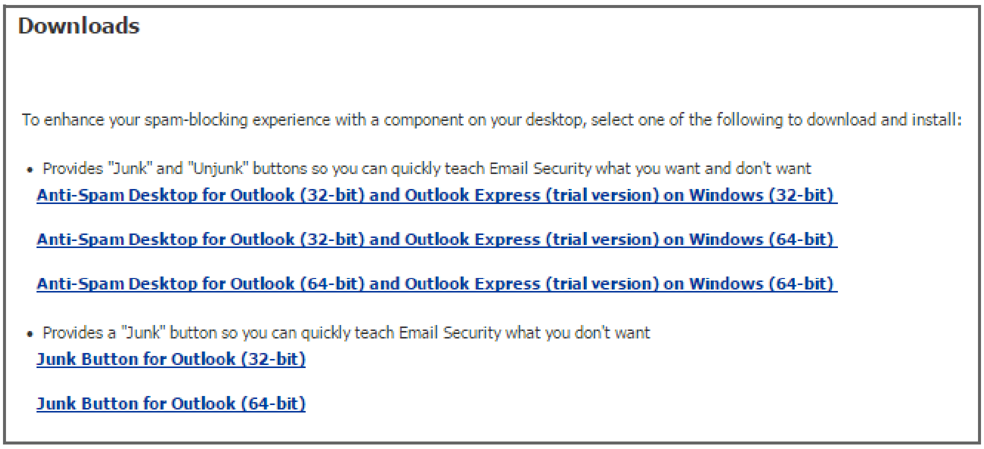
6 List the **Destination Path** where you want the backup stored.

7 Click on **Save** to configure the profile.

On the table displaying the FTP profiles, you can filter or sort the profiles by clicking on the drop-down menu to the right of each title. Then chose the options you want.

Downloads

SonicWall provides some tools you can download that enhance the spam-blocking experience on the desktop. Navigate to the **Downloads** page to download and install the following tools.



Downloads

To enhance your spam-blocking experience with a component on your desktop, select one of the following to download and install:

- Provides "Junk" and "Unjunk" buttons so you can quickly teach Email Security what you want and don't want

  Anti-Spam Desktop for Outlook (32-bit) and Outlook Express (trial version) on Windows (32-bit)

  Anti-Spam Desktop for Outlook (32-bit) and Outlook Express (trial version) on Windows (64-bit)

  Anti-Spam Desktop for Outlook (64-bit) and Outlook Express (trial version) on Windows (64-bit)

- Provides a "Junk" button so you can quickly teach Email Security what you don't want

  Junk Button for Outlook (32-bit)

  Junk Button for Outlook (64-bit)

The Anti-Spam Desktop for Outlook and Outlook Express options are trial versions of the SonicWall Anti-Spam Desktop feature. It’s offered in 32-bit and 64-bit combinations. This download provides “Junk” and “Unjunk” buttons for you to customize your own Email Security solution.

The Junk Button for Outlook link provides a “Junk” button for you to install on your own Microsoft Outlook program. Both 32-bit and 64-bit options are offered. These downloads help customize your Email Security solution.

8

Policy & Compliance

SonicWall Email Security's Policy Management feature 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.

This chapter contains the following sections:

- Policy Management and Mail Threats
- Filters
- Policy Groups
- Compliance

Policy Management and Mail Threats

As SonicWall Email Security evaluates email, it uses the following order when evaluating threats in email messages:

- Virus
- Likely Virus
- Policy Filters
- Phishing
- Likely Phishing
- Spam
- Likely Spam

For example, if a message is both a virus and a spam, the message is categorized as a virus since virus is higher in precedence than spam. If SonicWall Email Security determines that the message is not any of the above threats, it is delivered to the destination server.

Policy Management plays a key role in evaluating the email threats by filtering email based on message contents and attachments. You can create policy filters in which you specify an action or actions you want Email Security to take on messages that meet the conditions you define. For example, you can specify words to search for—a product term, for example—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.

ⓘ **NOTE:** Any of the policies configured in the Policy section take precedence over any entries made in the Allowed List.

Filters

The **Policy & Compliance > Filters** page is where you manage preconfigured files and define new filters for both inbound and outbound paths.

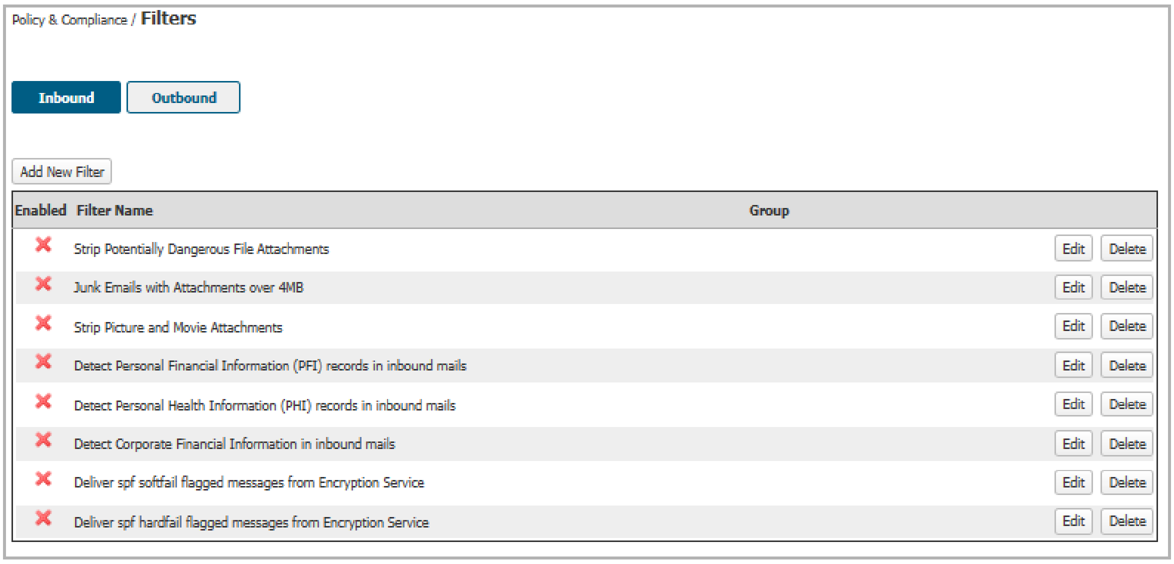
ⓘ **NOTE:** Policies created on the inbound path can not be shared with the outbound path and vice versa. See Managing Filters for examples of adding inbound and outbound policies.

Topics:

- Preconfigured Inbound Filters
- Preconfigured Outbound Filters
- Adding Filters
- Language Support
- Managing Filters
- Advanced Filtering

Preconfigured Inbound Filters

The following preconfigured filters are provided with Email Security. They are not enabled by default and need to be enabled if you want to use them.



Enabled	Filter Name	Group		
✖	Strip Potentially Dangerous File Attachments		Edit	Delete
✖	Junk Emails with Attachments over 4MB		Edit	Delete
✖	Strip Picture and Movie Attachments		Edit	Delete
✖	Detect Personal Financial Information (PFI) records in inbound mails		Edit	Delete
✖	Detect Personal Health Information (PHI) records in inbound mails		Edit	Delete
✖	Detect Corporate Financial Information in inbound mails		Edit	Delete
✖	Deliver spf softfail flagged messages from Encryption Service		Edit	Delete
✖	Deliver spf hardfail flagged messages from Encryption Service		Edit	Delete

To enable a preconfigured filter:

1 Identify the filter you want to enable.

2 Select **Edit**.

3 At the top of the **Edit Filter** page, check the box to **Enable this filter**.

4 Scroll to the bottom of the **Edit Filter** page and select **Save This Filter**.

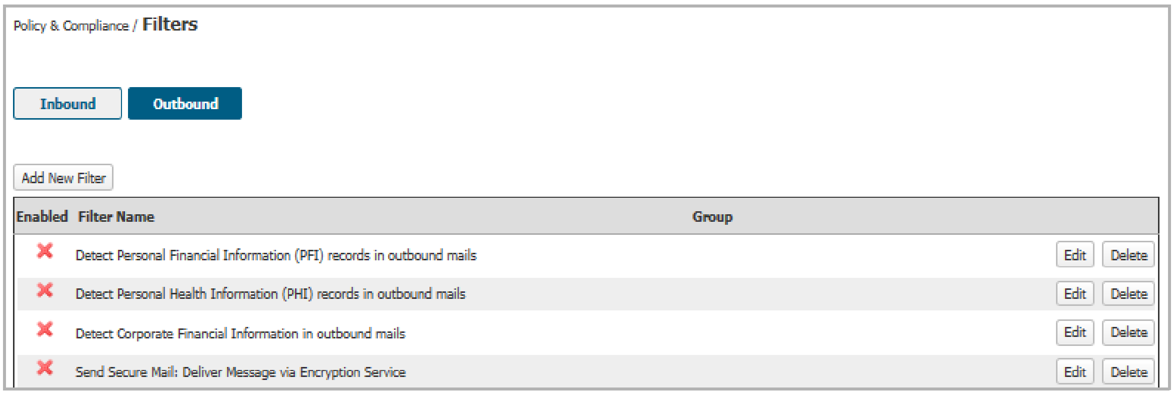
The following table describes the preconfigured inbound filters.

Preconfigured Inbound Filters

Filter name	Function
Junk emails with attachments over 4MB	Stores all incoming email messages over 4MB in size in the Junk Box.
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.
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.
Detect Personal Health Information (PHI) records in inbound mails	Detects personal health information by utilizing the Medical Drug Names pre-defined dictionary as an identifying tool.
Detect corporate financial information in inbound mails	Detects corporate financial information in the subject line or body of an email by utilizing the Financial Terms predefined dictionary as an identifying tool.
Detect Personal Financial Information (PFI) records in inbound mails	Detects personal financial information by using the Record ID definitions feature as an identifying tool looking for mails that match Social Security Number and Credit Card Number formats.
Deliver spf softfail flagged messages from Encryption Services	Allows delivery of messages sent from Encryption Services in the cloud that might otherwise be tagged as spam or likely spam if ssl.sonicsecoremail.com domain wasn't added to your SPF records.
Deliver spf hardfail flagged messages from Encryption Services	

Preconfigured Outbound Filters

The following preconfigured filters are provided with Email Security. They are not enabled by default and need to be enabled if you want to use them.



Enabled	Filter Name	Group		
✗	Detect Personal Financial Information (PFI) records in outbound mails		Edit	Delete
✗	Detect Personal Health Information (PHI) records in outbound mails		Edit	Delete
✗	Detect Corporate Financial Information in outbound mails		Edit	Delete
✗	Send Secure Mail: Deliver Message via Encryption Service		Edit	Delete

To enable a preconfigured filter:

1. Identify the filter you want to enable.
2. Select **Edit**.
3. At the top of the **Edit Filter** page, check the box to **Enable this filter**.
4. Scroll to the bottom of the Edit Filter page and select **Save This Filter**.

The following tabel describes the preconfigured outbound filters.

Preconfigured Outbound Filters

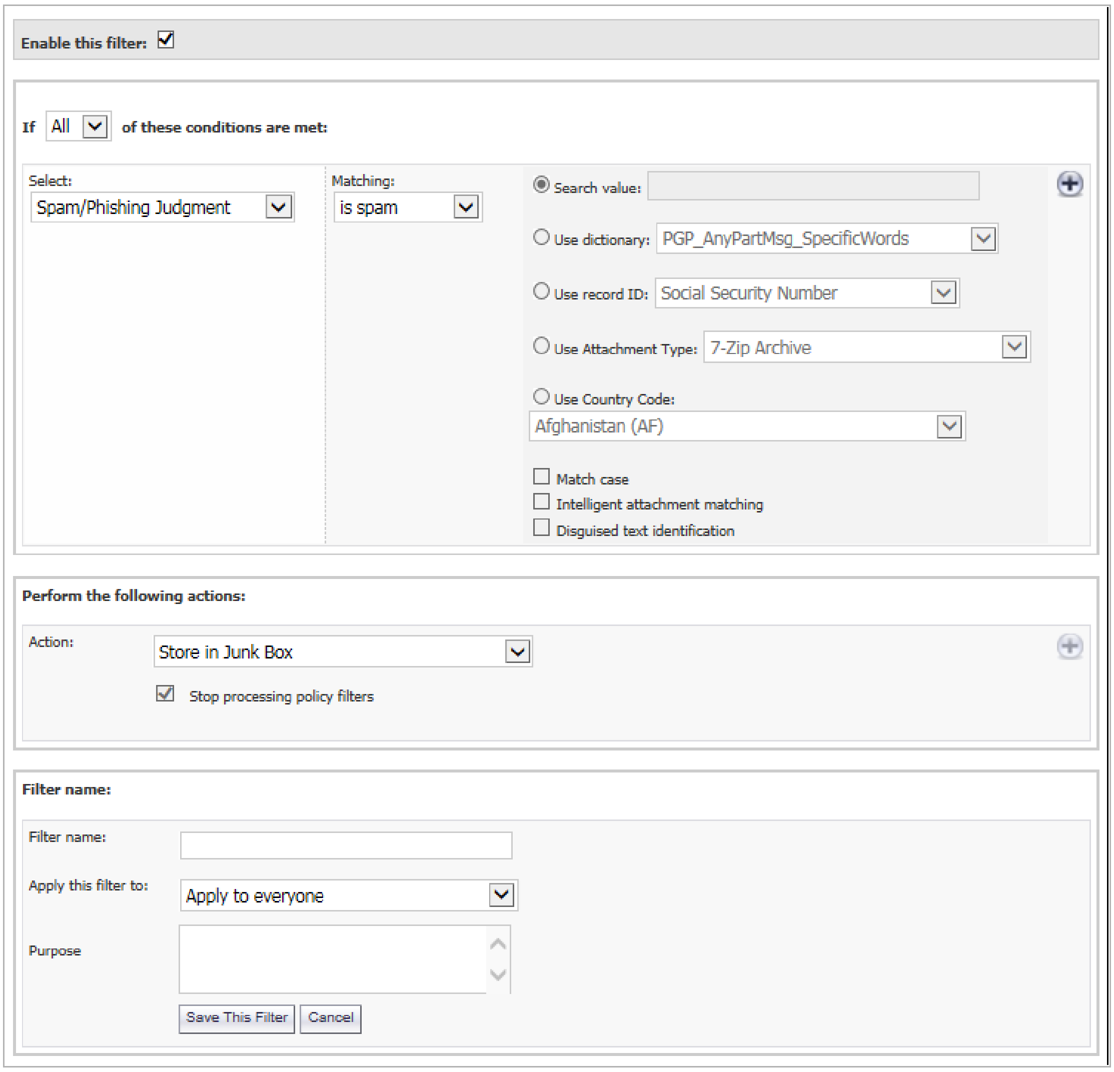
Filter name	Function
Detect Personal Financial Information (PFI) records in outbound mails	Detects personal financial information by using Record ID definitions feature as an identifying tool looking for mails that match Social Security Number and Credit Card Number formats.
Detect Personal Health Information (PHI) records in outbound emails	Detects personal health information by utilizing the Medical Drug Names pre-defined dictionary as an identifying tool.
Send Secure Mail: Deliver Message via SecureMail Server	Delivers messages using the SecureMail Server.
Detect Corporate Financial Information in Outbound Mails	Detects corporate financial information in the subject line or body of an email by utilizing the Financial Terms predefined dictionary as an identifying tool.
Send Secure Mail: Deliver Message via Encryption Service	Enables outbound messages to be sent to Encryption Service when the subject line starts with **[SECURE]**.

Adding Filters

You can add filters for email as it enters or exits your organization.

To create a policy filter:

1. Navigate to the **Policy & Compliance > Filters** page on the **MANAGE** view.
2. Select the **Inbound** or **Outbound** tab to create filters for inbound or outbound email messages.
3. Click the **Add New Filter** button.



Enable this filter: ☑

If All of these conditions are met:

Select: Spam/Phishing Judgment

Matching: is spam

● Search value:

○ Use dictionary: PGP_AnyPartMsg_SpecificWords

○ Use record ID: Social Security Number

○ Use Attachment Type: 7-Zip Archive

○ Use Country Code: Afghanistan (AF)

□ Match case

□ Intelligent attachment matching

□ Disguised text identification

Perform the following actions:

Action: Store in Junk Box

☑ Stop processing policy filters

Filter name:

Filter name:

Apply this filter to: Apply to everyone

Purpose

NOTE: The fields in the window are context sensitive; they change based on the actions you choose.

4 Note that the **Enable this Filter** checkbox is checked by default. Uncheck the box to create rules that do not go into effect immediately.

5 Choose whether the filter matches **All** of the conditions or **Any** of the conditions

- **All**—Causes email to be filtered only when *all* of the filter conditions apply (logical AND)
- **Any**—Causes email to be filtered when *any* single condition applies (logical OR)

6 In the **Select** field, choose the parts or types of message to filter See the following table for more information:

Select	Definition
Spam/Phishing Judgment	Filters messages based on the judgment that it is spam or phishing attempts.
Likely Spoof Judgment	Filters on messages based on the judgment that it is a Likely Spoof attempt.

Select	Definition
Address Book	For any email coming is the policy first checks to see if the email address is a valid address in the address book, then takes further action based on how the policy is defined.
From & MAIL FROM	Examines both envelope and header **From** fields for a match.
To/Cc/Bcc & RCPT TO	Examines both envelope **To** field and header **To/Cc/Bcc** fields for a match.
Subject	Filters by words in the subject
From	Filters by sender's name or portion of a sender's name.
To	Examines the To header field for a match.
CC	Examines the **CC** header field for a match.
Reply-To	Examines the **Reply-To** header field for a match.
Envelope MAIL FROM	Examines the **MAIL FROM** envelope field for a match.
Envelope RCPT TO	Examines the **RCPT TO** envelope field for a match.
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 headers	Filter by the RFC822 information in the message header fields, which includes information like 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
Attachment Type	Filter based on type of attachment
Country Code	Filter based on sender's country code
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
Source IP	Filter messages based on the sender's IP address
Single Message Header	Filter messages containing a single message header
Originating IP	Filter messages based on the IP address from where the message was sent

7 Choose the matching operation in the **Matching** field. The matching options vary based on the filtering option you selected.

8 Enter the value you want to filter in the **Search Value** text box, or select one of the other options listed, if enabled:

- **Use dictionary** and **Use record ID** are part of the Compliance Subscription License.

> ⓘ **NOTE:** If the Compliance Subscription License is active, the administrator has additional filtering conditions that can be set. The **Use dictionary** option of using terms from a dictionary can be selected, as well as the **Use Record ID** option which looks for numbers such as telephone numbers or social security numbers.

- **Use Attachment Type** allows you to select a specific type of file attachment. About 137 files types are listed.
- **Use Country Code** allows you to select the country code you want to filter on.

9 Select the appropriate check boxes to further refine your search:

- **Match Case**—Filters a word or words sensitive to upper and lower case.
- **Disguised Text Identification**—Filters disguised words through the sequence of its letters, for example Vi@gr@.

ⓘ **NOTE: Disguised Text Identification** cannot be used with **Match Case** and can be selected only for Body and Subject message parts.

10 Click the **+** icon if you want to add another layer of filtering.

You can add up to 20 layers. Filter layers are similar to rock sifters: Each additional layer adds further filtering that tests email for additional conditions.

11 Under **Perform the following actions**, select the response from the **Action** drop down list. The following table describes the available response actions:

Action	Effect
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.
Deliver and skip Spam and Phishing Analysis	The message is delivered without spam or phishing analysis.
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 Approval Box	The email message is stored in the Approval Box. It will not be delivered until an administrator approves it for delivery.
Reject with SMTP error code 550	The message is returned to sender with an error message indicating that it was not deliverable.
Deliver and reject with SMTP error code 550	The message is delivered to the recipient and is bounced back to the sender with an error message.
Route to	The message is routed to the specified email address. The message can be routed to only one email address.
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
Route to IP	The message is routed to the specified IP address. The message can be routed to only one IP address.
Deliver and Route to IP	Deliver to the recipients and also route to the specified IP address. The message can be routed to only one IP address.
Encrypt	Message is sent to the encryption center for encryption. This action is used for outbound messages. The administrator must provide a name or IP address of SMTP server for encryption at the Policy & Compliance > Compliance Module > Encryption page.
Decrypt	Message is sent to the decryption center for decryption. This action is used for inbound messages. The administrator must provide a name or IP address of SMTP server for encryption at the Policy & Compliance > Compliance Module > Encryption page.
Route to Encryption Service	Message is sent for encryption to protect private information.
Tag subject with	The subject of the email is tagged with a the specified term.

Action	Effect
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 an X-header to the email.
Remove X-header from message	Removes an X-header from an email.
Skip Capture	Message is not sent for Capture analysis.

12 Select the **Stop processing policy filters** checkbox when no additional filtering is required on a message. This check box is automatically selected and grayed out when you have selected a terminal action.

13 If additional actions need to be performed on the same message, select the **+** icon 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 is not available in the drop down list for further selection within the current filter rule.

14 Type a descriptive name in the **Filter Name** text box.

15 Select a policy group you want to apply this filter to. By default, **Apply to everyone** is selected and this filter applies to all email messages.

16 Add a brief description to the **Purpose** text box.

17 Click the **Save This Filter** button.

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, Email Security does not support adding text strings to email messages in languages other than English and does not support foreign language filter names.

Managing Filters

The Filters page lists all the filters created in the system for the **Inbound** and **Outbound** path. They are processed in the order they are listed.

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 check mark.

To change a filter that has been saved:

1 On the **MANAGE | Policy & Compliance > Filters** page, select the **Inbound** or **Outbound** view (wherever the filter is located).

2 Select the **Edit** button adjacent to the filter to be changed.

3 Change any of the filter conditions.

4 Select **Save This Filter**.

To delete a filter:

1 Select the **Delete** button adjacent to the filter.

2 Confirm your choice when asked.

To change the order of the filters:

1. Drag and drop the filter in the order you prefer.

Advanced Filtering

This section contains various advanced configuration examples related to Filters:

- Creating a Multi-Layered Filter
- Creating an Outbound Filter to Add a Company Disclaimer
- Configuring a Policy Filter for Inbound Email
- Exclusive Actions
- Parameterized Notifications

Creating a Multi-Layered Filter

You can create filters with multiple conditions chained together and multiple actions 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 multi-layered filter like the example above:

1. Click the Add New Filter button from the **Policy & Compliance > Filters > Inbound** page.
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**. **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].
7. Verify that the **Stop processing policy filters** check box is not enabled.
8. Select the **+** icon to the right to add another action.
9. Select the action **Route To** and set the **To** field to `engineering@company.com`.
10. Select the S**top Processing Policy Filters** check box to stop further policy filtering on this message.
11. Select the **Save This Filter** button.

Creating an Outbound Filter to Add a Company Disclaimer

This section provides steps to add a company disclaimer to the end of each outgoing message from your organization. In this example, if email is sent from anyone at sonicwall.com, the following message is appended to the end of the message: `This is my company disclaimer`

To create the outbound policy filter:

1. In the SonicWall management interface, navigate to the **Policy & Compliance > Filters** screen, and click the **Outbound** tab.
2. Click the **Add New Filter** button.
3. Select **All** conditions to be met.
4. Select **From** in the **Select** drop down list.
5. Select **Contains** in the Matching drop down list.
6. Type **`sonicwall.com`** In the **Search Value field**.
7. To protect against internal spammers or zombies, click the **+** icon to add another condition.
8. Select **Spam/Phishing Judgement** from the **Select** drop down list.
9. Select **is good** in the **Matching** drop down list.
10. Select the action **Append text to message**.
11. In the **Message text** type: **`This is my company disclaimer.`**
12. Type the **Filter Name**: **`Outbound Disclaimer`**.
13. Select **Apply to Everyone** from the drop down menu for the **Apply this filter to** field.
14. Add a brief description to the **Purpose** Text field: for example, **`Adds a company disclaimer to outgoing mail`**.
15. Click the **Save This Filter** button.

Configuring a Policy Filter for Inbound Email

To filter email messages sent to your organization that are not judged as spam but contain the words “job application” in the subject or body of the email message, follow the procedures listed:

If an email is:

- not judged as spam and
- the subject or body of the email contains the words job application,

then take the following actions:

- route the email to hr@sonicwall.com

To create the inbound policy filter like the example above:

1. Click the **Add New Filter** button under the **Inbound** tab.
2. Select **All** conditions to be met.
3. Select **Spam/Phishing Judgement** operation.
4. Set **Matching** to **is not spam**.
5. Select the **+** icon to add another condition.
6. Select the **Subject or Body** option from the drop down list.

7 Set **Matching** to **with specific phrase**.

8 Type the words `job application` in the **Search value** field.

9 Select the action **Route to**.

10 Enter the email address `hr@sonicwall.com` in the **To** field.

11 Name the filter `Resume Routing`.

12 Select **Apply to Everyone** from the drop down menu in the **Apply this filter to** section.

13 Add a brief description to the **Purpose** Text field.

14 Select the **Save This Filter** button.

Exclusive Actions

Exclusive actions are terminal in nature and no further policy filtering is possible after this action has been performed. The **Stop Processing Policy Filters** check box is automatically enabled and grayed out if an exclusive action is selected.

Parameterized Notifications

Email Security supports parameterized notifications where you can use pre-defined parameters in the text fields for the Issue Email Notification action. These parameters 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. Parameters for Notifications provides more details.

Parameters for Notifications

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_RECORDID%	the Record ID file name which has a matching pattern in the triggering email
%MATCHED_TERM%	the Dictionary term which matched in the triggering email

Policy Groups

In some cases, you may want 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.

> ⓘ **NOTE:** For administrative purposes, a user is a member of only one group. If a user is a member of more than one group, that user is treated as if they were only a member of the first group in the list.

Topics:

- Adding a New Policy Group
- Removing a Policy Group
- Listing Members

Adding a New Policy Group

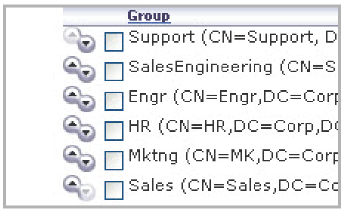
To add a new policy group:

1. Navigate to **Policy & Compliance > Policy Groups** on the **MANAGE** view.
2. Select the **Add Group** button.
3. If managing policy groups from multiple LDAP servers, select the source for the groups lists from the **Using Source** drop-down list and click **Go**.
4. From the **Find all groups** drop-down list, select one of three methods to locate a desired group:
    - **equal to (fast)**—search using the actual name, which is a faster search
    - **starting with (medium)**—search using the first few characters, which may take more time
    - **containing (slow)**—search using a substring of characters, which is the slowest search
5. Type a search string in the text box and click **Go**.
6. Once the list of group names is displayed, check the box of the group or groups you wish to add.
7. Click on the **Add Group** button. The group appears in table on the main page.

Removing a Policy Group

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 a 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.


Group

- □ Support (CN=Support, D
- □ SalesEngineering (CN=S
- □ Engr (CN=Engr,DC=Corp
- □ HR (CN=HR,DC=Corp,D
- □ Mktng (CN=MK,DC=Corp
- □ Sales (CN=Sales,DC=Cc

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 is applied to email messages for jdoe@company.com.

Listing Members

You can view a list of the members of a specific policy group.

1. Navigate to **Policy & Compliance > Policy Groups** on the **MANAGE** view.
2. Check the box by the group name you want to see.
3. Select **List Members**.
4. Close the window when done.

Compliance

The **Policy & Compliance > Compliance** page on the **MANAGE** view is accessible through the optional purchase of a Compliance Subscription License Key. It helps organizations ensure that email complies with relevant regulations and/or corporate policies. Once the Compliance Module is activated, the network administrator has access to the Encryption and Archiving features as well as additional filtering tools that enhance the standard module.

When the Compliance Module license expires, filters that were created during the valid license period continue to work, taking advantage of the advanced features. However, the administrator cannot add any new filters until the Compliance Subscription License Key us renewed.

Topics:

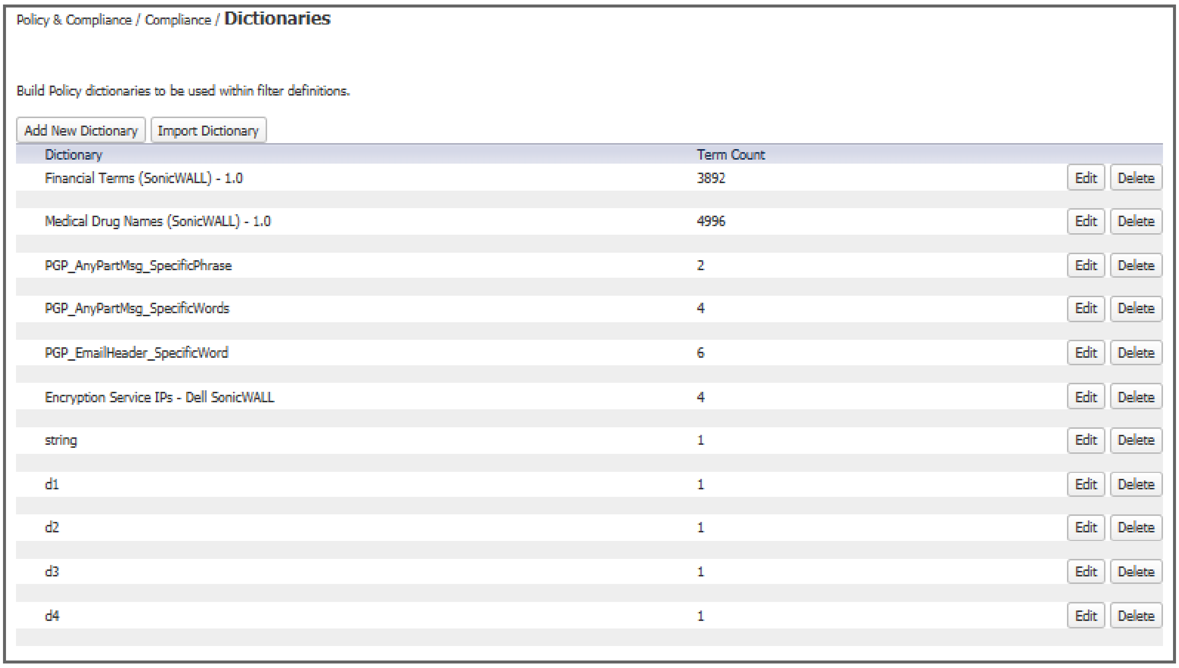
- Dictionaries
- Approval Boxes
- Encryption
- Record ID Definitions
- Archiving

Dictionaries

A dictionary is a convenient collection of words or phrases that you can group together for use in policy filters. A dictionary can be specified as a search value in a policy filter. Dictionaries can be created or modified manually or by importing from a file on the file system.

A predefined dictionary is a group of words or phrases all belonging to a specific theme such as medical or financial terms, which can be used as a database of words that filters can look for. By default, SonicWall provides these pre-installed dictionaries, which can be modified by clicking on the **Edit** button.

- Financial Terms
- Medical Drug Names
- Encryption Service IPs



Policy & Compliance / Compliance / **Dictionaries**

Build Policy dictionaries to be used within filter definitions.

Dictionary	Term Count		
Financial Terms (SonicWALL) - 1.0	3892	Edit	Delete
Medical Drug Names (SonicWALL) - 1.0	4996	Edit	Delete
PGP_AnyPartMsg_SpecificPhrase	2	Edit	Delete
PGP_AnyPartMsg_SpecificWords	4	Edit	Delete
PGP_EmailHeader_SpecificWord	6	Edit	Delete
Encryption Service IPs - Dell SonicWALL	4	Edit	Delete
string	1	Edit	Delete
d1	1	Edit	Delete
d2	1	Edit	Delete
d3	1	Edit	Delete
d4	1	Edit	Delete

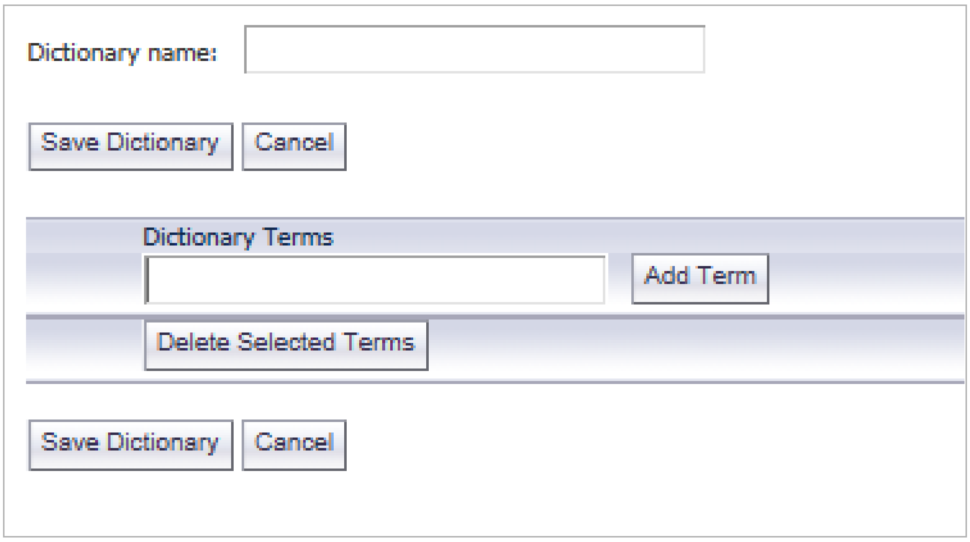
Topics:

- Add New Dictionary
- Import Dictionary
- Delete Dictionaries or Terms

Add New Dictionary

To manually add a dictionary:

1 Click on the **Add New Dictionary** button.



2 Type the new dictionary name in the **Dictionary name** field.

3 Enter a word or phrase in the **Dictionary Terms** text field.

4 Select **Add Term**.

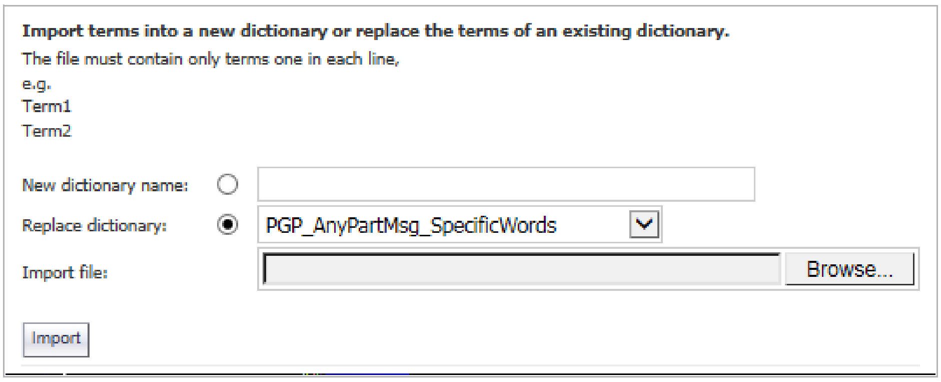
5 Repeat for all the terms you want to add to the dictionary.

6 Click **Save Dictionary**.

Import Dictionary

To import a dictionary from a file on the file system:

1 Click on the **Import Dictionary** button.



Import terms into a new dictionary or replace the terms of an existing dictionary.

The file must contain only terms one in each line,

e.g.
Term1
Term2

New dictionary name: ○

Replace dictionary: ● PGP_AnyPartMsg_SpecificWords

Import file:

2 Choose **New dictionary name** or **Replace dictionary** by selecting the appropriate button next to your selection.

3 Find the import file by selecting **Browse...** and navigating to the correct location.

The imported file should contain one word or phrase per line and each line should be separate by a carriage return.

4 Click the **Import** button.

Delete Dictionaries or Terms

To delete a dictionary:

1 Navigate to **Policy & Compliance | Compliance > Dictionaries** on the **MANAGE** view.

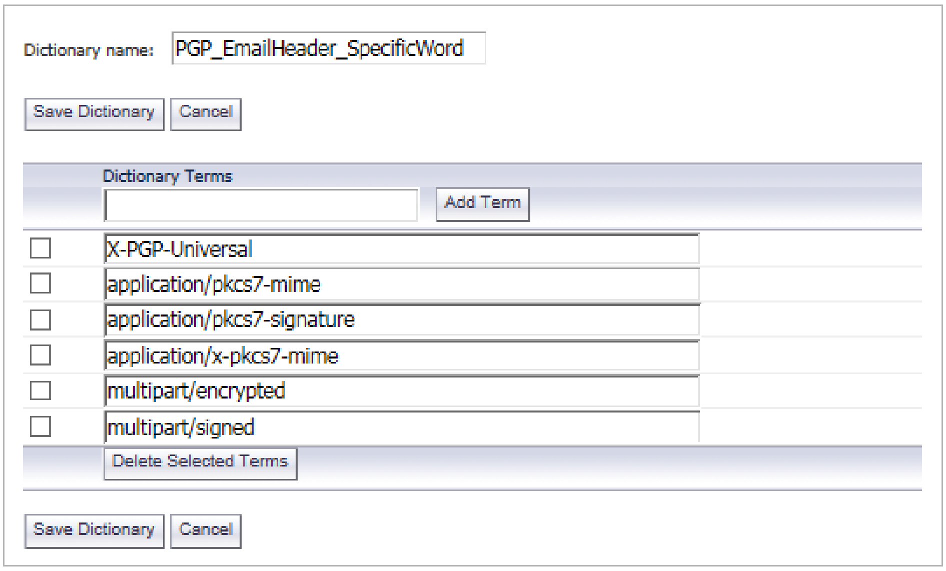
2 Select the **Delete** button for the dictionary you want removed.

3 Confirm your intention to delete that dictionary when asked.

To delete terms from a dictionary:

1 Navigate to **Policy & Compliance |Compliance > Dictionaries** on the **MANAGE** view.

2 Select the **Edit** button for the dictionary whose terms you want to remove.



Dictionary name: PGP_EmailHeader_SpecificWord

Dictionary Terms

☐ X-PGP-Universal
☐ application/pkcs7-mime
☐ application/pkcs7-signature
☐ application/x-pkcs7-mime
☐ multipart/encrypted
☐ multipart/signed

3 Check the box by the terms you want to delete.

4 Select **Delete Selected Terms** (you may need to scroll to the bottom of the list to see this button).

5 Select **Save Dictionary** save the changes.

Approval Boxes

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

To see a list of the Approval Boxes that have been created, select **Approval Box Manager** from the drop down list in the **View** field. The **Approval Box Manager** view allows you to edit or delete existing Approval Boxes, and to create new Approval Boxes.

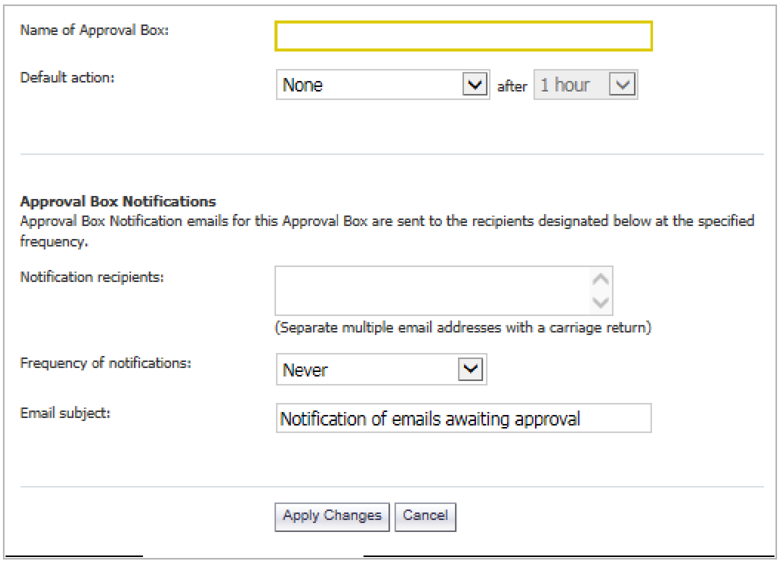
To see the contents of a particular Approval Box, choose the desired Approval Box name from the table. This page allows you to search the messages stored in that Approval Box and to take action on any of those messages.

ⓘ **NOTE:** Only users who have administrative rights can see the contents of an approval box. See Users, Groups & Organizations for managing user rights and privileges.

To set up an Approval Box:

1 Navigate to **Policy & Compliance |Compliance Module > Approval Boxes** on the **MANAGE** view.

2 Create the Approval Box by selecting **Add New Approval Box**.



Name of Approval Box:

Default action: None after 1 hour

Approval Box Notifications

Approval Box Notification emails for this Approval Box are sent to the recipients designated below at the specified frequency.

Notification recipients:

(Separate multiple email addresses with a carriage return)

Frequency of notifications: Never

Email subject: Notification of emails awaiting approval

3 Enter the **Name of Approval Box**. This name appears in the approval box table and in the drop down list that allows you to select the detailed view of individual approval boxes.

4 From the **Default action** drop down list, select an action to be taken. This action is automatically taken on the message waiting for approval if the administrator does not respond to the notification within the time specified.

None	No action is taken. The email remains in the Approval Box.
Approve & Deliver	The email is passed to the recipient.
Delete	The email is deleted.
Bounce Back to Sender	The email is automatically bounced back to the sender and removed from the Approval Box after the specified length of time elapses.

5 Select the amount of time the messages are held in the Approval Box before action is automatically taken. The time values range from 1 hour to 30 days.

6 Enter a list of Notification recipients in the text box. Separate multiple email addresses with a carriage return.

ⓘ **NOTE:** Make sure that the email recipients you list are users that have administrative rights to the SonicWall server. If they do not have administrative access, they cannot view the approval boxes when they receive email notification.

7 Select a **Frequency of notifications** value from the drop down list for this approval box. Email notification is sent according to the schedule you choose here.

8 Write the **Email subject** line for this notification, like `Notification of emails awaiting approval`.

9 Click the **Apply Changes** button to save your changes.

10 Navigate to the **Policy & Compliance | Filters** page.

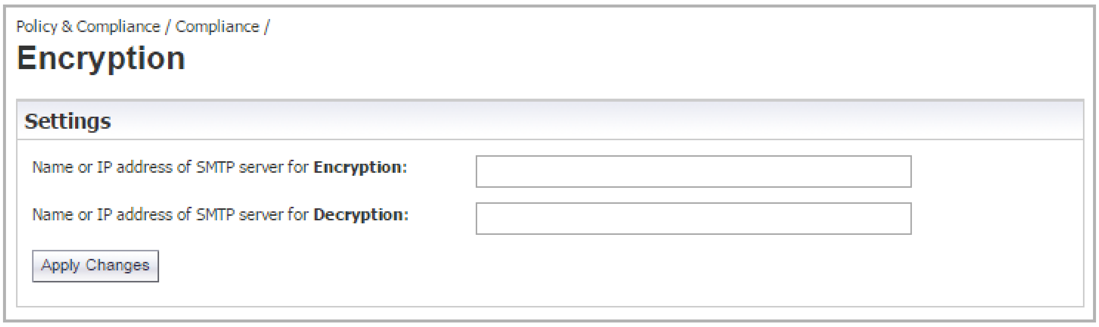
11 Create a policy filter that sets the **Action** to **Store in Approval Box**.

12 Choose the desired Approval Box for email messages caught by that filter.

Encryption

Use the **Policy & Compliance | Compliance Module > Encryption** section to configure the servers used to encrypt and decrypt messages. Once configured, you may create a policy filter for which the action is to encrypt or decrypt messages.

A policy action of encrypt can be used to direct confidential outbound messages to the encryption server. A policy action of decrypt can be used to direct confidential inbound messages to the decryption server.



Policy & Compliance / Compliance /

Encryption

Settings

Name or IP address of SMTP server for **Encryption**:

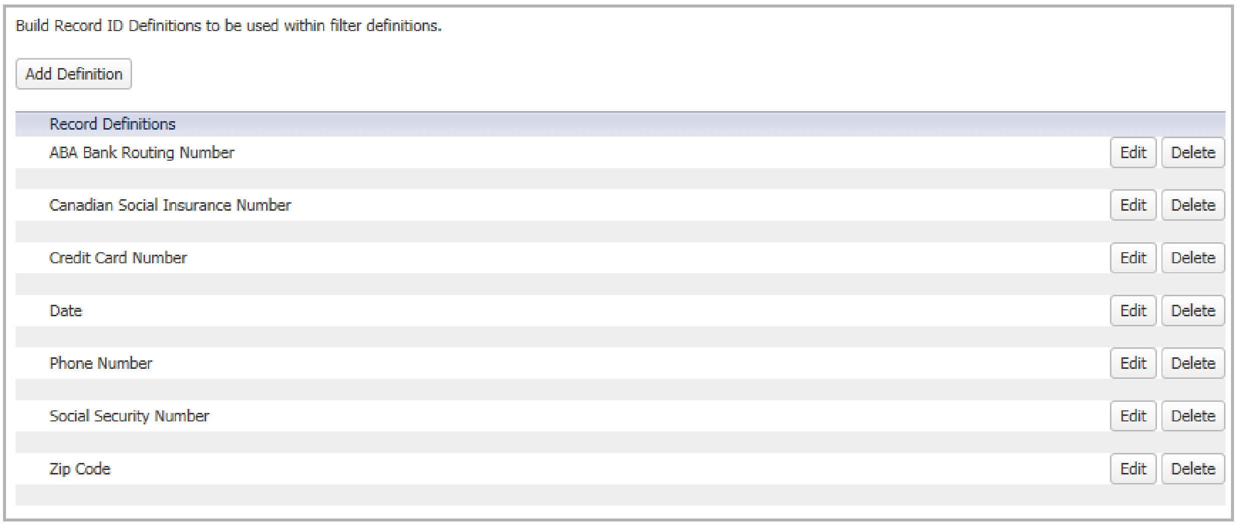
Name or IP address of SMTP server for **Decryption**:

Record ID Definitions

Record ID Definitions can be used to detect specific IDs described by a series of generic patterns. The P**olicy & Compliance | Compliance Module > Record ID Definitions** section allows the administrator to define a cluster or clusters of letters and numbers into logical sets of groups such as social security numbers, patient medical record numbers, or credit card numbers. When these patterns are discovered, compliance actions can be taken to ensure that the organization's privacy and security regulations are met. The filter stops processing a message after it finds the first matching Record ID Definition.

By default, Email Security provides the following Record ID Definitions pre-installed:

- ABA Bank Routing Number
- Canadian Social Security Number
- Credit Card Number
- Date
- Phone Number
- Social Security Number
- Zip Code



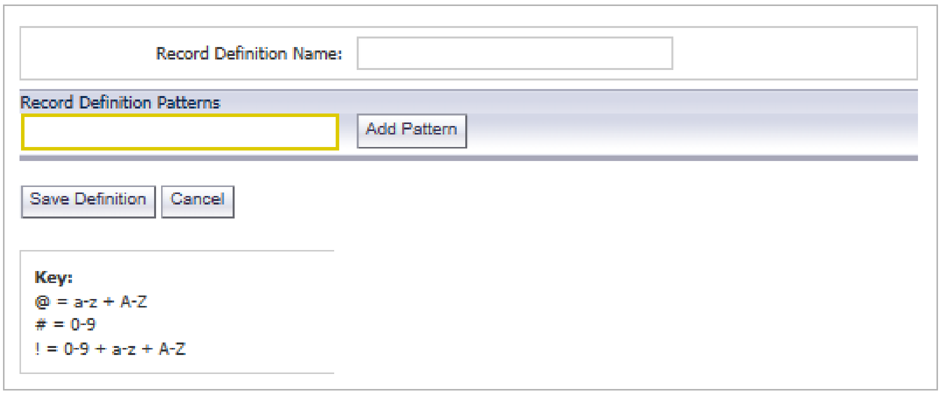
Build Record ID Definitions to be used within filter definitions.

Record Definitions		
ABA Bank Routing Number	Edit	Delete
Canadian Social Insurance Number	Edit	Delete
Credit Card Number	Edit	Delete
Date	Edit	Delete
Phone Number	Edit	Delete
Social Security Number	Edit	Delete
Zip Code	Edit	Delete

To add a new Record ID Definition:

1 Navigate to the **Policy & Compliance | Compliance > Record ID Definitions** page.

2 Click the **Add New Record ID Definition** button.



Record Definition Name:

Record Definition Patterns

Key:
@ = a-z + A-Z
= 0-9
! = 0-9 + a-z + A-Z

3 Enter a name in the **Record Definition Name** field.

4 Enter a **Records Definition Pattern**, including correct spacing, dashes or other symbols. Use the key to set values to the sets of characters.

5 Click **Add Pattern** to add the term to the Record ID. Repeat this step for each Record ID as necessary.

6 Select **Save Definition** when finished.

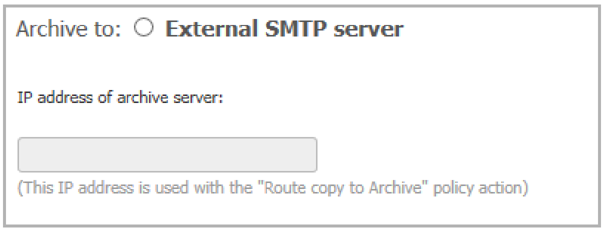
Archiving

The **Policy & Compliance | Compliance > Archiving** section on the **MANAGE** view is used to configure how messages are archived. Once configured, you may create a policy filter for which the action is **Route copy to archive**. Messages can be archived either to a remote archive server or to a file system.

Archiving to an External SMTP Server

To archive messages to an external SMTP server:

1 Navigate to the **Policy & Compliance | Compliance > Archiving** page on the **MANAGE** view.



Archive to: ○ External SMTP server

IP address of archive server:

(This IP address is used with the "Route copy to Archive" policy action)

2 Select the **External SMTP Server** option.

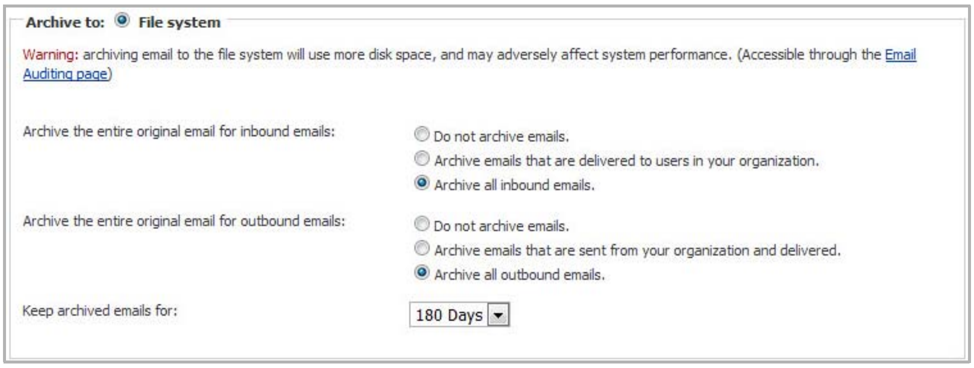
3 Enter the **IP address of archive server** where email messages should be routed for archiving. This IP address is used with the **Route copy to archive** policy action.

Archiving to a File System

To archive messages to a file system:

1 Navigate to the **Policy & Compliance | Compliance > Archiving** page on the **MANAGE** view.

2 Click the **File system** option.



Archive to: ● File system

Warning: archiving email to the file system will use more disk space, and may adversely affect system performance. (Accessible through the Email Auditing page)

Archive the entire original email for inbound emails:
○ Do not archive emails.
○ Archive emails that are delivered to users in your organization.
● Archive all inbound emails.

Archive the entire original email for outbound emails:
○ Do not archive emails.
○ Archive emails that are sent from your organization and delivered.
● Archive all outbound emails.

Keep archived emails for: 180 Days

3 Select the archive settings for both inbound and outbound emails. The following options are available:

- **Do not archive emails**—Email messages are not archived.
- **Archive emails that are delivered to users in your organization**—Email messages that are delivered are archived. Quarantined email messages are not archived.
- **Archive all <inbound/outbound> emails**—All emails are archived, including those that are quarantined in the Junk Box.

4 Select a length of time for emails to be archived. Values range from 1 Day to 7 Years.

5 Select **Apply Changes**.

9

System Setup | Server

This section provides configuration procedures for server administration and settings.

Topics:

- Administration
- LDAP Configuration
- Updates
- Monitoring
- Host Configuration
- Advanced

Administration

You can manage the following key settings on the **Server > Administration** page:

- Email Security Master Account
- User Interface Preference
- Password Policy
- Invalid Login Policy
- Login Custom Text
- Allow Admin Access from Specific IPs
- Quick Configuration

Email Security Master Account

Change the master account username and password in the Email Security Master Account section.

ⓘ | **NOTE:** SonicWall strongly recommends that you change the master account password.

To change the password:

1. Navigate to Email Security **Master Account** section of the **Server > Administration** page on the **MANAGE** view. Note that the **Username** you originally registered with appears as the default Username.
2. Type in the **Old Password**.
3. Type in the **New Password**.
4. Type the same new password in the **Confirm password** field.

5. Click **Apply Changes**.

User Interface Preference

The user interface was enhanced in the Email Security 9.1 release. The new menu structure aligns commands under the key functions of **MONITOR**, **INVESTIGATE**, and **MANAGE**. Related commands are grouped on the left-hand menu under divider labels for easier navigation.

In the **User Interface Preference** section, you can choose which interface you want to use. The **Enhanced** interface is the default, but you can select **Classic** if you prefer the old interface. Be sure to **Apply Changes** if you change the setting.

A table that maps the old interface to the new interface is provided in Interface Map.

Password Policy

You can define the requirements for a secure password policy in this section.

To configure the password policy for users:

1. Navigate to the **Password Policy** section of the **Server > Administration** page on the **MANAGE** view.
2. Check the box to enable the following parameters. Leave unchecked if you don’t want to require that feature.
    - Require upper case characters: A-Z
    - Require lower case characters: a-z
    - Require numeric characters: 0-9
    - Require special characters: ~!@#$%^&*_-+='|(){}[]"<>,.?/
    - Allow OU Admins to change password policy
3. Set the minimum number of characters required for passwords in the **Minimum password length** field.
4. From the drop down list, select the amount of hours after which the Change Password link expires. If the user has not accessed the link within the amount of hours selected, a new Change Password link needs to be sent.
5. Click **Apply Changes**.

Invalid Login Policy

You can configure a user lockout feature, locking out user accounts if the number of unsuccessful attempts to login is reached on the Invalid Login Policy section.

> **NOTE:** The Invalid Login Policy is only available if the Global Administrator configures this feature for all users. Locked out users are displayed on the page at **System Setup | Server > Users, Groups & Organizations > Users** on the **MANAGE** view.

To configure the invalid login policy:

1. On the **System Setup | Server > Administration** page, navigate to the **Invalid Login Policy** section.

2 Specify the number of invalid attempts allowed before the user account is locked in the **Number of unsuccessful attempts before lockout** field. The default value is 5, but can range between 0-9. If the value is set to 0, the feature is disabled.

3 Specify the amount of time the user account is locked in the **Lockout Interval** field.

The user has to wait for this time interval to lapse before being able to login again; any correct or incorrect attempts are not be allowed. The default value is 15 minutes. The hours value can range from 0-72 hours, and the minutes value can range from 1-59 minutes.

4 Select the **Alert administrator when account is locked** check box to alert the administrator with an message when an account is locked.

5 Click **Apply Changes**.

To reset a locked out account:

1 Go to the **System Setup | Users, Groups & Organizations > Users** page.

2 Scroll down to **Locked Users**.

3 Select the user and click **Unlock User**.

Login Custom Text

To customize the text that appears when users log into Email Security:

1 Navigate to the **Server > Administration** page.

2 Scroll to the **Login Custom Text** section.

3 Enter custom text in the space provided.

4 Select **Apply Changes**.

Allow Admin Access from Specific IPs

This feature allows the administrator to add restricted IP addresses or address ranges. This restricts administrators so that they have admin access only from those specific IP addresses. The IP addresses can be entered in these formats: IPv4, IPv6, or IPv4 CIDR. Multiple IPs can be entered but must be separated by commas.

ⓘ | **IMPORTANT:** Users with admin roles can be locked out of web access if the incorrect IPs are specified.

Quick Configuration

Most organizations that are using SonicWall Email Security can configure their system by using the Quick Configuration option, located at the bottom of the **System Setup | Server > Administration** page. Note that you must configure the same choices for message handling for each SonicWall appliance to use Quick Configuration. For more complex installations and advanced options, use the appropriate options in the left-hand side under **System Setup** and **Security Services**.

LDAP Configuration

SonicWall Email Security 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 on your mail server, this information is automatically reflected in Email Security in real time.

Many enterprise networks use directory servers like Active Directory or Lotus Domino to manage user information. These directory servers support LDAP, and Email Security can automatically get user information from these directories using LDAP. You can run SonicWall Email Security without access to an LDAP server as well.

ⓘ **NOTE:** 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 uses the following data from your mail environment:

- **Login Name and Password**

  When users attempt to log into the Email Security server, their login name and password are verified against the mail server using LDAP authentication. Therefore, changes made to the usernames and passwords are automatically uploaded to SonicWall Email Security in real time.

- **Multiple Email Aliases**

  If your organization allows users to have multiple email aliases, Email Security 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**

  Email groups or distribution lists in your organization are imported into SonicWall Email Security. 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. SonicWall recommends completing the LDAP configuration 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.

The default view for the LDAP Configuration page shows the **Available LDAP Servers** section expanded and the other sections (Global Configurations, Server Configuration, LDAP Query Panel, and Add LDAP Mappings) minimized. The **Available LDAP Servers** lists the LDAP servers that have been configured and provides the option to add, edit, or delete a server.

Configuring LDAP

Configuring the LDAP server is essential to enabling per-user access and management. These settings are limited according to the preferences set in the User Management pane.

To add an LDAP server or configure an existing server:

1. Navigate to the **Server > LDAP Configuration**.
2. Click the **Add Server** button to add a new LDAP Server or select the **Edit** icon to dedit a server’s configuration. The Server Configuration section of the page opens.

   ⓘ **NOTE:** When the **Server Configuration** section is expanded to allow editing, the **LDAP Query Panel** and **Add LDAP Mappings** sections are also enabled for editing.

Server Configuration

To configure or edit a server:

1 Check one of the following boxes that appear under the **Settings** section:

- **Show Enhanced LDAP Mappings fields**—Select this option for Enhanced LDAP or LDAP Redundancy. You have to specify the Secondary Server IP address and Port number.
- **Auto-fill LDAP Query fields when saving configurations**—Select this option to automatically fill the LDAP Query fields upon saving.

2 Enter the following information under the **LDAP Server Configuration** section:

- **Friendly Name**—The friendly name for your LDAP server.
- **Primary Server Name or IP address**—The DNS name or IP address of your LDAP server. (Configuration checklist parameter M)
- **Port number**—The TCP port running the LDAP service. The default LDAP port is 389. (Configuration checklist parameter N)
- **LDAP server type**—Choose the appropriate type of LDAP server from the drop down list.
- **LDAP page size**—Specify the maximum page size to be queried. The default size is 100.
- **Requires SSL**—Select this check box if your server requires a secured connection.
- **Allow LDAP referrals**—Leaving this option unchecked disables LDAP referrals and speed up logins. You may select this option if your organization has multiple LDAP servers in which the LDAP server can delegate parts of a request for information to other LDAP servers that may have more information.

3 In the **Authentication Method** section, specify if the LDAP login method for your server is by **Anonymous Bind** or **Login**.

4 Specify the **Login name** and **Password**. This is the credential used to allow a user access to the LDAP resource. It may be a regular user on the network, and does not have to be a network administrator.

> ⓘ **NOTE:** Some LDAP servers allow any user to acquire a list of valid email addresses. 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.

5 Click the **Test LDAP Login** 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.

6 Click **Save Changes**.

Global Configurations

In the **Global Configurations** section, you define settings that apply universally across all LDAP server configurations. Click on the circle beside the title to expand the section and define the settings.

Domain Aliases

You can require that end users authenticate using an alias. For Active Directory servers the pseudo-domains are the LDAP configuration friendly names paired with the NetBIOS domain name. It is otherwise the same as the LDAP friendly name. Any aliases created are made available in the drop-list on the logon screen.

The aliases can be alphanumeric, allowing up to 200 characters maximum. Some special characters are allowed, including hyphen, underscore, and dot, but no spaces. If a pseudo-domain has multiple aliases, separate each alias with a comma.

Settings

You can opt to **Show a list of domains to end users for authentication**. Just check the box to enable that feature.

You can also specify the number of minutes between refreshes of the list of users on the system by setting the **Usermap Frequency** field. Specify the value in minutes.

Select **Save Changes** when finished setting Global Configurations.

LDAP Query Panel

To access the **LDAP Query Panel** settings, click the Friendly Name link or the **Edit** button for the server you wish to configure. If the "Auto-fill LDAP Query Fields" check box is selected in the Settings section, the fields in the LDAP Query Panel section are automatically filled in with default values after the basic configuration steps are completed.

Query Information for LDAP Users

Email Security uses your existing Active Directory or LDAP server to authenticate groups as they log into their Junk Boxes. This LDAP configuration section must be filled out correctly to return the complete list of groups who are allowed to log into their Junk Box. If a group does not appear in this list, their email is still filtered, but they can not log in to the group junk box. Refer to the detailed field help for information on each of the text fields.

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.
   - **Use SMTP addresses only**—Select the check box to enable the use of SMTP addresses.
2. Click the **Test User Query** button to verify that the configuration is correct.
3. Click **Save Changes** to save and apply all changes made.

NOTE: Click the **Auto-fill User Fields** button to have SonicWall Email Security automatically complete the remainder of this section.

Query Information for LDAP Groups

Email Security uses your existing Active Directory or LDAP server to authenticate groups as they log into their Junk Boxes. This LDAP configuration section must be filled out correctly to return the complete list of groups who are allowed to log into their Junk Box. If a group does not appear in this list, their email is still filtered, but they can not log in to the group junk box. Refer to the detailed field help for information on each of the text fields.

If you have a large number of user mailboxes, applying these changes could take several minutes.

1 Enter values for the following fields:
   - **Directory node to begin search**—The node of the LDAP directory to start a search for users.
   - **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.

2 Click the **Test User Query** button to verify that the configuration is correct.

3 Click **Save Changes** to save and apply all changes made.

ⓘ **NOTE:** Click the Auto-fill Group Fields button to have SonicWall Email Security automatically complete the remainder of this section.

Add LDAP Mappings

SonicWall Email Security uses your existing Active Directory or LDAP server to authenticate end users as they log in to their personal Junk Boxes. The **Add LDAP Mappings** segment of the page must be correctly filled out to return the complete list of users who are allowed to log in to their Junk Box. If a user does not appear in this list, their email is filtered, but they can not log in to their personal junk box.

For the Microsoft Window Environment

In a Microsoft Windows environment, you need to specify the NetBIOS domain name, sometimes called the pre-Windows 2000 domain name.

To locate the NT/NetBios domain name:

1 Login to your domain controller.

2 Navigate to S**tart > All Programs > Administrative Tools > Active Directory Domains and Trusts**.

3 In the left pane of the Active Directory Domains and Trusts dialog box, highlight your domain.

4 Click **Action**.

5 Click **Properties**. In the domain's Properties dialog box on the General tab you should find the domain name or pre-Windows 2000 name.

To add the Windows NT/NetBIOS domain names:

1. Add the Windows NT/NetBIOS Domain Names into the field provided. Domain names can be made of up to 200 alphanumeric characters with hyphens and periods allowed.
2. Separate multiple domain names with a comma.
3. Click **Save Changes** to save the new domain names.

For the LDAP Environment

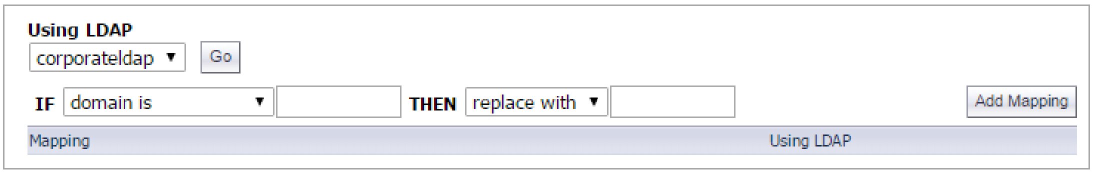
On some LDAP servers, such as Lotus Domino, some valid addresses do not appear in LDAP, for example, LDAP servers that only store the “local” or “user” portion of the email addresses. This section provides a way to add additional mappings from one domain to another. For example, a mapping could be added that would ensure emails addressed to anybody@engr.corp.com are sent to anybody@corp.com.

It also provides a way of substituting single characters in email addresses. For example, a substitution could be created that would replace all the spaces to the left of the “@” sign in an email address with a “-”. In this example, email addressed to Casey Colin@corp.com would be sent to Casey-Colin@corp.com.

NOTE: This feature does not make changes to your LDAP system or rewrite any email addresses; it makes changes to the way SonicWall Email Security interprets certain email addresses.

To add LDAP Mappings:

1. Scroll to the Conversion Rules section, and click **View Rules**.



2. From the first and second drop down list, choose one of the following combinations:

First drop down menu	Second drop down menu	Resulting action
domain is	**replace with**	The domain name typed in the first field is replaced with the domain name typed in the second field.
domain is	**also add**	When domain listed in the first field is found, the second domain is added to the list of valid domains.
left hand side character is:	**replace with**	The character typed in the first field is replaced with all characters to the left of the “@” sign in the email address.
left hand side character is:	**also add**	A second email address is added to the list of valid email addresses.

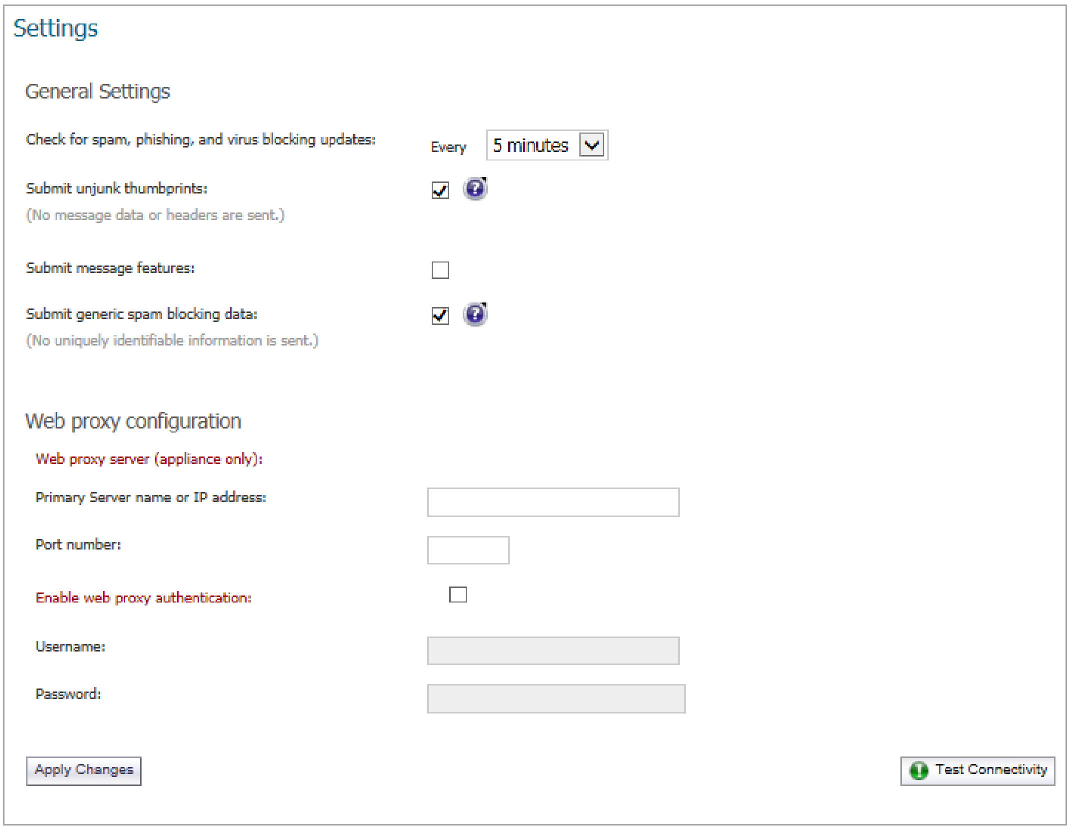
3. Enter text into the text fields as dictated by your choices.
4. Click the **Add Mapping** button.

Updates

SonicWall Email Security uses collaborative techniques as one of many tools to block junk messages. The collaborative database incorporates thumbprints of junked email from SonicWall Anti-Spam Desktop and users. Your server uses the HTTP protocol to communicate with SonicWall to download data used to block spam, phishing, viruses, and other evolving threats.

To configure settings for updates to the Email Security service:

1 Navigate to the **System Setup | Server > Updates** page.



Settings

General Settings

Check for spam, phishing, and virus blocking updates: Every 5 minutes

Submit unjunk thumbprints: ☑
(No message data or headers are sent.)

Submit message features: □

Submit generic spam blocking data: ☑
(No uniquely identifiable information is sent.)

Web proxy configuration

Web proxy server (appliance only):

Primary Server name or IP address:

Port number:

Enable web proxy authentication: □

Username:

Password:

2 From the drop-down menu select how often your system contacts SonicWall to **Check for spam, phishing, and virus blocking updates**.

The recommended frequency is 20 minutes. Setting this value too low generates unnecessary HTTP traffic. It may adversely affect the performance of your Email Security appliance or software and does not improve junk blocking effectiveness. Setting this value too high may result in less frequent updates, also causing junk blocking to be less effective.

3 Check the box for **Submit unjunk thumbprints** if you want to submit thumbprints to SonicWall when a user Unjunks a message.

Thumbprints sent to SonicWall contributes to the collaborative community by improving junk-blocking accuracy. Note that these thumbprints contain no readable information.

4 Check the box to **Submit message features**.

5 Check the box for **Submit generic spam-blocking data** if you want to help SonicWall customer support and help improve spam blocking.

No emails, email content, header information, or any other uniquely identifiable information is ever sent. Sample information that is sent includes: volume of messages processes and junked, success of various junking methods, and number of users protected.

To configure a web proxy server:

1. Specify the web proxy server **Primary Server name or IP address**.
2. Specify the **Port Number** for the web proxy server.
3. If you want to **Enable web proxy authentication** automatically, check the box and enter the **Username** and **Password**.
4. Click on **Apply Changes**.
5. Click the **Test Connectivity** button to verify that you successfully connected to the Data Center.

Monitoring

The **System Setup | Server > Monitoring** screen allows you to configure settings and alerts for system monitoring. Some of these fields may be pre-defined based on the information provided upon initial setup of Email Security.

ⓘ **NOTE:** If you are running SonicWall Email Security in split mode, and you route outbound email through Email Security, 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.

Topics:

- Configure System Monitoring
- Alert Suppression Schedule
- Miscellaneous
- Monitor Configure

Configure System Monitoring

You can set up Email Security to monitor certain parameters and notify key personnel.

To configure the Monitoring section:

1. Provide the **Email address of the administrator who receives emergency alerts** in the text box. Enter the complete email address: for example, user@example.com. Separate multiple email addresses with a comma.
2. Provide the Email address of administrator who receives outbound quarantine notifications.

   Notifications are not sent more than once every ten minutes. If this field is left blank, notifications are not sent.
3. If Email Security has been configured to be an MTA, specify the **Postmaster for the MTA**. This person receives notifications generated by the MTA. Notifications are not sent more than once every ten minutes.
4. If you want to **Use MX Record to deliver mail**, check the box.

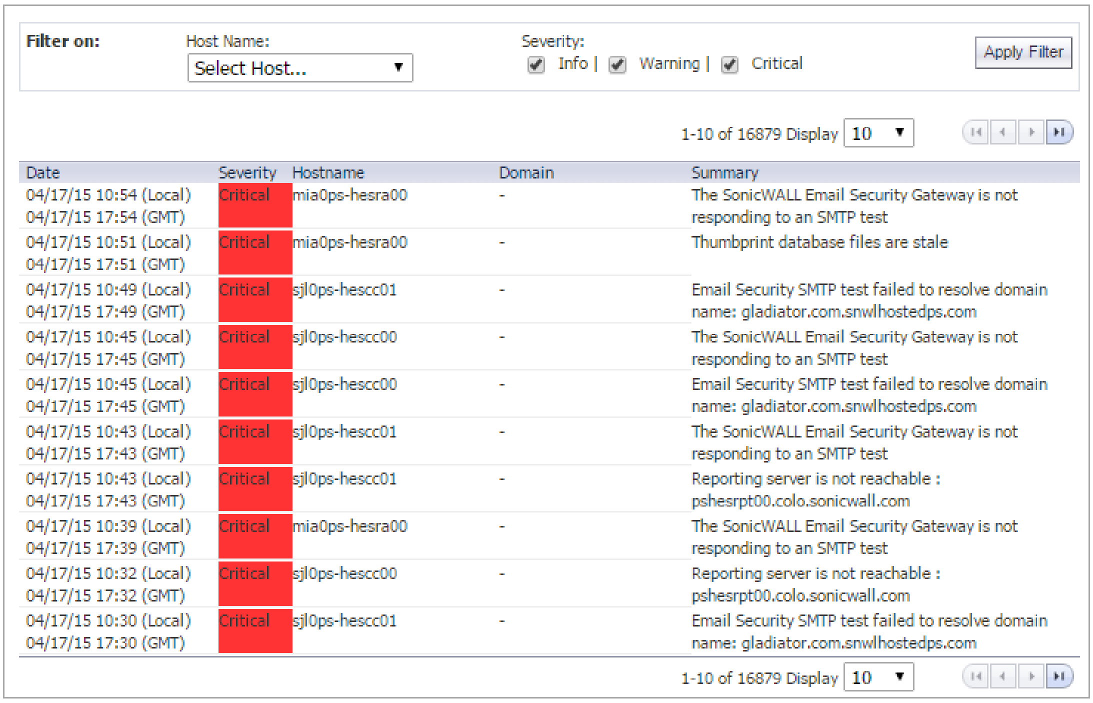
5 Enter the **Name or IP address of backup SMTP servers**. You may have one or more SMTP servers that are used as fallback servers to send alerts to if the configured downstream email server(s) cannot be connected. Separate multiple entries with a comma.

6 Enter a **Customized signature** to append at the end of your email messages.

7 Click on **Test Fallbacks** to test the name or IP address(es) listed as backup SMTP servers.

8 Click on **Apply Changes**. If you want to go back to prior settings click on **Revert**.

9 Click on **View Alerts** to view all configured alerts. You can filter by server or by host name. Time stamp and summary of the issue is also provided.



Filter on: Host Name: Select Host... Severity: ☑ Info | ☑ Warning | ☑ Critical

1-10 of 16879 Display 10

Date	Severity	Hostname	Domain	Summary
04/17/15 10:54 (Local) 04/17/15 17:54 (GMT)	Critical	mia0ps-hesra00	-	The SonicWALL Email Security Gateway is not responding to an SMTP test
04/17/15 10:51 (Local) 04/17/15 17:51 (GMT)	Critical	mia0ps-hesra00	-	Thumbprint database files are stale
04/17/15 10:49 (Local) 04/17/15 17:49 (GMT)	Critical	sjl0ps-hescc01	-	Email Security SMTP test failed to resolve domain name: gladiator.com.snwlhostedps.com
04/17/15 10:45 (Local) 04/17/15 17:45 (GMT)	Critical	sjl0ps-hescc00	-	The SonicWALL Email Security Gateway is not responding to an SMTP test
04/17/15 10:45 (Local) 04/17/15 17:45 (GMT)	Critical	sjl0ps-hescc00	-	Email Security SMTP test failed to resolve domain name: gladiator.com.snwlhostedps.com
04/17/15 10:43 (Local) 04/17/15 17:43 (GMT)	Critical	sjl0ps-hescc01	-	The SonicWALL Email Security Gateway is not responding to an SMTP test
04/17/15 10:43 (Local) 04/17/15 17:43 (GMT)	Critical	sjl0ps-hescc01	-	Reporting server is not reachable : pshesrpt00.colo.sonicwall.com
04/17/15 10:39 (Local) 04/17/15 17:39 (GMT)	Critical	mia0ps-hesra00	-	The SonicWALL Email Security Gateway is not responding to an SMTP test
04/17/15 10:32 (Local) 04/17/15 17:32 (GMT)	Critical	sjl0ps-hescc00	-	Reporting server is not reachable : pshesrpt00.colo.sonicwall.com
04/17/15 10:30 (Local) 04/17/15 17:30 (GMT)	Critical	sjl0ps-hescc01	-	Email Security SMTP test failed to resolve domain name: gladiator.com.snwlhostedps.com

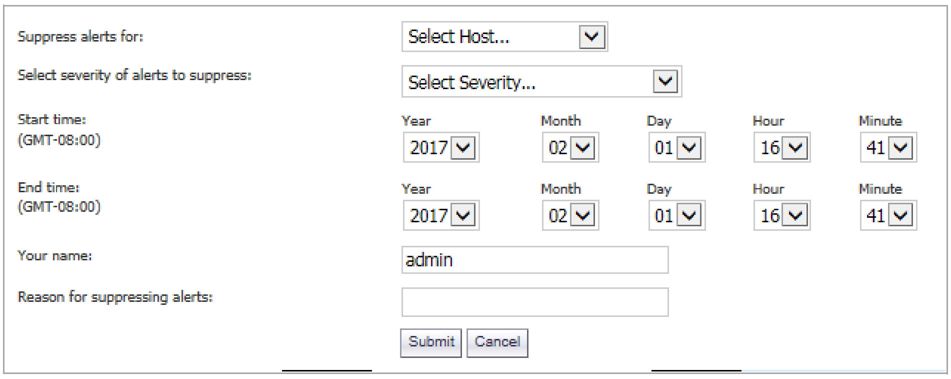
1-10 of 16879 Display 10

Alert Suppression Schedule

You can suppress alerts for short periods of time, for example, during a product maintenance window, if you want.

To suppress alerts:

1 Click on **Schedule Alert Suppression**.



Suppress alerts for: Select Host...

Select severity of alerts to suppress: Select Severity...

Start time: (GMT-08:00) Year 2017 Month 02 Day 01 Hour 16 Minute 41

End time: (GMT-08:00) Year 2017 Month 02 Day 01 Hour 16 Minute 41

Your name: admin

Reason for suppressing alerts:

2 Select the host that you want to **Suppress alerts for** from the drop-down list.

3 In the drop-down list for **Select severity of alerts to suppress**, choose on of the following options:

- Info Alerts
- Info + Warning Alerts
- Info + Warning + Critical Alerts.

4 Set the **Start time**.

5 Set the **End time**.

6 Enter **Your name**.

7 Enter the **Reason for suppressing alerts**.

8 Click **Submit** to finish setting an alert suppression schedule.

Miscellaneous

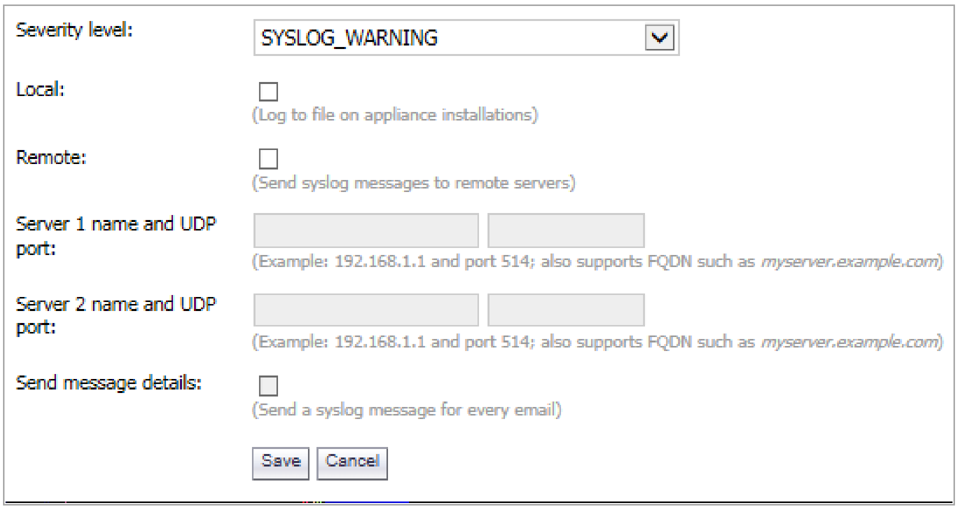
In the Miscellaneous section, configure the system logging and specify the age-out period for the alerts history logs.

To specify the age-out period:

1 Enter the number of days in the field provided for the **Age-out for alerts history logs**.

To configure system logging:

1 Click on Configure System Logging.



Severity level: SYSLOG_WARNING

Local: □ (Log to file on appliance installations)

Remote: □ (Send syslog messages to remote servers)

Server 1 name and UDP port: (Example: 192.168.1.1 and port 514; also supports FQDN such as *myserver.example.com*)

Server 2 name and UDP port: (Example: 192.168.1.1 and port 514; also supports FQDN such as *myserver.example.com*)

Send message details: □ (Send a syslog message for every email)

2 Set the lowest security level to be included in the alerts logs. Anything at that level and higher is sent to the syslog. For example, choosing the default level of SYSLOG_ALERT means that only messages of level SYSLOG_ALERT and SYSLOG_EMERGENCY are sent to the syslog. The following table lists the severity levels from highest to lowest.

NOTE: Logging lower severity messages means more data is logged.

SYSLOG_EMERGENCY	The system is unusable. Because this is the highest on the severity scale, this level minimizes the amount of logging.
SYSLOG_ALERT	Action must be taken immediately. This is the default severity level for the syslog.
SYSLOG_CRITICAL	Critical conditions.
SYSLOG_ERROR	Error conditions.
SYSLOG_WARNING	Warning conditions.
SYSLOG_NOTICE	Normal, but significant conditions.
SYSLOG_INFORMATIONAL	Informational messages.
SYSLOG_DEBUG	Debug-level messages. Because this is the lowest on the severity scale, this level maximizes the amount of logging.

ⓘ **NOTE:** The severity level chosen for the syslog is not related to the log level chosen for EMS logging on the **Server > Advanced** page.

3 Select where you want the logs to be written and stored:

- Check the **Local** box to write syslogs to the EMS server.

  ⓘ **NOTE:** For Windows software installations of Email Security, syslogs are written to the Windows Event Viewer. For Email Security appliances, syslogs are written to files on the EMS server. On appliances, syslog files may be downloaded from **Server > Advanced**.

- Check the **Remote** box to send syslogs to remote servers. Specify the IP addresses and ports of one or two servers to receive syslog messages. Port 514 is the recommended port for syslog.

  ⓘ **NOTE:** The second server is not a fallback server: if two servers are configured, syslogs are sent to both remote servers.

- If both **Local** *and* **Remote** are checked, syslogs are written locally and sent to remote servers.

  ⓘ **IMPORTANT:** If neither check box is checked, then syslogs are not written anywhere.

4 To send a syslog message for every email, check the box for **Send message details**. This option is available only if the syslog severity chosen is one of the lowest two levels, SYSLOG_INFO or SYSLOG_DEBUG

ⓘ **IMPORTANT:** If you receive a lot of email, choosing to send a syslog message for every email can result in a very large amount of data being sent to the syslog.

5 Click on **Save** to save your settings.

Monitor Configure

In this section, define the queue size alert. Make the following selections as needed:

- Set the **MTA Process Queue Size Alert** in the field provided.
- Select **Apply Changes** if you made changes to the queue size.
- Select **Apply Default Value** if you want to apply the default value of the queue size. The default value is 500.
- Select **Revert** to revert back to the prior queue

Host Configuration

On the **System Setup | Server > Host Configuration** page, you can make changes to the server on which the SonicWall Email Security product is installed. After applying these settings, you can then use the **Restart Services**, **Reboot this Server**, or **Shut Down Service** buttons at the top of the Host Configuration page.

ⓘ **NOTE:** On a Hosted Email Security solution, the button choices are somewhat different: select **Restart Services** or **Reboot this Server**.

Hostname

To change the hostname of this server:

1 Enter the new fully-qualified hostname in the **Hostname** field. The hostname cannot be changed to an IP address.

> ⓘ **IMPORTANT:** Changing the hostname causes a number of changes to be made to the Email Security settings and configuration files and may rename some of the directories in the installation and data directories.

2 Click the **Apply Changes** button

> ⓘ **NOTE:** The system performs a reboot following the hostname change.

HTTPS Settings

On the HTTPS Settings section, you can enable HTTP and HTTPS access on specific ports. The following are the settings you can configure. Click the **Apply Changes** button when done.

Enable HTTP access on port	Check the box to enable this setting. Enter the port number in the field provided. The default port for HTTP is Port 80.
Enable HTTPS (SSL) access on port	Check the box to enable this setting. Enter the port number in the field provided. The default port for HTTPS is Port 443.
Redirect access from HTTP to HTTPS	Select the check box to enable redirecting access from HTTP to HTTPS.

Date & Time Settings

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

Appliance Date and Time

On appliance-based solutions, set the date and time as follows:

1 Select the time zone from the drop-down list for **Available time zones**.

2 Set the time and date using the drop down lists provided for **Year**, **Month**, **Day**, **Hour** and **Minute**.

ⓘ **NOTE:** Hours are set using a 24-hour format.

NOTE: If the server is running Microsoft Windows, use the Windows Control Panel to configure data and time settings.

3 Select **Apply Changes** to save any changes.

Appliance NTP Settings

On appliance-based solutions, enable NTP settings as follows:

1 Enable **Network Time Protocol** by checking the box. It synchronizes server time using UDP on port 123.

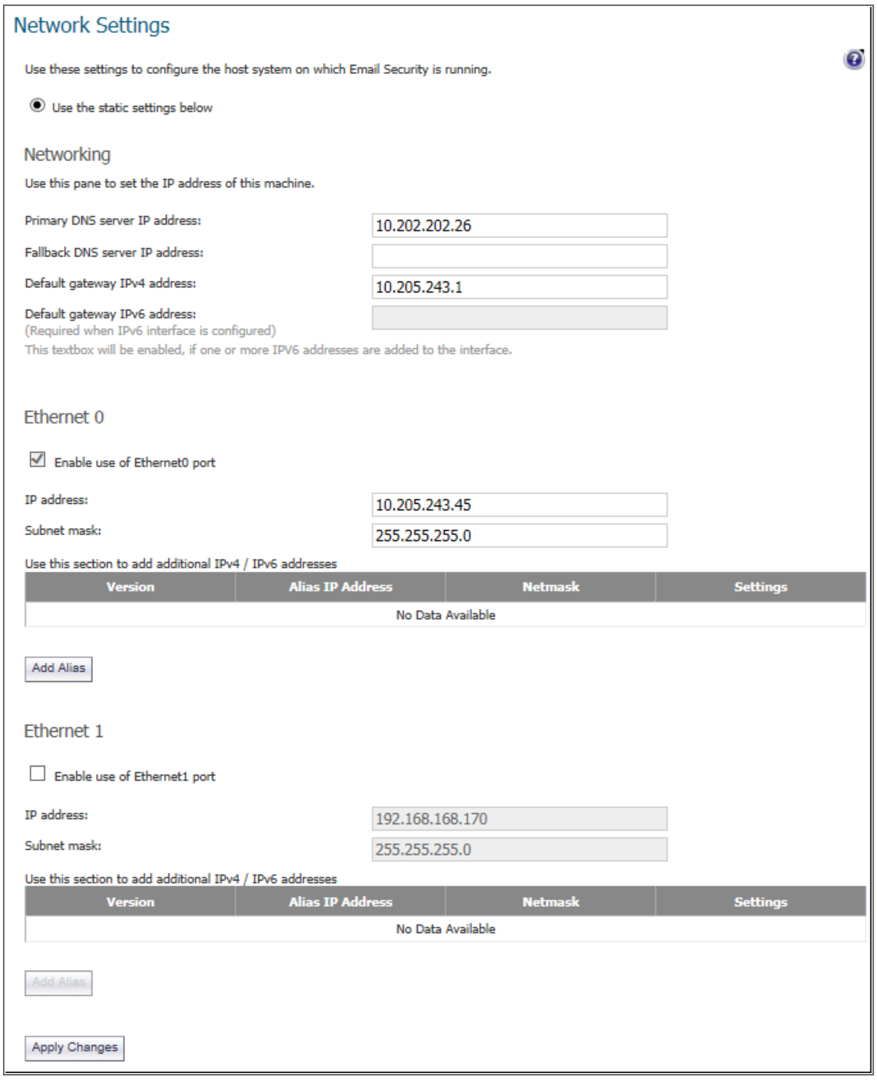
2 Provide the list of NTP servers to use for synchronizing the time. Up to 8 entries are allowed. Separate each by a carriage return.

3 Select **Apply Changes** to save any changes.

Network Settings

On the **Networking**, you can configure the host server to use DHCP or a static IP address. If you chose DHCP (Dynamic Host Configuration Protocol), all the necessary settings are automatically found from the network DHCP server.

If DHCP (Dynamic Host Configuration Protocol) is chosen, all the necessary settings are retrieved automatically from the network DHCP server. If static IP settings are chosen, the IP address, DNS servers, default gateway, and subnet mask must be configured.



Network Settings

Use these settings to configure the host system on which Email Security is running.

● Use the static settings below

Networking

Use this pane to set the IP address of this machine.

Primary DNS server IP address:	10.202.202.26
Fallback DNS server IP address:	
Default gateway IPv4 address:	10.205.243.1
Default gateway IPv6 address: (Required when IPv6 interface is configured)	

This textbox will be enabled, if one or more IPV6 addresses are added to the interface.

Ethernet 0

☑ Enable use of Ethernet0 port

IP address:	10.205.243.45
Subnet mask:	255.255.255.0

Use this section to add additional IPv4 / IPv6 addresses

Version	Alias IP Address	Netmask	Settings
No Data Available			

Add Alias

Ethernet 1

☐ Enable use of Ethernet1 port

IP address:	192.168.168.170
Subnet mask:	255.255.255.0

Use this section to add additional IPv4 / IPv6 addresses

Version	Alias IP Address	Netmask	Settings
No Data Available			

Add Alias

Apply Changes

If you choose static IP settings, set the following:

Primary DNS Server IP address: The IP address of the server which is the primary Domain Name Server for this network.

Fallback DNS Server IP address: The IP address of the server which is the fallback Domain Name Server for this network.

Default gateway IPv4 address: The IP address of the server which is the default gateway for this network.

Default gateway IPv6 address: Required when IPv6 interface is configured.

For Ethernet 0:

1 Check the box if you want to **Enable the use of Ethernet 0 port**.

2 Enter the **IP address** in the text field.

3 Enter the **Subnet mask** in the text field.

4 Click **Add Alias** if you need to add more IPv4 or IPv6 addresses.

For Ethernet 1:

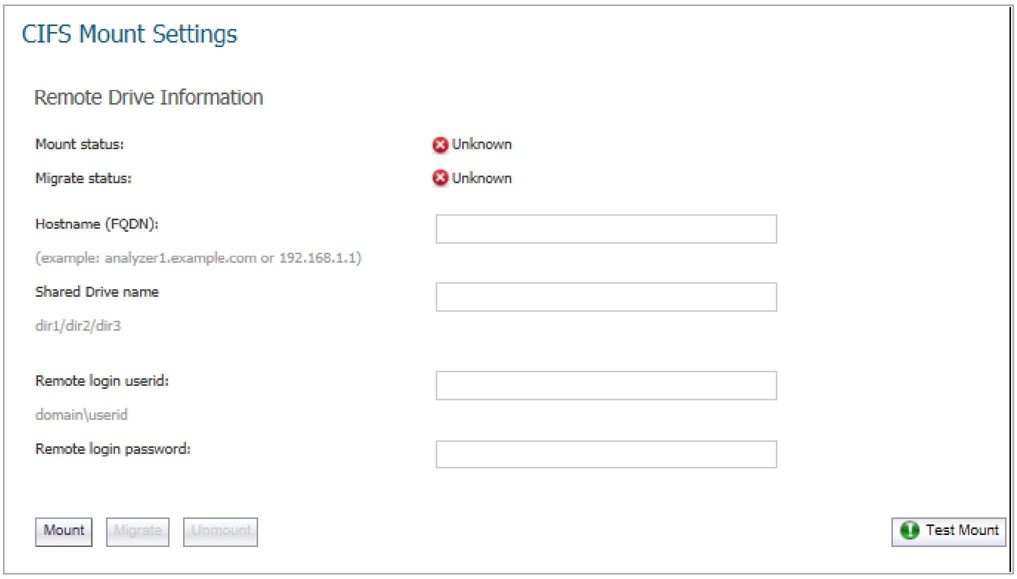
1. Check the box if you want to **Enable the use of Ethernet 1 port**.
2. Enter the **IP address** in the text field.
3. Enter the **Subnet mask** in the text field.
4. Click **Add Alias** if you need to add more IPv4 or IPv6 addresses.

If you make any changes to the Network Settings, be sure to **Apply Changes**.

CIFS Mount Settings

In an appliance-based solution, an external storage drive can be mounted to increase the appliance's data. The available data on the current drive is migrated to the external storage drive, increasing the storage limit for the appliance. For dual control centers, the same external drive can be mounted on both control centers to share the data. The two control centers could be used either to share the load or as a failover.

- **Mount status:** Displays the mount status of the external drive. If no external drive is connected, status is shown as **Unknown**.
- **Migrate status:** Displays the status of the migration from the local data to the external drive.
- **Hostname (FQDN):** Enter the hostname or IP address for the host managing the external drive.
- **Shared Drive Name:** Enter the shared drive name of the remote drive.
- **Remote login userid:** Enter the user ID for logging into the host. Use the format: domain\userid.
- **Remote login password:** Enter the password for logging into the host.
- **Mount:** Mounts the remote drive once the test mount passes.
- **Migrate**: Migrates data from the local drive to the external drive.
- **Unmount**: Unmounts the remote drive.
- **Test Mount:** Tests whether the external drive is mounting or not.



CIFS Mount Settings

Remote Drive Information

Mount status: ☒ Unknown

Migrate status: ☒ Unknown

Hostname (FQDN):

(example: analyzer1.example.com or 192.168.1.1)

Shared Drive name

dir1/dir2/dir3

Remote login userid:

domain\userid

Remote login password:

Advanced

On the **System Setup | Server > Advanced** page, you can configure a variety of settings, such as customize the STMP banner, configure logging levels, set log levels, reset to factory settings, download system/log files, and set other advanced features.

ⓘ **IMPORTANT:** The Advanced page contains tested values that work well in most configurations. Changing these values my adversely affect performance.

Topics:

- General Settings
- Miscellaneous Settings
- Reset Settings

General Settings

A series of general settings can be defined or enabled as described below. When done setting the options, click on **Apply Changes** to save or click on **Reset to Defaults** to return the settings to the system default.

General Settings

Option	Definition
Message Management	
Customize SMTP banner:	Use this setting to specify the SMTP banner. Be sure to use valid characters and syntax for an SMTP header.
Replace SonicWall 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. Enter a new name in this field.
DNS Timeout for SPF:	Enter a value between 1 to 30 seconds. This sets the number of seconds SonicWall Email Security searches for the SPF record of the sender. If Email Security cannot find the SPF record in the number of seconds specified, it times out and does not return the SPF record of the sender. The default value is 2 seconds.
Saved emails will automatically be deleted when older than:	Enter the number of days that you want to preserve the data in the email archives. Lowering this number means less disk space is used, but note that you will not have report data older than the number of days specified.
Permit users to add members of their own domain to their Allowed Lists:	Selecting the **on** button allows users to add people within their domain to their personal Allowed Lists. For example, if you work at example.com and enable this feature, all users at example.com can be added to your Allowed List. As a result, email messages between internal users are not filtered by the Email Security product. You can either add people manually or configure to automatically add each person to whom users send email.

General Settings

Option	Definition
Save a copy of every email that enters your organization:	When the **on** button is selected, folders with the entire contents of every email are created in the logs directory of each server that analyzes email traffic (All-In-One Servers and Remote Analyzers). The emails are saved before being analyzed for threats by Email Security. Because saving inbound emails can be handled independently, separate folders are used for inbound email.
Save a copy of every email that leaves your organization:	When the **on** button is selected, folders with the entire contents of every email are created in the logs directory of each server that analyzes email traffic (All-In-One Servers and Remote Analyzers). The emails are saved before being analyzed for threats by Email Security. Because saving outbound emails can be handled independently, separate folders are used for saved outbound email.
Other Settings	
Log level:	Use this option to change the log level for Email Security. Change the log level to increase or decrease the amount of information stored in your logs. Log level 1 provides the maximum quantity of logging information; level 6 results in the least. The default level is 3.
Reports data will be deleted when older than:	Enter the number of days of data you want to preserve for reporting information. Reducing this number means less disk space is used, but note that report data older than the number of days specified will not be available. The default value is 366 days.
Test Connectivity to reports database:	Click the **Test Connectivity** button to verify that you can access the Reports database. If this test fails, custom reports will not work and the database is not updated. If this test fails during normal operation, contact a system administrator immediately. Refer to **Reports and Monitoring** for more information on accessing and customizing reports.
SNMP Settings (for split configurations)	
SNMP:	When the **on** button is selected, SNMP is enabled, allowing other SNMP-enabled upstream servers to pull information from it.
SNMP Community String:	Enter the SNMP string in the text field. This is the friendly same of your server.
SSH Settings	
SSH	The default setting is **off**. When the **on** button is selected, it allows someone with the proper credentials to temporarily access the secure shell.

Miscellaneous Settings

Use the Miscellaneous Settings section to download system/log files.

To download or email the system/ log files

1. Select the **Type of File** from the drop-down list.
2. Use the **Choose specific files** list to select one or more files to download.

3 Choose the delivery method:

  - Select **Download** to download the files locally.
  - Click the **Email To** button, enter the **Recipient email address** in the dialog box, and click **Send**.

ⓘ **NOTE:** Emailing very large files and directories may be problematic depending on the size and limitations of your email system.

Reset Settings

The Reset Settings section provides tools for cleaning up certain options and resetting others to the default.

Cleanup Per User

The **Cleanup Per User** tool deletes address books and settings filters of non-existent users in your Email Security user list.

- Check the box to **Use last generated report to clean up**. This refers the latest generated report for Per User Cleanup. The report is generated as a `.txt` file.
- Click **Generate Report** to generate an updated list of users.
- Click **Cleanup Per user** to use the Per User Cleanup tool to delete files of non-existent users.

Delete All Users' Allowed and Blocked Lists

All users' allowed and block lists on this server can be permanently deleted. The corporate Allowed and Blocked Lists are also deleted, along with Allowed and Blocked Lists for all groups. If you wish to retain any of this data, you need to back it up from the **Backup/Restore** page and download it to your local hard drive before deleting. Click the **Delete All** button to perform this action.

ⓘ **IMPORTANT:** With this action all Allowed and Blocked Lists are permanently deleted and can't be recovered.

Reinitialize Appliance to Factory Settings

You can reinitialize the settings for this Email Security product to the factory default values. All log, settings, data, license keys, etc. on this server are permanently deleted. If you wish to retain any of this data, you need to back it up from the **Backup/Restore** page and download it to your local hard drive before deleting. Click the **Reinitialize Appliance** button to perform this action.

After clicking the **Reinitialize Appliance** button, you are logged out and redirected to the login page. It takes several minutes for the reinitialization process to finish. When reinitialization is complete, the server automatically reboots itself. When the reboot is finished, you need to reconfigure the appliance from scratch.

Reset Licenses

Reset all license key information associated with this SonicWall Email Security server by clicking the **Reset Licences** button. License keys can be restored by visiting https://www.mysonicwall.com/.

After clicking the Reset Licenses button, the license keys are deleted. You no longer have access to a majority of the user interface features, and many left-hand navigation links direct you to the License Management page.

10

System Setup | Customization and Certificates

This section provides information on **System Setup | Customization** and **System Setup | Certificates** options.

Topics:

- Customization
- Certificates

Customization

Topics:

- User View Setup
- Branding

User View Setup

On the **System Setup | Customization > User View Setup** page, configure how the end users access the system and what features they can manage.

To configure User View Setup:

1 Under the **User View Setup** section, select following options:

   a Check the **Login enabled** box to allow users to log into Email Security and have access to their per-user Junk Box. If you disable this, mail is still analyzed and quarantined, but users do not have access to their Junk Box.

   b Select the **Anti-Spam** box to include the user-configurable options available for blocking spam emails. Users can customize the categories People, Companies, and Lists into their personal Allowed and Blocked lists. You can choose to grant **Full user control over anti-spam aggressiveness settings** by checking the box, or force them to accept the corporate aggressiveness defaults by leaving the check box empty.

   c Check the **Reports** box to provide junk email blocking information about your organization. Even if this option is checked, users may view only a small subset of the reports available to administrators.

   d Check the **Policy** box if you want end users to define their own policy filters. Note that these would be a subset of the policy filters listed in Policy & Compliance > Filters.

   e Check the **Settings** box to provide options for management of the user's Junk Box f Check the **Spam Management** box to allow individual spam management.

g Check the **Allow audit view to Helpdesk users** box to allow those with the Helpdesk role to view the information in the Auditing section.

ⓘ **NOTE:** Checked items appear in the navigation tool bar for users.

2 Under the **User download settings** section:

a With the **Allow users to download SonicWall Junk Button for Outlook** check box selected, users can download the Email Security Junk Button for Outlook. The Junk Button is a lightweight plugin for Microsoft Outlook that allows users to mark emails they receive as junk, but it does not filter email.

b With the **Allow users to download SonicWall Anti-Spam Desktop for Outlook and Outlook Express** check box selected, users will be able to download the Anti-Spam Desktop. Anti-Spam Desktop is a plugin for Microsoft Outlook and Outlook Express that filters spam and allows users to mark emails they receive as junk or good email.

c With the **Allow users to Download SonicWall Secure Mail Outlook plugin** check box selected, users will be able to download the Secure Mail plugin for Microsoft Outlook. The Secure Mail button allows users to send mail securely through the Encryption Service.

3 Define the settings for **Quarantined Junk Mail Preview Settings**:

a Select the **Users can preview their own quarantined junk mail** check box to enable users to view their individual mail that is junked.

b Choose which other types of users can preview quarantined junk mail for the entire organization. These roles are configured within SonicWall Email Security.

- Administrators
- Help Desk and Group Administrators

4 Set the **Reports view** setting. Users are not usually shown reports which include information about users, such as email addresses. Select the **Show reports that display information about individual employees** check box to give user access to those reports.

5 Define the **Miscellaneous** Settings:

a Enter an **Optional login help URL for your organization**. 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, Email Security provides a default login help screen. If a URL is entered, that page is launched when the user clicks the Login Help link. Click the **Test Connectivity** button to verify this URL is valid.

b Select the **Show Forgot Your Password Link** check box to enable this feature for users.

c To send notification to the Administrator when the ‘Forgot Your Password’ link is clicked, select the **Alert administrator when Forgot Your Password request is raised** check box.

Branding

Branding provides the ability to customize aspects of the user interface. Administrators can upload replacement assets for the key branding elements, including company name, logo, and other branding assets. Navigate to **System Setup | Customization > Branding** on the **MANAGE** view to configure Branding feature settings. Select either the **Quick Settings** tab or the **Packages** tab. The **Quick Settings** tab allows administrators to specify global settings for the most commonly modified asset files on the GUI. The **Packages** tab allows administrators to manage, upload, and apply branding packages to their GUI.

Topics:

- Quick Settings
- Packages

Quick Settings

Use the Quick Settings tab on the **System Setup | Customization > Branding** page to specify global settings for particular user interface elements.

ⓘ **NOTE:** Any settings specified in this section overrides those specified by deployed packages.

Text Preferences

The **Contact Us URL** is the email address or URL that appears as the “Contact Us” link at the footer of each page. This field supports “http://”, “https://”, and “mailto:” formats. To change the **Contact Us URL**, type the email address or URL in the field provided.

Click the **Test Connectivity** button to verify the email address or URL you specified is valid.

Image Preferences

The **Image Preferences** files can all be modified by clicking the **Browse...** button or clicking the **Download** icon. The **Browse...** option allows you to select a file from your local system. The **Download** icon downloads the default SonicWall image file. Note that an error message displays if you upload an incorrect file type.

The following Image Preferences can be modified:

- Web Icon file—This field replaces the 4-bit SonicWall logo that appears in the address bar of every web page across all browser platforms.
- Logon logotype file—This field replaces the logon, logout, and mini-logon generic bitmap that displays the SonicWall challenge screen layout and design.
- Logon backdrop art file—This field replaces the logotype bitmap that appears upon every challenge screen.
- Page logotype file—This field replaces the short version of the SonicWall logotype that appears at the top of each web page’s banner art.
- Page header art file—This field replaces the SonicWall banner art bitmap at the top of each web page.
- Pop-up logotype file—This field replaces the smaller version of the SonicWall logotype that appears at the top of each pop-up dialog’s page banner art.
- Pop-up header art file—This field replaces the smaller version of the SonicWall banner art that appears at the top of each pop-up dialog page.

Junk Summary Preferences

The **Junk Summary Preferences** can all be modified by clicking the **Browse...** button or clicking the **Download** icon. The **Browse...** option allows you to select a file from your local system. The **Download** icon downloads the default SonicWall image file. Note that an error message displays if you have uploaded an incorrect file type.

The following Junk Summary Preferences can be modified:

- **Junk Summary logotype file**—This field replaces the black-on-white logotype that always appears at the top of each Junk Summary email.
- **Junk Summary header art file**—This field replaces the Junk Summary banner art bitmap at the top of each page.

Click the **Save** button when you have finished modifying settings on the **Quick Settings** tab.

Packages

The Packages tab allows administrators to manage, upload, and apply branding packages to their user interface. The Manage Packages table displays the available packages the administrator can apply, including the SonicWall brand package.

> **NOTE:** The SonicWall branding package can never be deleted, but administrators can edit or delete all other brand packages that have been uploaded.

To upload a new package:

1. Navigate to **System Setup | Customization > Branding** on the **MANAGE** view.
2. Click the **Packages** button.
3. Click the **Upload** button under the **Manage Packages** section.

   > **NOTE:** Uploads are restricted to `.zip` files and must contain the exact structure of the directories being modified or replaced.

4. Click on **Browse...** and navigate to and select the **File to upload**.
5. Enter the **Brand Label** name.
6. Enter the **Full name** of the packaging label.
7. Provide the email address or web sites as a contact point listed in the **Contact Us** field.
8. Add any additional notes about the package in the **Notes** field.
9. Click on **Save** to upload the package.

To manage the packages once they are loaded in the table, you can click on the management icons (**Edit**, Download, or **Delete**) listed in the **Configure** column of the table.

Certificates

On the **System Setup | Certificates** page, you can configure settings specific to certificates, including trusted certificate authentication and enabling secured access. Refer to the following sections for more information:

- Generate/Import
- Generate CSR
- Configure

Generate/Import

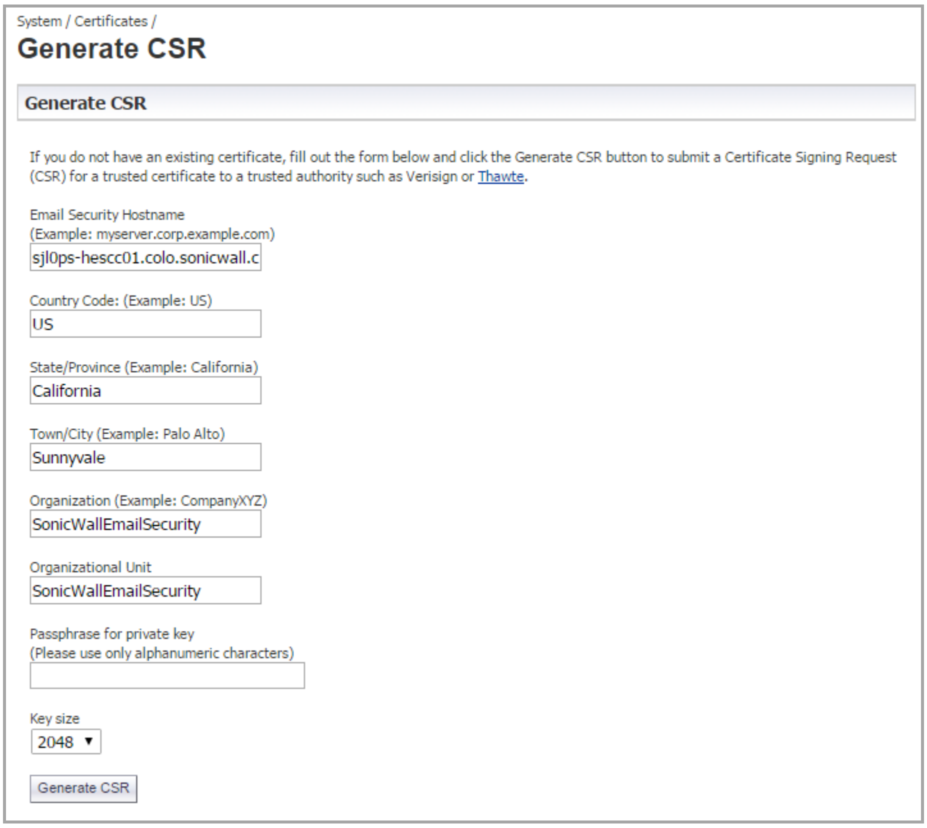
Choose between self signing and trusted certificate authority and enter the appropriate settings.

To generate a certificate:

1. Navigate to **System Setup | Certificates > Generate/Import**.
2. Enter the **Certificate Name** in the field provided.
3. Select one of the following:
   - **Generate generic self-signed SSL certificate**—Select this option to have Email Security generate a generic self-signed SSL certificate. Specify the **Passphrase for private key** in the field provided.
   - **Generate a self-signed SSL certificate**—Select this option to have Email Security generate a self-signed SSL certificate. Specify the **Hostname to be used when generating this certificate** and the **Passphrase for private key** in the fields provided.
   - **Import an existing certificate issued by a trusted authority like RapodSSL, Verisign and other CAs. The product supports PKCS #12 (.p12 or .pfx), PKCS #7 and PEM formats**—Complete the following for this option:
     - **Upload a PKCS #12/PKCS #7/PEM certificate** by clicking **Choose File** and selecting the appropriate file.
     - **Upload Private Key for PKCS #7/PEM certificate** by clicking **Choose File** and selecting the appropriate file.
     - Enter the **Passphrase for private key** in the field provided.
     - Enter the **Password for PKCS #12** file in the field provided.
4. Click the **Generate/Import** button.

Generate CSR

If you do not have an existing certificate, navigate to **System Setup | Certificates> Generate CSR** on the **MANAGE** view. Fill out the form and click the **Generate CSR** button to submit a Certificate Signing Request (CSR) for a trusted certificate to a trusted authority, such as Verisign or Thawte.



System / Certificates /

Generate CSR

Generate CSR

If you do not have an existing certificate, fill out the form below and click the Generate CSR button to submit a Certificate Signing Request (CSR) for a trusted certificate to a trusted authority such as Verisign or Thawte.

Email Security Hostname
(Example: myserver.corp.example.com)
sjl0ps-hescc01.colo.sonicwall.c

Country Code: (Example: US)
US

State/Province (Example: California)
California

Town/City (Example: Palo Alto)
Sunnyvale

Organization (Example: CompanyXYZ)
SonicWallEmailSecurity

Organizational Unit
SonicWallEmailSecurity

Passphrase for private key
(Please use only alphanumeric characters)

Key size
2048

Configure

On the **System Setup | Certificates > Configure** screen, a table is generated that shows the server name, certificate type, and if it is SMTP or HTTPS.

- Click the **Help** icon of a specific certificate to see the certificate details.
- Click the **Download** icon to download the certificate to your local hard drive.
- Click the **Delete** icon to delete the certificate from the Email Security system.
- Click the **Apply** button to apply the certificate to the server.

11

Users, Groups & Organizations

The Users, Groups & Organizations section gives you the ability to set parameters on individuals or on subsets of the whole company. Topics include:

- Users
- Groups
- Organizations
- Users and Groups in Multiple LDAP

NOTE: To manage users and groups, you have to configured your SonicWall Email Security setup to synchronize with your organization’s LDAP server. Refer to LDAP Configuration for more information on configuring LDAP settings and queries.

Users

System Setup | Users, Groups & Organizations > Users displays the list of users who can log in. The list is determined by the query entered on the **System Setup | Server > LDAP Configuration** page. While Email Security filters the email messages received by users not on the list, such users cannot log in to configure their individual settings.

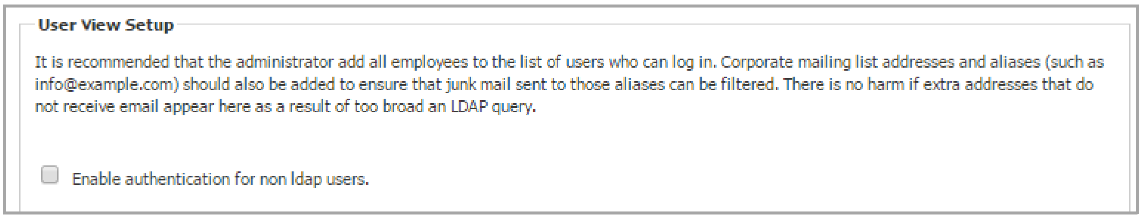
NOTE: The user data may come from multiple sources, so before performing a task on any user, select an option from the **Using Source** drop-down list, then click **Go**.

Select the **Refresh Users & Group** button to refresh the entries in the data table.

User View Setup

The administrator should add all employees to the list of users who can log in. Corporate mailing lists and aliases (such as info@example.com) should also be added to ensure junk mail sent to those aliases can be filtered. No harm is caused if extra addresses that do not receive email appear here as a result of too broad an LDAP query.

To **Enable authentication for non-LDAP users**, select the corresponding check box in the User View Setup section.



User View Setup

It is recommended that the administrator add all employees to the list of users who can log in. Corporate mailing list addresses and aliases (such as info@example.com) should also be added to ensure that junk mail sent to those aliases can be filtered. There is no harm if extra addresses that do not receive email appear here as a result of too broad an LDAP query.

□ Enable authentication for non ldap users.

Searching for Users

If too many users show in a window, you can conduct a search using the **Find all users in column** search tool.

To use this search feature:

1. Navigate to the **System Setup | Users, Groups & Organizations > Users** page.
2. In the drop-down list, choose the search type: **User Name** or **Primary Email**.
3. In the next drop down list, select from the search parameters: **equal to (fast)**, **starting with (medium)**, or **containing (slow)**.
4. In the text field, type the word or phrase you are searching for.
5. Check the box if you want the search to **Show LDAP entries** or **Show non-LDAP entries** next to each option.
6. Click **Go**.

Sorting the User List

To sort the list of users, click the **User Name** or **Primary Email** heading. The arrowhead in the column indicates whether the data is sorted in ascending or descending order. Click the arrowhead to reverse the order.

Signing In as a User

You can sign in as any user in the list, see their Junk Box, and change the settings for that user. You can also manage an user's delegates for them. Select the check box next to the User Name, then click the **Sign In as User** button.

The user's Junk Box is displayed and you can make changes as needed. Refer to the *SonicWall Email Security 9.1 User Guide* for more information, if needed.

Editing User Rights

Administrators can assign different privileges to different users by assigning them pre-defined roles. The pre-defined roles are described below.

Pre-defined Roles for Users and Groups

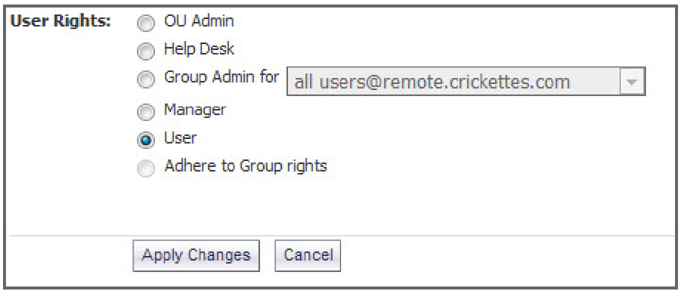
Role	Description
Admin	The Admin role has full administrative rights to a specific list of domains the Global Administrator specifies. Typically, the Global Administrator of an enterprise-sized organization may wish to delegate the management of a smaller group of domains, or Organizational Units, between several users requiring administrative rights for successful management of these OUs. The OU Admin can log in as any other user within the group of domains assigned to change a user's individual settings, view and manage Junk Boxes, and configure other areas of the SonicWall system.
Help Desk	A user assigned as Help Desk has access to the corporate Junk Box and can unjunk items. This role also allows the user to log in as any user to change that user's individual settings and view Junk Boxes. The Help Desk role does not allow the user to change global settings or other server configurations.

Pre-defined Roles for Users and Groups

Role	Description
Group Admin for	A group administrator role is similar to the Help Desk role except that this role's privileges are limited to users for the group that they are specified to administer. The Group Admin role is always associated with one or more groups added to the Spam Blocking Options for Groups section.
Manager	A user assigned as Manager has access to corporate Reports and Monitoring screens. The user cannot change any configuration settings, nor are they able to sign in as any other user.
User	A user role is only allowed to log in to the SonicWall Email Security system, has access to his own individual user settings, and can only customize his own settings.
Support	A user assigned as Support is given the same privileges as an administrator and is typically assigned to support staff that need temporary access to the system. The support role can then be revoked when that user no longer needs the elevated access.
Adhere to Group rights	The user rights are made to adhere to the right of the group.

To assign a role to a user:

1 Select the user and click on **Edit User Rights** button.



User Rights:
○ OU Admin
○ Help Desk
○ Group Admin for all users@remote.crickettes.com
○ Manager
● User
○ Adhere to Group rights

2 Choose which role to assign to a user. (Refer to Pre-defined Roles for Users and Groups.)

3 Click on **Apply Changes**.

Resetting User Message Management 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.

Adding a User

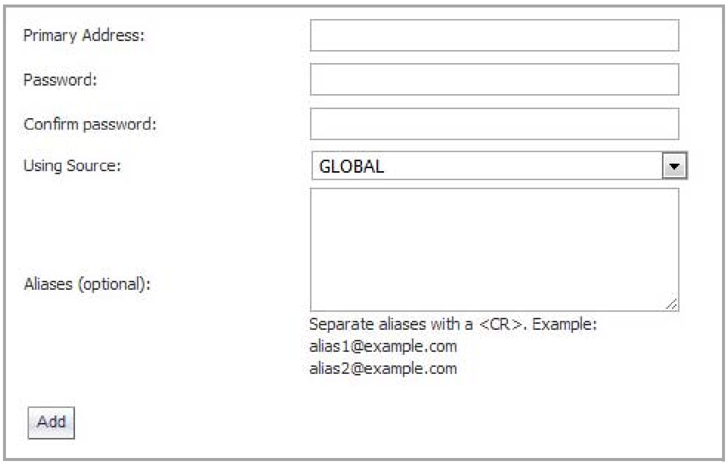
The administrator can add individual non-LDAP users.

1 Fill out the **Primary Address** field.

2 If users have aliases associated with them, added them the **Aliases** field. Separate each alias with a carriage return.

3 Click **Add**. This is not dependent on LDAP status.

NOTE: Users added in this way remain non-LDAP users. Their User Rights cannot be changed. Their source is listed as Admin. Users can edit their Junk Box setting only if the administrator sets the Junk Box setting: **Enable "Single Click" viewing of messages** to **Full access** on the **System Setup | Junk Box > Junk Box Summary Notifications** page.



Primary Address:

Password:

Confirm password:

Using Source: GLOBAL

Aliases (optional):

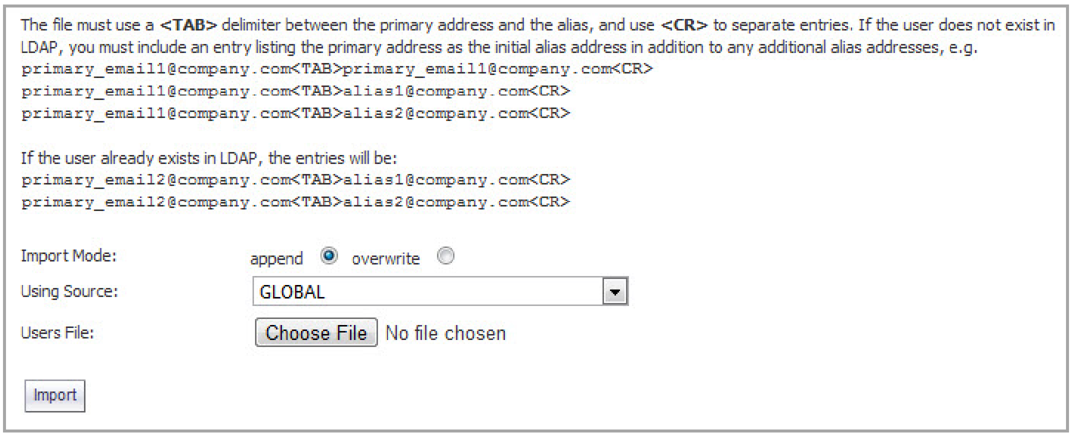
Separate aliases with a <CR>. Example:
alias1@example.com
alias2@example.com

Removing Users

The administrator can remove individual non-LDAP users. First select a non-LDAP user by using the check box in front of the name, then click the **Remove** button to delete the name from the list.

Importing Users

The administrator can add multiple non-LDAP users by importing a list of names. The list is made up of the primary addresses followed by the corresponding aliases of the users. The imported file can be appended to the existing names, or overwrite them. The format of the file is tab-delimited. One may use an Excel spreadsheet to generate a user list and save it as a tab-delimited file.



The file must use a **<TAB>** delimiter between the primary address and the alias, and use **<CR>** to separate entries. If the user does not exist in LDAP, you must include an entry listing the primary address as the initial alias address in addition to any additional alias addresses, e.g.

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
primary_email1@company.com<TAB>alias2@company.com<CR>
```

If the user already exists in LDAP, the entries will be:

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

Import Mode: append ● overwrite ○

Using Source: GLOBAL

Users File: Choose File No file chosen

To import the list:

1 Click the **Import** button.

2 Set the **Import Mode** to **append** or **overwrite**.

3 Browse... to locate the file and click **Import**.

Exporting Users

The administrator can download a tab-delimited list by clicking **Export**. The file generated lists multiple non-LDAP users and can edited and imported later.

Locked Users

On the Users page, in the **Locked Users** section, SonicWall Email Security displays a list of users that are currently locked out. The administrator can reset the lockout for any user.

To unlock the user:

1 Check the box by the locked out user or select multiple users.

2 Select the **Unlock User** button.

Groups

Navigate to the **System Setup | Users, Groups & Organizations > Groups** page to manage Group settings. Settings on this page are optional. The members of each group listed on this page are determined from LDAP. Groups are refreshed automatically from LDAP once per hour

This section describes how SonicWall Email Security lets you query and configure groups of users managed by an LDAP server. Most organizations create LDAP groups on their Exchange server according to the group functions. Different groups may have—or need—different settings specified. Configure LDAP groups on your corporate LDAP server before configuring the rights of users and groups on SonicWall Email Security in the LDAP Configuration screen.

SonicWall Email Security allows you to assign roles and set spam-blocking options for user groups. Though a user can be a member of multiple groups, SonicWall 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.

ⓘ | **NOTE:** Any policy filter created by a group admin is applicable to all users belonging to the group.

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

This section includes the following topics:

- Assigning Roles to Groups Found in LDAP
- Set Junk Blocking Options for Groups Found in LDAP

Assigning Roles to Groups Found in LDAP

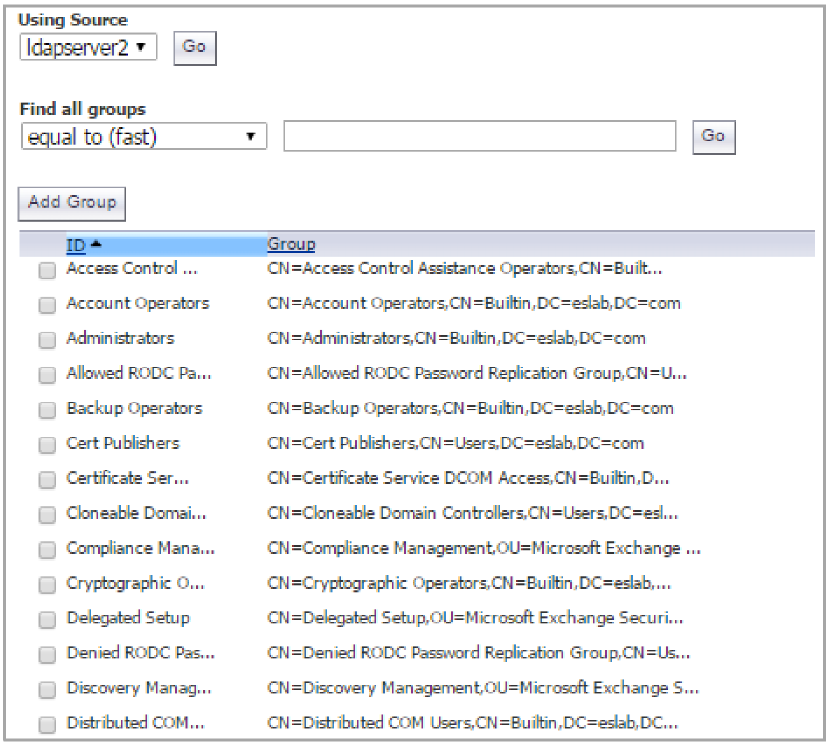
Topics:

- Finding and Adding a Group
- Removing a Group
- Listing Group Members
- Setting an LDAP Group Role

Finding and Adding a Group

To find a group to add:

1 Click the **Add Group** button under the heading **Assign Roles to Groups Found in LDAP**.



Using Source

ldapserver2 ▾ Go

Find all groups

equal to (fast) ▾ Go

Add Group

	ID ▲	Group
□	Access Control ...	CN=Access Control Assistance Operators,CN=Built...
□	Account Operators	CN=Account Operators,CN=Builtin,DC=eslab,DC=com
□	Administrators	CN=Administrators,CN=Builtin,DC=eslab,DC=com
□	Allowed RODC Pa...	CN=Allowed RODC Password Replication Group,CN=U...
□	Backup Operators	CN=Backup Operators,CN=Builtin,DC=eslab,DC=com
□	Cert Publishers	CN=Cert Publishers,CN=Users,DC=eslab,DC=com
□	Certificate Ser...	CN=Certificate Service DCOM Access,CN=Builtin,D...
□	Cloneable Domai...	CN=Cloneable Domain Controllers,CN=Users,DC=esl...
□	Compliance Mana...	CN=Compliance Management,OU=Microsoft Exchange ...
□	Cryptographic O...	CN=Cryptographic Operators,CN=Builtin,DC=eslab,...
□	Delegated Setup	CN=Delegated Setup,OU=Microsoft Exchange Securi...
□	Denied RODC Pas...	CN=Denied RODC Password Replication Group,CN=Us...
□	Discovery Manag...	CN=Discovery Management,OU=Microsoft Exchange S...
□	Distributed COM...	CN=Distributed COM Users,CN=Builtin,DC=eslab,DC...

2 Choose the search mechanism in the **Find all groups** field. Select from **equal to (fast)**, **starting with (medium)**, or **containing (slow)**.

> **NOTE:** The type of search you choose could affect the length of the search. The relative speed is indicated in the parentheses.

3 Type the search string in the text box.

4 Click **Go** to begin the search.

> **NOTE:** Optionally, you can scroll through the list of groups to locate the group you want to add.

5 Check the box next to the group you want to include.

6 Click **Add Group**. A message displays stating that the group was added successfully.

Removing a Group

To remove a group:

1 Click the check box adjacent to the group(s) to remove.

2 Click the **Remove Group** button. A success message displays.

Listing Group Members

To list group members:

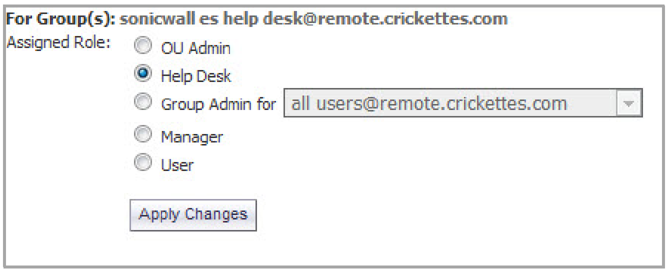
1. Click the check box adjacent to the group to list.
2. Click the **List Group Members** button. Users belonging to that group are listed in a pop-up window.

Setting an LDAP Group Role

All members of a group are also given the role assigned to the group.

To set the role of a group:

1. Click the check box adjacent to the group to edit.
2. Click **Edit Role**.



For Group(s): sonicwall es help desk@remote.crickettes.com

Assigned Role:
○ OU Admin
● Help Desk
○ Group Admin for: all users@remote.crickettes.com
○ Manager
○ User

3. Select the appropriate role that you want to assign to the group. Definitions for these roles can be found in Pre-defined Roles for Users and Groups.
4. Click **Apply Changes**. A message appears stating that the group was changed successfully.

> **NOTE:** Email Security 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, but are updated within an hour.

Set Junk Blocking Options for Groups Found in LDAP

In this section of the Groups page, you can set up and manage the groups that need to be set up for junk blocking. Each group can have different settings.

Topics:

- Find and Add a Group
- Remove a Group
- List Members
- Edit Junk Blocking Options

Find and Add a Group

To find a group to add:

1. Click the **Add Group** button under the heading **Set Junk Blocking Options for Groups Found in LDAP**.

2 Choose the search mechanism in the **Find all groups** field. Select from **equal to (fast)**, **starting with (medium)**, or **containing (slow)**.

> **NOTE:** The type of search you choose could affect the length of the search. The relative speed is indicated in the parentheses.

3 Type the search string in the text box.

4 Click **Go** to begin the search.

5 Check the box next to the group you want to include.

6 Select **Add Group**. A message displays stating that the group was added successfully.

Remove a Group

To remove a group:

1 Select the check box adjacent to the group or groups to remove.

2 Click the **Remove Group** button. A success message displays.

List Members

To list group members:

1 Select the check box adjacent to the group to list.

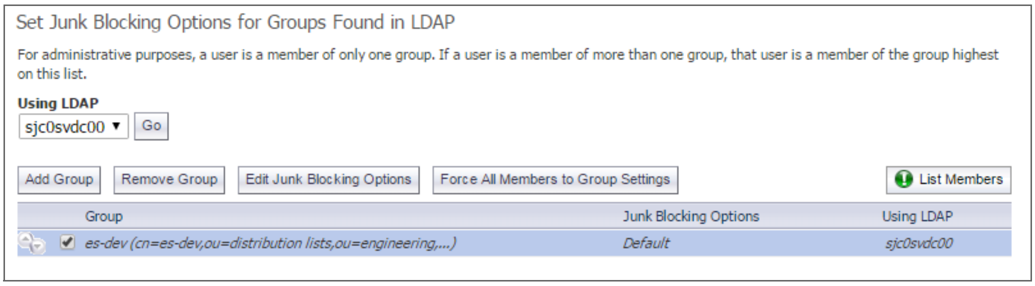
2 Click the **List Group Members** button. Users belonging to that group are listed in a pop-up window.

Edit Junk Blocking Options

Once a group has been added you can set up the junk blocking options for the group. You can choose to adhere to junk blocking parameters that have been defined for the corporate level, or you can customize the options for each group. The following parameters can be set:

- User View Setup
- Anti-Spam Aggressiveness
- Languages
- Spam Management
- Phishing Management
- Virus Management
- Anti-Spoofing

To edit junk blocking options:



Set Junk Blocking Options for Groups Found in LDAP

For administrative purposes, a user is a member of only one group. If a user is a member of more than one group, that user is a member of the group highest on this list.

Using LDAP

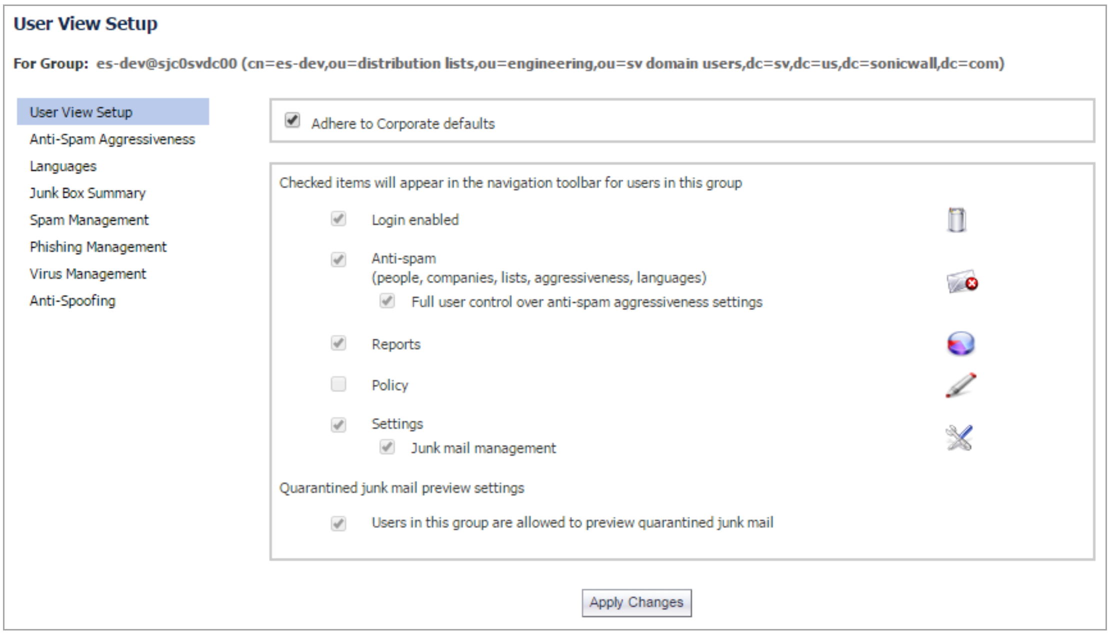
sjc0svdc00 ▼ Go

Add Group
Remove Group
Edit Junk Blocking Options
Force All Members to Group Settings
List Members

	Group	Junk Blocking Options	Using LDAP
☑	*es-dev (cn=es-dev,ou=distribution lists,ou=engineering,...)*	*Default*	*sjc0svdc00*

1 Check the box by the name of the group for which you want update junk blocking options.

2 Select **Edit Junk Blocking Options**. The following page displays with User View Setup as the default view. Each of the Junk Blocking Options are described in more detail the following sections.



User View Setup

For Group: es-dev@sjc0svdc00 (cn=es-dev,ou=distribution lists,ou=engineering,ou=sv domain users,dc=sv,dc=us,dc=sonicwall,dc=com)

☑ Adhere to Corporate defaults

Checked items will appear in the navigation toolbar for users in this group

☑ Login enabled

☑ Anti-spam
(people, companies, lists, aggressiveness, languages)

☑ Full user control over anti-spam aggressiveness settings

☑ Reports

□ Policy

☑ Settings

☑ Junk mail management

Quarantined junk mail preview settings

☑ Users in this group are allowed to preview quarantined junk mail

User View Setup

The User View Setup option for Junk Blocking controls what options are available to the users in this group when they log in to the server using their user name and password. Enable any of the options by checking the box associated with the option. The options are defined in User View Setup Options. Be sure to select **Apply Changes** when done.

User View Setup Options

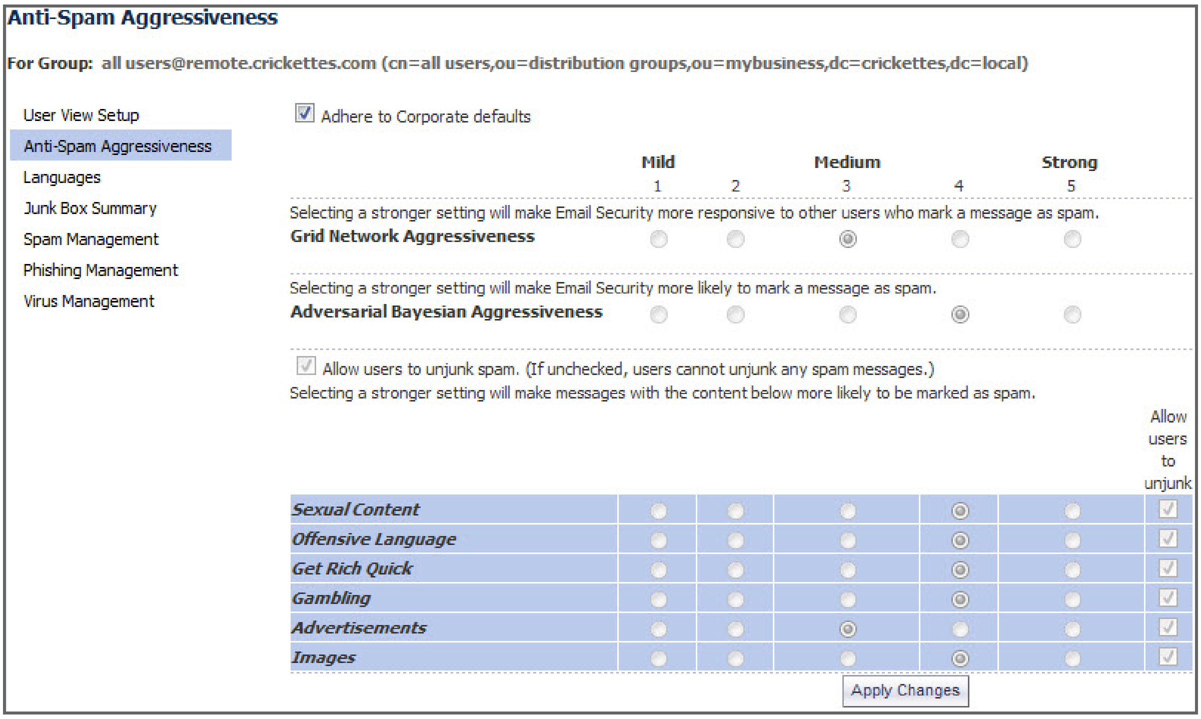
Option	Definition
Adhere to Corporate defaults	Sets the group options the same as the options defined at the corporate level. If this option is selected ,the other options are grayed out and not available.
Login enabled	Enables users in this group to log into their Junk Box.
Anti-spam	Allows or blocks specified people companies, lists, aggressiveness and languages. You can enable more user control by checking the box for **Full user control over anti-spam aggressiveness settings**.
Reports	Allows users in this group to view their spam reports.

User View Setup Options

Option	Definition
Settings	Enables users in this group to view their settings. You can allow user access to their junk management settings by also checking the box for **Junk mail management**.
Quarantined junk mail preview settings	Allows users to preview quarantined junk mail if the box is checked for **Users in the group are allowed to preview quarantined junk mail**.

Anti-Spam Aggressiveness

On the Junk Blocking Options page, select **Anti-Spam Aggressiveness** on the left of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the anti-spam aggressiveness as described below.



Anti-Spam Aggressiveness

For Group: all users@remote.crickettes.com (cn=all users,ou=distribution groups,ou=mybusiness,dc=crickettes,dc=local)

☑ Adhere to Corporate defaults

	Mild 1	2	Medium 3	4	Strong 5	
Selecting a stronger setting will make Email Security more responsive to other users who mark a message as spam. **Grid Network Aggressiveness**	○	○	●	○	○	
Selecting a stronger setting will make Email Security more likely to mark a message as spam. **Adversarial Bayesian Aggressiveness**	○	○	○	●	○	

☑ Allow users to unjunk spam. (If unchecked, users cannot unjunk any spam messages.)
Selecting a stronger setting will make messages with the content below more likely to be marked as spam.

	1	2	3	4	5	Allow users to unjunk
Sexual Content	○	○	○	●	○	☑
Offensive Language	○	○	○	●	○	☑
Get Rich Quick	○	○	○	●	○	☑
Gambling	○	○	○	●	○	☑
Advertisements	○	○	●	○	○	☑
Images	○	○	○	●	○	☑

To configure Anti-Spam Aggressiveness settings for a group:

1 Choose the appropriate **GRID Network Aggressiveness** level for this group. Note that selecting a stronger setting will make Email Security more responsive to other users who mark a message as spam.

2 Choose the appropriate **Adversarial Bayesian Aggressiveness** level for this group. Note that selecting a stronger setting makes Email Security more likely to mark a message as spam.

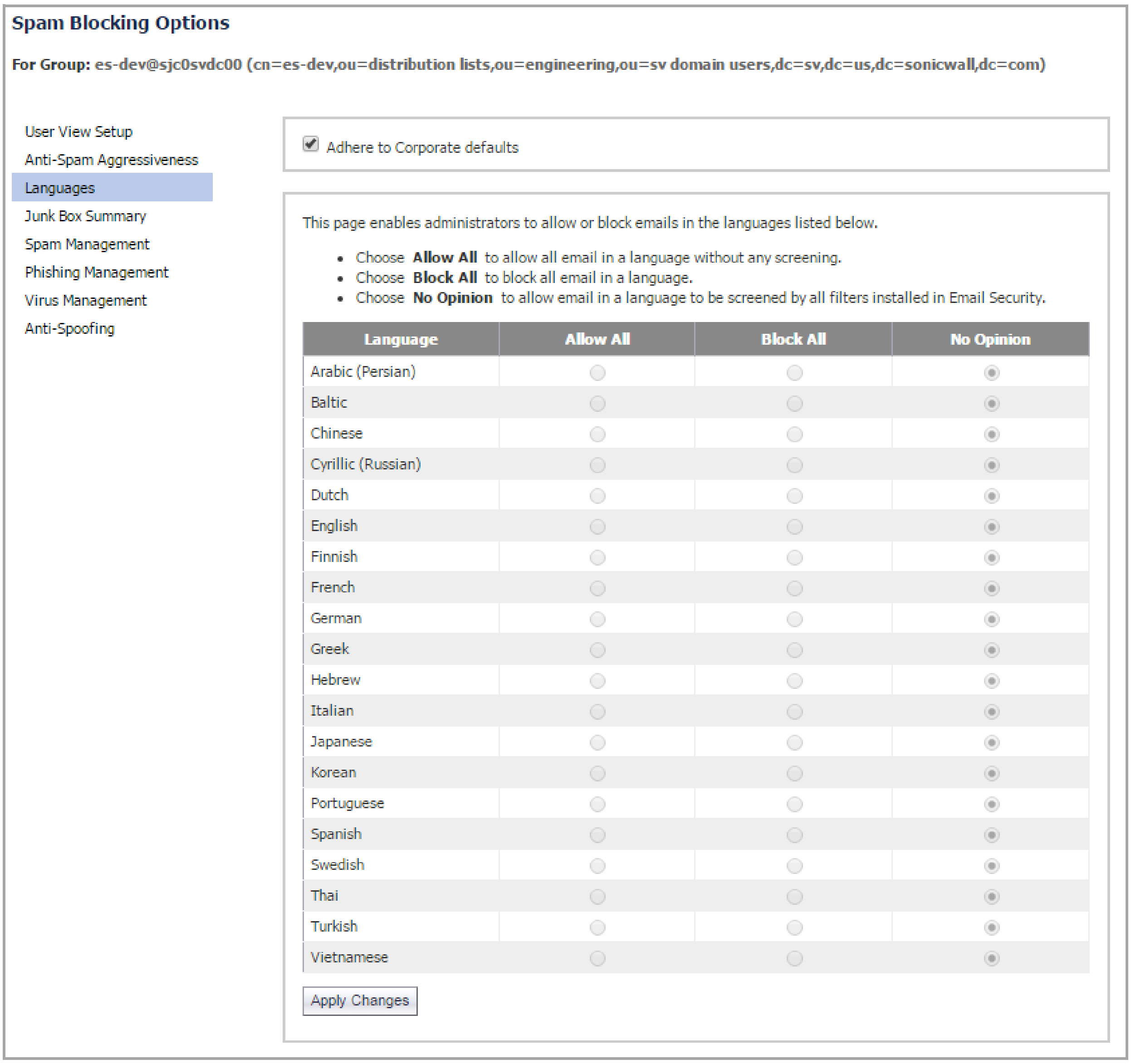
3 Select the check box to **Allow users to unjunk spam**. If the check box is unchecked, users are not able to unjunk spam messages.

4 For each category of spam, determine level and whether members of the group are allowed to unjunk their Junk Boxes.

5 Click **Apply Changes**.

Languages

On the Junk Blocking Options page, select **Languages** on the left of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the blocking options as described below.



Spam Blocking Options

For Group: es-dev@sjc0svdc00 (cn=es-dev,ou=distribution lists,ou=engineering,ou=sv domain users,dc=sv,dc=us,dc=sonicwall,dc=com)

☑ Adhere to Corporate defaults

This page enables administrators to allow or block emails in the languages listed below.

- Choose **Allow All** to allow all email in a language without any screening.
- Choose **Block All** to block all email in a language.
- Choose **No Opinion** to allow email in a language to be screened by all filters installed in Email Security.

Language	Allow All	Block All	No Opinion
Arabic (Persian)	○	○	●
Baltic	○	○	●
Chinese	○	○	●
Cyrillic (Russian)	○	○	●
Dutch	○	○	●
English	○	○	●
Finnish	○	○	●
French	○	○	●
German	○	○	●
Greek	○	○	●
Hebrew	○	○	●
Italian	○	○	●
Japanese	○	○	●
Korean	○	○	●
Portuguese	○	○	●
Spanish	○	○	●
Swedish	○	○	●
Thai	○	○	●
Turkish	○	○	●
Vietnamese	○	○	●

To determine the foreign language emails that groups can receive:

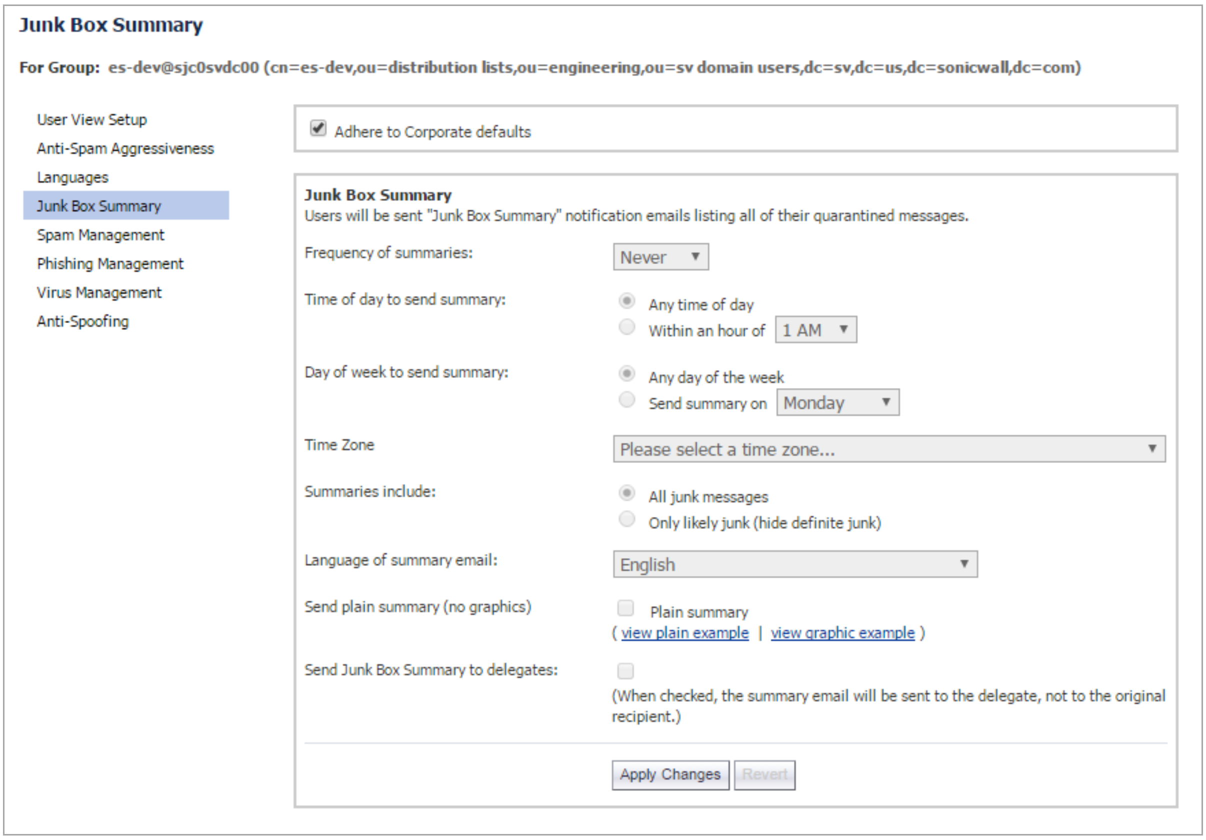
1 Select one of the following options for each language:

- **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 SonicWall Email Security.

2 Click **Apply Changes** to save setting made.

Junk Box Summary

On the Junk Blocking Options page, select **Junk Box Summary** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for the Junk Box Summary as described below.



Junk Box Summary

For Group: es-dev@sjc0svdc00 (cn=es-dev,ou=distribution lists,ou=engineering,ou=sv domain users,dc=sv,dc=us,dc=sonicwall,dc=com)

☑ Adhere to Corporate defaults

Junk Box Summary

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

Frequency of summaries: Never ▼

Time of day to send summary: ● Any time of day ○ Within an hour of 1 AM ▼

Day of week to send summary: ● Any day of the week ○ Send summary on Monday ▼

Time Zone: Please select a time zone... ▼

Summaries include: ● All junk messages ○ Only likely junk (hide definite junk)

Language of summary email: English ▼

Send plain summary (no graphics): □ Plain summary (view plain example | view graphic example)

Send Junk Box Summary to delegates: □ (When checked, the summary email will be sent to the delegate, not to the original recipient.)

To configure settings for the Junk Box for groups:

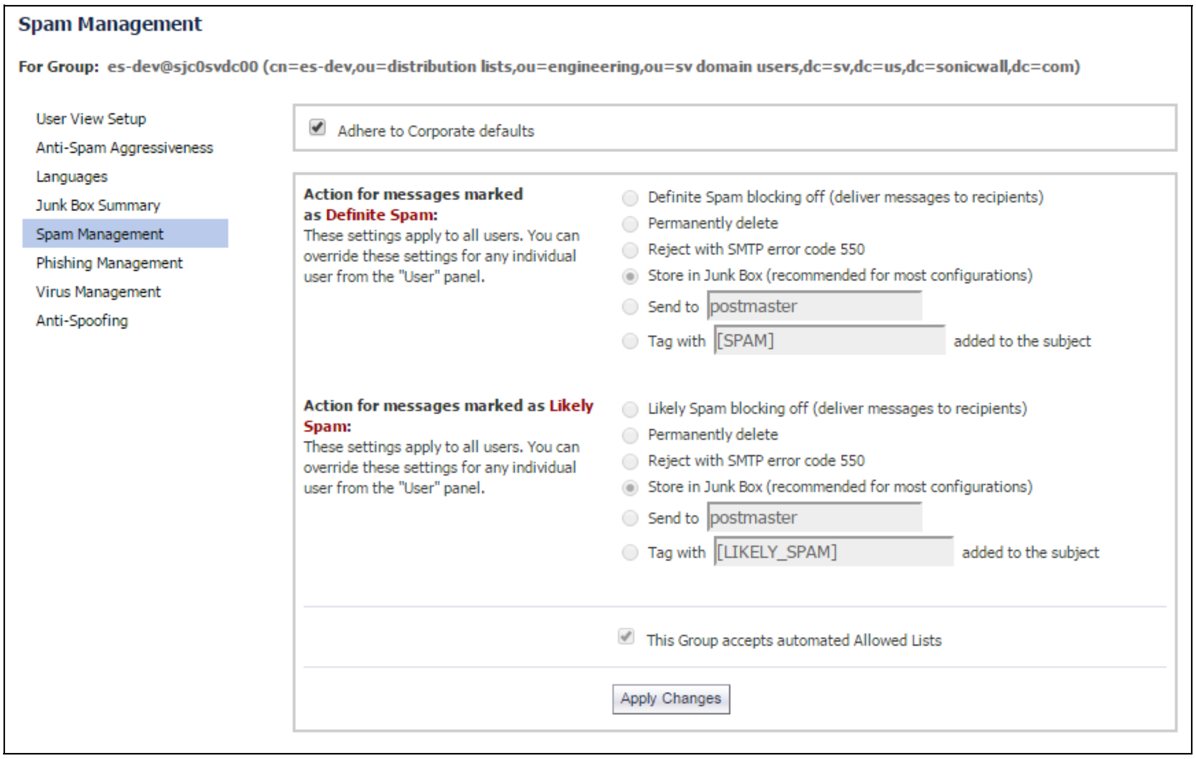
1. Select the **Frequency of Summaries** sent to users. Options include: **Never**, **1 Hour**, **4 Hours**, **1 Day**, **3 Days**, **7 Days** or **14 Days**.
2. Select the **Time of Day** users receive junk summary emails. Choose **Any time of day** or **Within an hour of** <*select hour*>.
3. Select the **Day of the Week** users receive junk summary emails. Choose **Any day of the week** or **Send summary on** <*select day*>.
4. Choose one option for summaries to include: **All junk messages** or **Only likely junk (hide definite junk)**.
5. Select the **Language of Summary Email** from the drop down list.
6. Check the box if you want to receive a **Plain Summary.** The default is to receive a Graphic Summary.
7. Select the check box to if you want to **Send Junk Box Summary to Delegates**.

   NOTE: When this check box is selected, the summary email is sent to the delegate, not to the original recipient.

8. Click **Apply Changes**.

Spam Management

On the Junk Blocking Options page, select **Spam Management** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for mail tagged as Definite Spam and LIkely Spam as described below.



Spam Management

For Group: es-dev@sjc0svdc00 (cn=es-dev,ou=distribution lists,ou=engineering,ou=sv domain users,dc=sv,dc=us,dc=sonicwall,dc=com)

☑ Adhere to Corporate defaults

Action for messages marked as Definite Spam:
These settings apply to all users. You can override these settings for any individual user from the "User" panel.

○ Definite Spam blocking off (deliver messages to recipients)
○ Permanently delete
○ Reject with SMTP error code 550
● Store in Junk Box (recommended for most configurations)
○ Send to postmaster
○ Tag with [SPAM] added to the subject

Action for messages marked as Likely Spam:
These settings apply to all users. You can override these settings for any individual user from the "User" panel.

○ Likely Spam blocking off (deliver messages to recipients)
○ Permanently delete
○ Reject with SMTP error code 550
● Store in Junk Box (recommended for most configurations)
○ Send to postmaster
○ Tag with [LIKELY_SPAM] added to the subject

☑ This Group accepts automated Allowed Lists

To manage Definite Spam or Likely Spam for this group:

1 Chose an action for messages marked as Definite Spam. The options are defined below.

- **Spam blocking off (deliver messages to recipients)**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Spam, messages are permanently deleted.
- **Reject with SMTP error code 550**—Messages are sent back to the sender. 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.
- **Store in Junk Box (recommended for most configurations)**—Messages are quarantined in the Junk Box for review and deletion later.
- **Send to**—Specify an email address for the recipient.
- **Tag with**—Label the email to warn the user. The default is [SPAM] or [LIKELY_SPAM].

2 Choose an action message marked as Likely Spam. The options are the same as defined for Step 1.

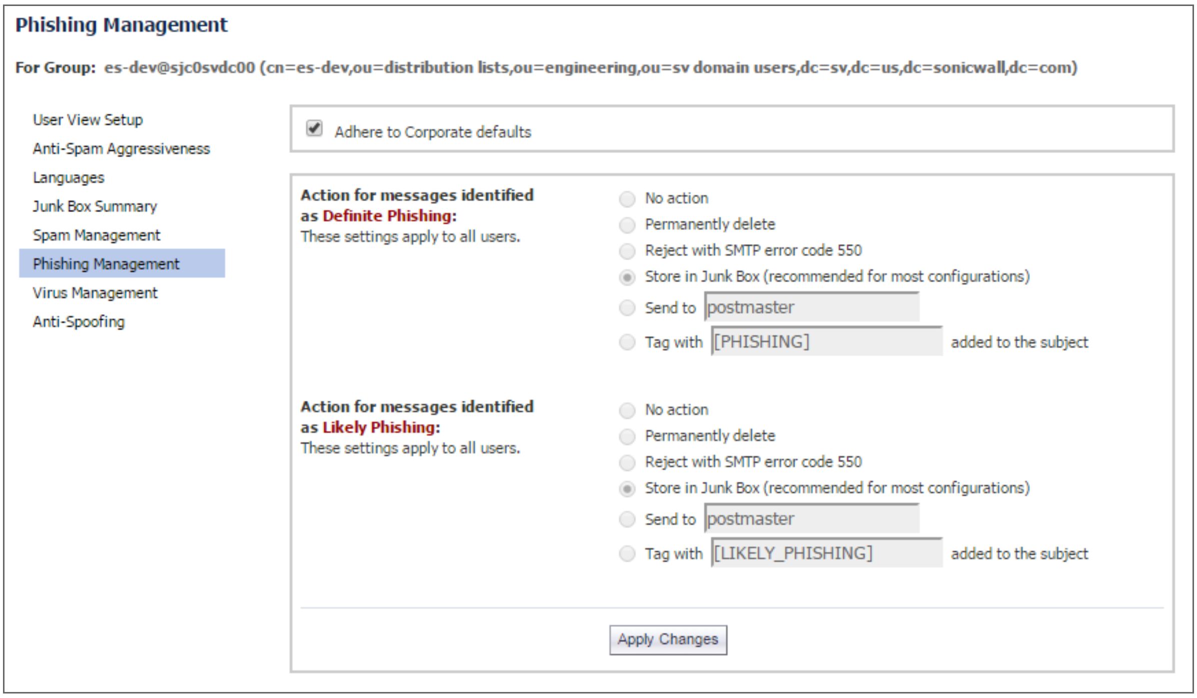
3 Select the check box **This Group accepts automated Allowed Lists** if you want automated Allowed Lists to apply to this group.

4 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, you can configure phishing management differently for different groups. However, unlike Spam Management options, these settings cannot be altered for individual users.

On the Junk Blocking Options page, select **Phishing Management** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for mail tagged as Definite Phishing and LIkely Phishing as described below.


Phishing Management

For Group: es-dev@sjc0svdc00 (cn=es-dev,ou=distribution lists,ou=engineering,ou=sv domain users,dc=sv,dc=us,dc=sonicwall,dc=com)

☑ Adhere to Corporate defaults

Action for messages identified as Definite Phishing:
These settings apply to all users.

○ No action
○ Permanently delete
○ Reject with SMTP error code 550
● Store in Junk Box (recommended for most configurations)
○ Send to postmaster
○ Tag with [PHISHING] added to the subject

Action for messages identified as Likely Phishing:
These settings apply to all users.

○ No action
○ Permanently delete
○ Reject with SMTP error code 550
● Store in Junk Box (recommended for most configurations)
○ Send to postmaster
○ Tag with [LIKELY_PHISHING] added to the subject

To manage Definite Phishing or Likely Phishing for this group:

1 Chose an action for messages marked as Definite Phishing. The options are defined below.

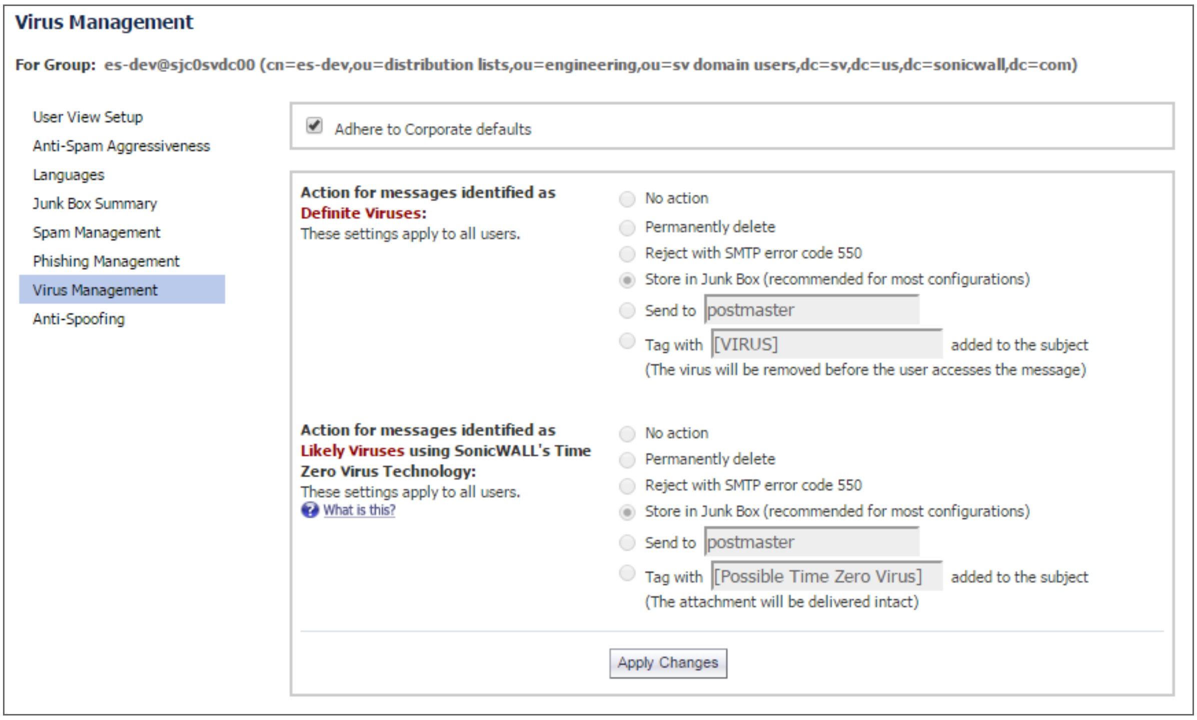
- **No action**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Phishing, messages are permanently deleted.
- **Reject with SMTP error code 550**—Messages are sent back to the sender. In cases of self-replicating viruses that engage the sender’s address book, this can inadvertently cause a denial-of-service to a non-malicious user.
- **Store in Junk Box (recommended for most configurations)**—Messages are quarantined in the Junk Box for review and deletion later.
- **Send to**—Specify an email address for the recipient.
- **Tag with**—Label the email to warn the user. The default is [SPAM] or [LIKELY_SPAM].

2 Choose an action message marked as Likely Phishing. The options are the same as defined for Step 1.

3 Click **Apply Changes**.

Virus Management

On the Junk Blocking Options page, select **Virus Management** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for mail tagged as Definite Viruses and LIkely Viruses as described below.



Virus Management

For Group: es-dev@sjc0svdc00 (cn=es-dev,ou=distribution lists,ou=engineering,ou=sv domain users,dc=sv,dc=us,dc=sonicwall,dc=com)

☑ Adhere to Corporate defaults

Action for messages identified as Definite Viruses:
These settings apply to all users.

- ○ No action
- ○ Permanently delete
- ○ Reject with SMTP error code 550
- ● Store in Junk Box (recommended for most configurations)
- ○ Send to postmaster
- ○ Tag with [VIRUS] added to the subject
  (The virus will be removed before the user accesses the message)

Action for messages identified as Likely Viruses using SonicWALL's Time Zero Virus Technology:
These settings apply to all users.
What is this?

- ○ No action
- ○ Permanently delete
- ○ Reject with SMTP error code 550
- ● Store in Junk Box (recommended for most configurations)
- ○ Send to postmaster
- ○ Tag with [Possible Time Zero Virus] added to the subject
  (The attachment will be delivered intact)

To manage Definite Viruses or Likely Viruses for this group:

1 Chose an action for messages marked as Definite Viruses. The options are defined below.

- **No action**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Phishing, messages are permanently deleted.
- **Reject with SMTP error code 550**—Messages are sent back to the sender. 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.
- **Store in Junk Box (recommended for most configurations)**—Messages are quarantined in the Junk Box for review and deletion later.
- **Send to**—Specify an email address for the recipient.
- **Tag with**—Label the email to warn the user. The default is [SPAM] or [LIKELY_SPAM].

2 Choose an action message marked as Likely Viruses. The options are the same as defined for Step 1.

3 Click **Apply Changes**.

Anti-Spoofing

On the **Junk Blocking Options** page, select **Anti-Spoofing** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options as described below.

To configure the anti-spoofing settings:

1 If you want to **Ignore allow lists** for SPF hard failures, check the box provided.

2 Choose an action message marked as **SPF hard fail**. The options are:

No Action	No action is taken against messages marked as SPF hard fail.
Permanently delete	Messages marked as SPF hard fail are permanently deleted.
Reject with SMTP error code 550	Messages marked as SPF hard fail are rejected with an SMTP error code 550.
Store in Junk Box (recommended for most configurations)	Messages marked as SPF hard fail are stored in the Junk Box. This is the recommended setting for most configurations.
Send to [field]	Messages marked as SPF hard fail are sent to the user specified in the available field. For example, you can send to `postmaster`.
Tag with [field] added to the subject	Messages marked as SPF hard fail are tagged with a term in the subject line. For example, you may tag the messages `[SPF Hard Failed]`.
Add X-Header: X-[field]:[field]	Messages marked as SPF hard failed add an X-Header to the email with the key and value specified to the email message. The first text field defines the X-Header. The second text field is the value of the X-Header. For example, a header of type X-`EMSJudgedThisEmail` with value `spfhard` results in the email header as: `X-EMSJudgedThisEmail:spfhard`.

3 For SPF soft failures, decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

4 For DKIM settings, decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

5 Choose the action to take for messages marked as **DKIM signature failed**. The options are the same as those listed for Step 2. In the text field, you can use text to indicate DKIM failures, rather than SPF failures.

6 Select **Apply Changes** when done.

Forcing All Members to Group Settings

Select the check box next to the Group(s) you want to adhere to Group Settings. Then, click the **Force All Members to Group Settings** button. All individual settings are overwritten by the Group Settings.

Organizations

The **System Setup | Users, Groups & Organizations > Organizations** page lists the available organizational units associated with the SonicWall solution.

This section includes the following topics:

- Organizations Overview
- Adding an Organization
- Signing In as an OU Admin

- Configuring OU Settings
- Removing an Organization

Organizations Overview

Organizations are a smaller group of domains set by the Global Administrator as an efficient way of managing an entire enterprise-sized SonicWall system setup. These subset groups, also known as an Organizational Unit (OU), are managed by a sub-administrator, called the OU Administrator. The OU Administrator role has full administrative rights to the OU he has been assigned to by the Global Administrator.

The OU Admin can log in as any other user within the group of domains assigned to edit a user's individual settings, edit group settings for groups within their OU, and manage Junk Boxes, and view Reports. The OU Admin is not able to add or remove domains from an Organization, regardless if he is the OU Admin of that Organization; only the Global Administrator has the ability to perform these tasks.

Adding an Organization

To add an organization:

1 Navigate to the **System Setup | Users, Groups & Organizations > Organizations** page.

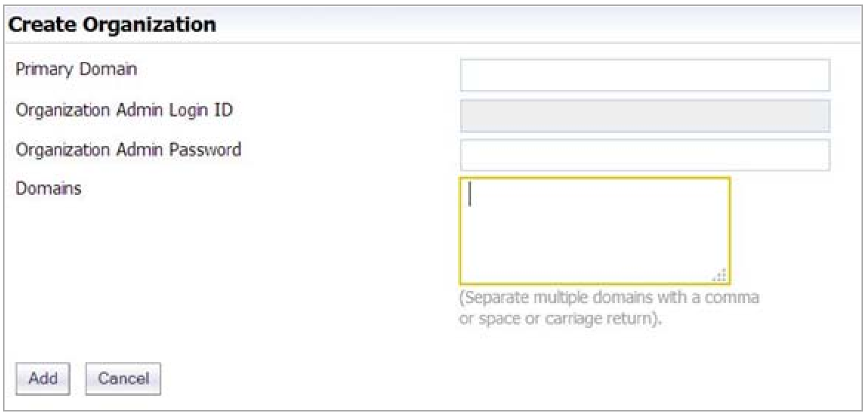
2 Click the **Add Organization** button.

3 Enter the **Primary Domain**. Acceptable domains follow the form of `domain.com` or `sub.domain.com`. The **Organization Admin Login ID** is automatically populated based on what is entered as the Primary Domain.

4 Enter the **Organization Admin Password**.

5 Add any other **Domains** to the field provided. Separate multiple domains with a comma, space or carriage return.

6 Then, click the **Add** button. A notification appears, stating that old data is being migrated to the organization level. Acknowledge the notification by clicking **OK**.


Create Organization
Primary Domain
Organization Admin Login ID
Organization Admin Password
Domains
(Separate multiple domains with a comma or space or carriage return).
Add
Cancel

Consider the following when creating a new organization:

- User settings are migrated to the newly created organization.
- LDAP configured at the Global Administrator level is not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the LDAP for his organization. Neglecting to configure the LDAP can potentially break user authentication for domains of that organization.

- Group Settings configured at the Global Administrator level are not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the Group Settings for his organization.
- User Rights configured at the Global Administrator level is not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the User Rights for the users in his organization.
- Group Roles configured at the Global Administrator level are not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the Group role for the groups in his organization.

ⓘ **NOTE:** Any domains added in the Create Organization screen that are not already listed in the **Network Architecture > Server Configuration** page are not automatically added to the server. The Global Administrator needs to add these domains to the Network Architecture path separately.

Signing In as an OU Admin

As a Global Administrator, you can sign in to any **Organization** as an OU Admin. Click the **Sign in as OU Admin** icon. You are automatically directed as the OU Admin to the respective OU in a new window. Click the **Log Out** icon to log out as the OU Admin.

Configuring OU Settings

As a Global Administrator, you can subscribe to alerts for a specific Organization so that you are notified about updates and changes made to this Organization. Click the **Settings** icon of the Organization you want alerts for. Then, click the **Change** link in the **Alerts** column, and confirm your choice.

Removing an Organization

To delete an Organization, click the **Remove** button of the Organization you wish to delete.

Users and Groups in Multiple LDAP

The administrators of each organization can create a master LDAP group that encompasses all their users and groups. That master group can then be used to administer SonicWall settings across the organization, even if there are multiple domains. With a group that contains all the members of the LDAP, the administrator effectively administers the LDAP.

See the following sections for more information:

- Users
- Groups

Users

When an administrator logs in and views the **System Setup | Users, Groups & Organizations > Users** page, one sees all the email addresses that exist on that instance of SonicWall. The administrator can then narrow the view to only the entries from that LDAP.

ⓘ **NOTE:** The **Using Source** selection allows administrators to access users who were added directly to SonicWall, and did not come in through an LDAP entry. These entries are not deleted with an LDAP deletion.

Topics:

- Filtering through User View Setup
- Finding a Specific User
- Adding a New User
- Deleting a User

Filtering through User View Setup

To filter the user view setup by source:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Organizations**, and then **Users**.
3. Scroll down to **User View Setup**.
4. From the **Using Source** drop down menu, choose the LDAP source associated with the users you want to view. Click **Go**.

You only see the users associated with that LDAP source. The list of users can be sorted by user name, primary email address, user rights, or source. If you have already filtered by source, sorting by source will not retrieve anything outside the filter.

To sort a list of users, click on the column heading that describes the sort type. Click again to sort in reverse order.

Each LDAP user record has a check box next to it. To edit a user or users, select the box. If you select one user, you can log in as that user or edit that user's rights, for example, to elevate them to group admin or help desk-level rights. If you select more than one user, you can only change their message management style to the default style.

Finding a Specific User

Because an LDAP source usually has many records, SonicWall has provided several ways of looking for a specific user.

To find a specific user:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Organizations**, and then click **Users**.
3. Scroll down to **User View Setup**.
4. From the F**ind all users in column** drop down menu, choose either the username or the primary email address to search on.
5. Choose which type of search you want. Exact matches are the fastest, but matches contain your search term may help you more if you cannot remember the exact username or address you are looking for.
6. Enter your search term.
7. Click **Go**. You see the users who mach your search criteria.

Adding a New User

If you want to add a user who does not appear in the automatically-generated list from your LDAP, you can choose to manually add an account. If an LDAP is not provided, the user will be added to the default LDAP source. You cannot add users to your LDAP from the Email Security interface.

To add a user:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Organizations**, and then click **Users**.
3. Scroll down to **User View Setup**.
4. Click **Add**.
5. Enter the user's fully-qualified email address, choose a source (if any), and any aliases you wish to associate with the user.

Deleting a User

To delete a user:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Organizations**, and then **Users**.
3. Scroll down to **User View Setup**.
4. Select the user you wish to delete. Deleting a user will not remove the user's LDAP entry, only the entry in the Email Security system.
5. Click **Remove**.

Groups

Use the **Users, Groups & Organizations > Groups** page to incorporate or extend existing LDAP groups. You can also change a group's security role in the Email Security system and view the membership of a group.

This section contains the following subsections:

- Filtering through Group View
- Changing a Group's Role
- Viewing Members of a Group
- Setting Junk Blocking by Group

Filtering through Group View

To filter the group view by source:

1. Log in as the Email Security administrator.
2. Click **Users, Groups & Organizations**, and then **Groups**.
3. Scroll down to **Assign Roles to Groups Found in LDAP**.
4. From the **Using Source** drop down menu, choose the LDAP source associated with the groups you want to view. Click **Go**.

5 If you do not see the group you want, click the **Add Group** button. You can choose an existing group from one of your sources. You cannot create a group that does not exist.

Changing a Group’s Role

You can change each group’s role in Email Security. These roles determine a user’s permissions to change Email Security settings, including user settings.

To change a group’s role:

1 Log in as the Email Security administrator.

2 Click **Users, Groups & Organizations**, and then **Groups**.

3 Scroll down to **Assign Roles to Groups Found in LDAP**.

4 Select the box next to the group you want to change.

5 Click **Edit Role**.

6 In the pop-up window, choose the role you want that group to have. You can choose only one role per group. If a user is in multiple groups, permissions are granted in the order in which the groups are listed in the user’s profile.

7 Click **Apply Changes**. You see a status update at the top of the page.

Viewing Members of a Group

To view the members of a particular group:

1 Log in as the Email Security administrator.

2 Click **Users, Groups & Organizations**, and then **Groups**.

3 Scroll down to **Assign Roles to Groups Found in LDAP**.

4 Select the box next to the group to see its membership.

5 Click **List Members**. A pop-up window displays that lists the group’s membership by primary email address.

Setting Junk Blocking by Group

You can use the existing LDAP groups to configure the filtering sensitivity for different user groups. For example, your sales group might need to receive email written in foreign languages.

To set junk blocking by group:

1 Log in as the Email Security administrator.

2 Click **Users, Groups & Organizations**, and then **Groups**.

3 Scroll down to **Set Junk Blocking Options for Groups Found in LDAP**.

4 Under **Using LDAP**, select your LDAP.

5 Select a group to edit.

6 Click **Edit Junk Blocking Options**. The Group Junk Blocking Options window displays. Follow the recommendations described in Anti-Spam.

12

System Setup | Network and Junkbox Commands

This section provides configuration procedures for the network and Junk Box settings.

Topics:

- Network
- Junk Box

Network

On the **System Setup | Server > Network** page, you can configure various settings:

- Server Configuration
- MTA Configuration
- Email Address Rewriting
- Trusted Networks

Server Configuration

The first step of server configuration is to select the Email Security architecture. Choose either **All in One** or **Split**. The user interface actively configures the display in response to your selection. Refer to Email Security Deployment Architecture for Appliances for more information on the different configurations.

To configure the your server, follow these general processes and see the details provided in the referenced sections.

For All in One Configuration	For Split Configuration
1. Select the **All in One** architecture on the **System Setup | Network > Server Configuration** page.	1. Select the **Split** architecture on the **System Setup | Network > Server Configuration** page.
2. Configure the inbound email flow and apply it as described in Inbound Mail Path Configuration.	2. Choose the button to designate the server as a **Remote Analyzer** or **Control Center**.
3. Configure the outbound email flow and apply it as described in Outbound Mail Path Configuration.	3. If you selected Control Center, choose the additional functions that may apply: **Main Control Center**, **Search Engine Server**, or **Reporting Server**. A Control Center can have more than one function.
4. Test mail servers.	4. Add or delete servers on a Split configuration as described in Managing Servers for a Split architecture.

For All in One Configuration	For Split Configuration
	5. Select the Remote Analyzer to configure the inbound email flow and apply it as described in Inbound Mail Path Configuration.
	6. Select the Remote Analyzer to configure the outbound email flow and apply it as described in Outbound Mail Path Configuration.
	7. Configure communications between Remote Analyzers and Control Centers as described in Configuring Communications for Split Configurations.
	8. Test mail servers.

Additional information on managing a Split configuration is provided in Changing Configurations.

Inbound Mail Path Configuration

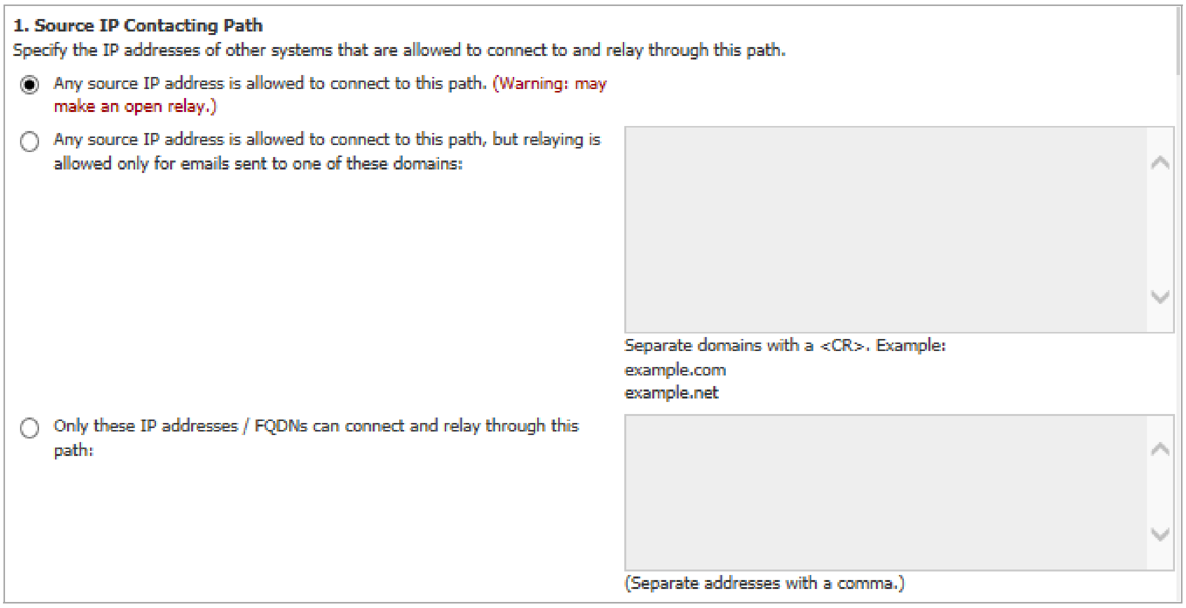
The inbound path options for both All in One and Split configurations are very similar. The window is divided into several segments with various options for each. Definitions and recommendations are reviewed in the following sections:

- Source IP Contacting Path for Inbound Mail
- Path Listens On for Inbound Mail
- Destination of Path for Inbound Mail
- Directory Harvest Attack (DHA) Protection Settings for Inbound Mail
- Advanced Settings for Inbound Mail

The following descriptions apply whether you select **Add Path** or **Edit Path**. To remove a path from the configuration, select the path and click **Delete Path.**

Source IP Contacting Path for Inbound Mail

The **Source IP Contacting Path** section allows you to specify the IP addresses of other systems that are allowed to connect to and relay through this path.


1. Source IP Contacting Path

Specify the IP addresses of other systems that are allowed to connect to and relay through this path.

● Any source IP address is allowed to connect to this path. (Warning: may make an open relay.)

○ Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains:

Separate domains with a <CR>. Example:
example.com
example.net

○ Only these IP addresses / FQDNs can connect and relay through this path:

(Separate addresses with a comma.)

Select one of the following options:

- **Any source IP address is allowed to connect to this path**—Use this setting if you want any sending email server to be able to connect to this path and relay messages. Using this option could make your server an open relay.

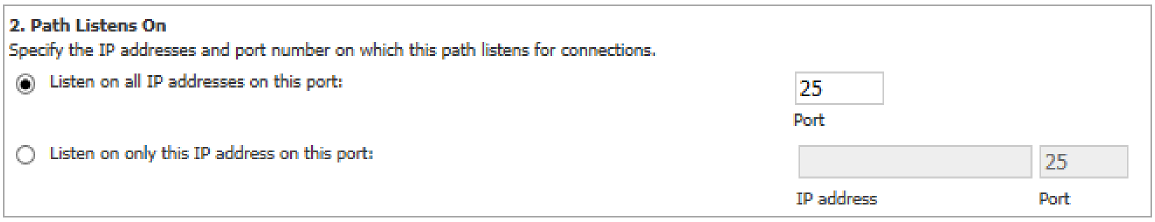
△ **CAUTION: This may make an open relay.**

ⓘ **NOTE:** You need to use this setting if you configure your SonicWall Email Security solution to listen for both inbound and outbound email traffic on the same IP address on port 25.

- **Any source IP address is allowed to connect to this path but relaying is allowed only for specified domains**—Use this setting if you want any sending email servers to connect to this path, but you want to relay messages only to the domains specified. Simply enter the domains in the space provided, adding one domain per line.
- **Only these IP addresses can connect and relay**—Use this setting if you know the sending email server IP addresses, and you do not want any other servers to connect. Separate multiple IP addresses with a comma.

Path Listens On for Inbound Mail

The **Path Listens On** section allows you to specify the IP addresses and port number on which the path listens for connections.


2. Path Listens On

Specify the IP addresses and port number on which this path listens for connections.

● Listen on all IP addresses on this port: 25 Port

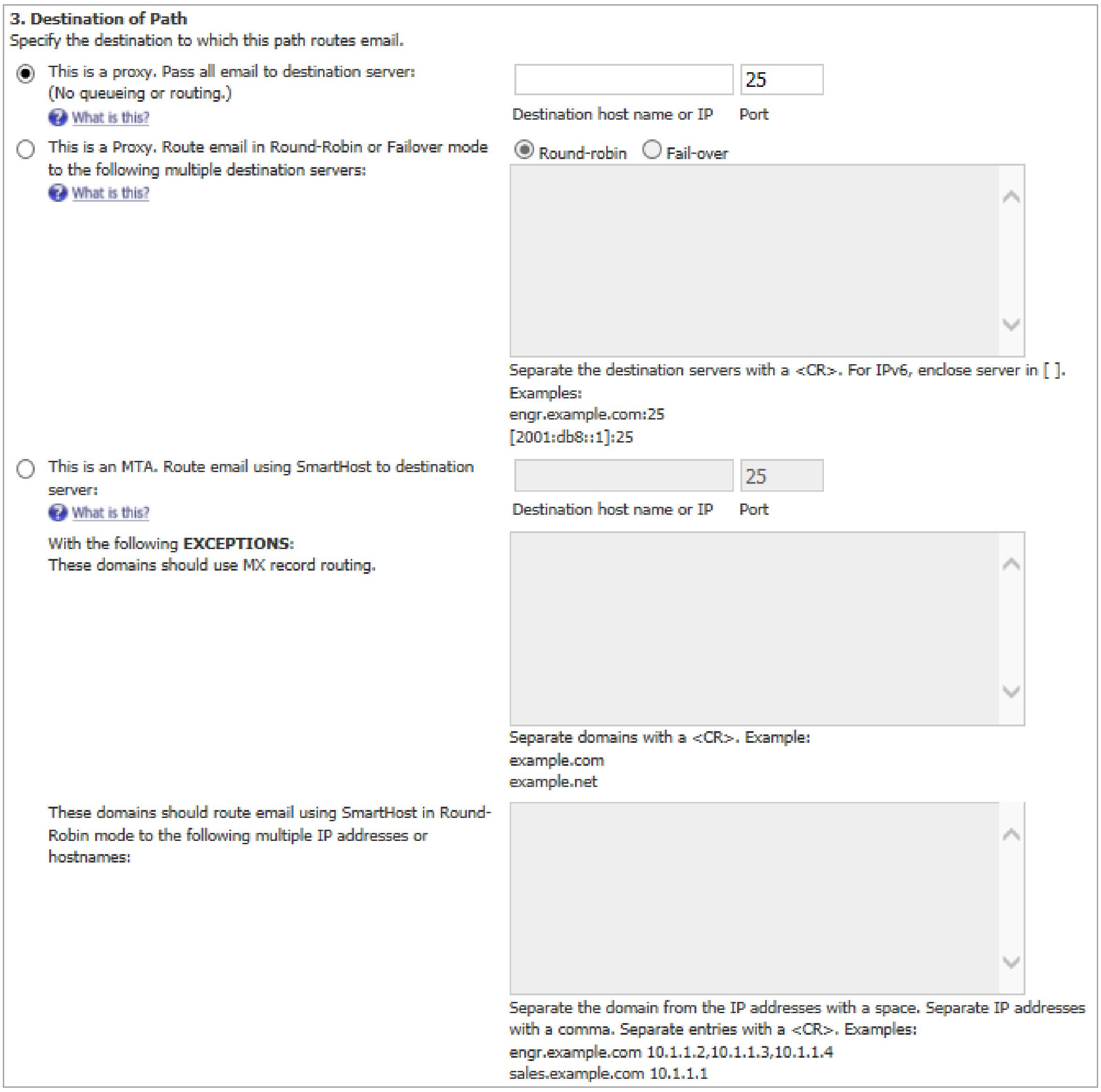
○ Listen on only this IP address on this port: IP address 25 Port

- **Listen for all IP address on this port**—This is the typical setting for most environments, 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 on this machine, you can specify which IP address and port number to listen on.

Destination of Path for Inbound Mail

Destination of Path section allows you to specify the destination server for all incoming email traffic in this path.



3. Destination of Path

Specify the destination to which this path routes email.

● This is a proxy. Pass all email to destination server:
(No queueing or routing.)
What is this?

25
Destination host name or IP Port

○ This is a Proxy. Route email in Round-Robin or Failover mode to the following multiple destination servers:
What is this?

● Round-robin ○ Fail-over

Separate the destination servers with a <CR>. For IPv6, enclose server in [ ].
Examples:
engr.example.com:25
[2001:db8::1]:25

○ This is an MTA. Route email using SmartHost to destination server:
What is this?

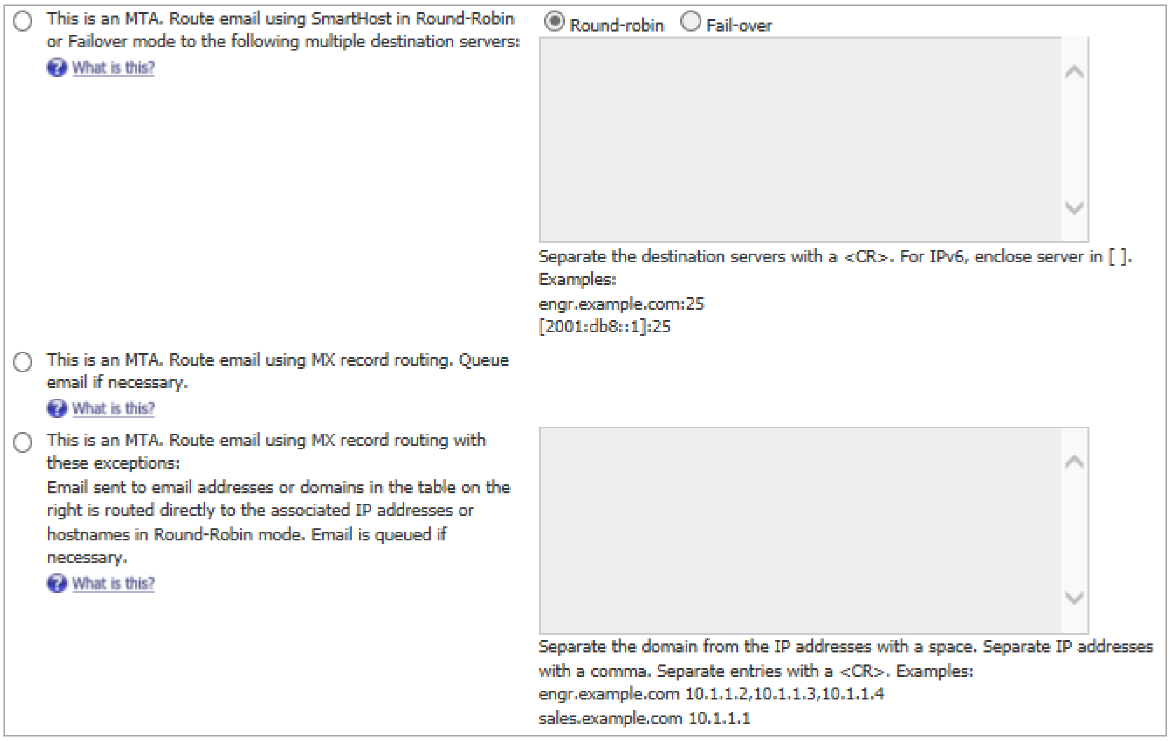
25
Destination host name or IP Port

With the following **EXCEPTIONS**:
These domains should use MX record routing.

Separate domains with a <CR>. Example:
example.com
example.net

These domains should route email using SmartHost in Round-Robin mode to the following multiple IP addresses or hostnames:

Separate the domain from the IP addresses with a space. Separate IP addresses with a comma. Separate entries with a <CR>. Examples:
engr.example.com 10.1.1.2,10.1.1.3,10.1.1.4
sales.example.com 10.1.1.1



○ This is an MTA. Route email using SmartHost in Round-Robin or Failover mode to the following multiple destination servers:

What is this?

● Round-robin ○ Fail-over

Separate the destination servers with a <CR>. For IPv6, enclose server in [ ]. Examples:
engr.example.com:25
[2001:db8::1]:25

○ This is an MTA. Route email using MX record routing. Queue email if necessary.

What is this?

○ This is an MTA. Route email using MX record routing with these exceptions:
Email sent to email addresses or domains in the table on the right is routed directly to the associated IP addresses or hostnames in Round-Robin mode. Email is queued if necessary.

What is this?

Separate the domain from the IP addresses with a space. Separate IP addresses with a comma. Separate entries with a <CR>. Examples:
engr.example.com 10.1.1.2,10.1.1.3,10.1.1.4
sales.example.com 10.1.1.1

- **This is a Proxy. Pass all email to destination server**—This setting configures the 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. Enter the host name or IP address and the port number of the downstream email server. Note that no queuing or routing are performed.
- **This is a Proxy. Route email in Round-Robin or Failover mode to the following multiple destination servers**—This setting configures the path to act as a proxy and relay messages to a downstream email server. If Round-Robin is selected, email is load-balanced by sending a portion of the email flow through each server listed in the text box. If Failover is selected, email is sent to the servers listed in the text box only if the downstream server is unavailable. Email is queued if all of the servers listed are unavailable.
- **This is an MTA. Route email using SmartHost to destination server**—This setting is similar to the “This is a Proxy. Pass all email to destination” option, except that incoming messages are accepted and queued if the downstream server is unavailable. In this instance, this path acts as a SMTP SmartHost. With this setting selected, you can also include Exceptions, specifying which domains should use MX record routing and which should use the associated IP address or hostname.
- **This is an MTA. Route email using SmartHost in Round-Robin or Failover mode to the following multiple destination servers**—This setting is similar to the previous MTA option, however incoming messages can be routed to multiple servers. If Round-Robin is selected, email is load-balanced by sending a portion of the email flow through each server listed in the text box. If Failover is selected, email is sent to the servers listed in the text box only if the downstream server is unavailable. Email is queued if all of the servers listed are unavailable.
- **This is an MTA. Route email using MX record routing. Queue email if necessary**—This setting routes any mail by standard MX (Mail Exchange) records. Messages can be queued on disk and will retry transmissions later if the destination SMTP server is not immediately available.
- **This is an MTA. Route email using MX record routing with these exceptions**—This setting routes any mail by standard MX (Mail Exchange) records. However, email messages sent to the email addresses or domains in the table to the right are routed directly to the associated IP address or hostname. Messages can be queued on disk and will retry transmissions later if the destination SMTP server is not immediately available.

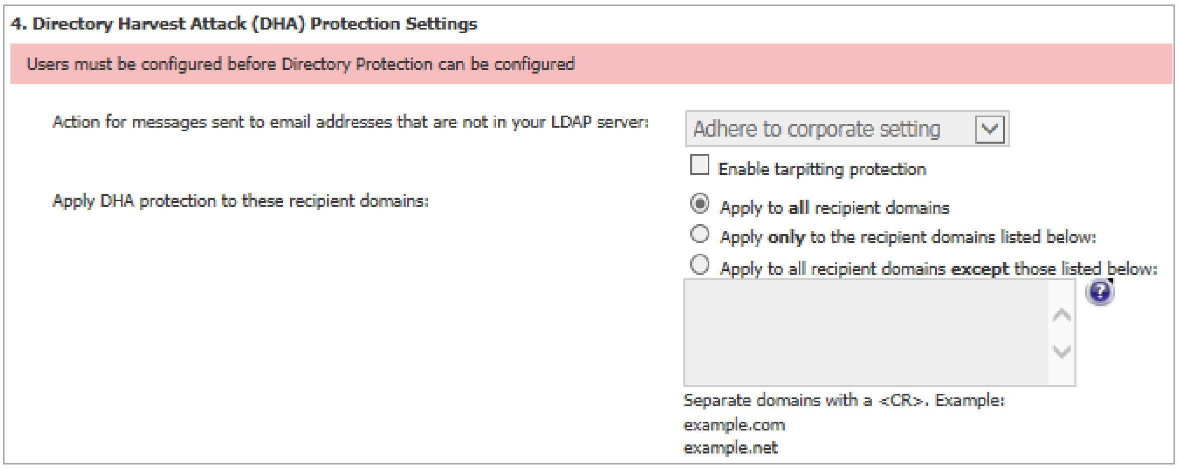
NOTE: You can specify email addresses in addition to domains in this routing table. Also, hostnames can be specified instead of IP addresses. For example, if you want to route customer service emails to one downstream server and the rest of the traffic to a different downstream server, you can specify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

```
service@mycompany.com
10.1.1.1

mycompany.com
internal_mailserver.mycompany.com
```

Directory Harvest Attack (DHA) Protection Settings for Inbound Mail

Directory Harvest Attack Protection allows you to configure settings to protect against spammers that attempt to find valid email addresses on your directory.



4. Directory Harvest Attack (DHA) Protection Settings

Users must be configured before Directory Protection can be configured

Action for messages sent to email addresses that are not in your LDAP server: Adhere to corporate setting

□ Enable tarpitting protection

Apply DHA protection to these recipient domains:

● Apply to **all** recipient domains

○ Apply **only** to the recipient domains listed below:

○ Apply to all recipient domains **except** those listed below:

Separate domains with a <CR>. Example:
example.com
example.net

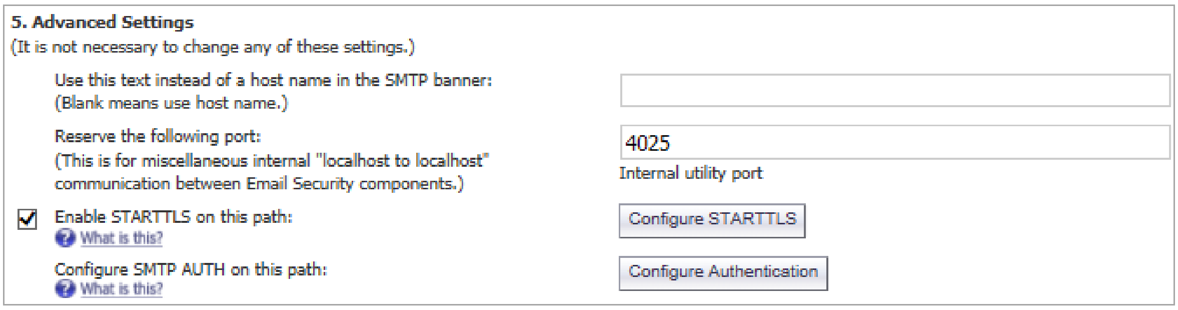
Configure any of the following settings:

- **Action for messages sent to email addresses that are not in your LDAP server**—Select one of the following from the drop down menu:
    - **Adhere to corporate setting—**Messages from addresses not in your LDAP adhere to the corporate settings.
    - **Process all messages the same—**Messages from addresses not in your LDAP will be processed the same as messages from addresses in your LDAP server.
    - **Permanently delete—**Messages from addresses not in your LDAP will be permanently deleted.
    - **Reject invalid addresses—**Messages from addresses not in your LDAP will be rejected.
    - **Always store in Junk Box—**Messages from addresses not in your LDAP will be stored in your Junk Box.
- **Enable tarpitting protection**—Select the check box to enable tarpitting protection, which slows the transmission of email messages sent in bulk by spammers.
- **Apply DHA protection to these recipient domains**—Select one of the following options for applying DHA protection:
    - **Apply to all recipient domains**—Select to apply DHA protection to all recipient domains.
    - **Apply only to the recipient domains listed below**—In the text box, specify the recipient domains to which DHA protection applies.

- **Apply to all recipient domains except those listed below**—In the text box specify the recipient domains to which DHA protection does NOT apply.

Advanced Settings for Inbound Mail

The following settings are optional. When finished configuring settings, click Apply to save changes made for the outbound path.



5. Advanced Settings
(It is not necessary to change any of these settings.)

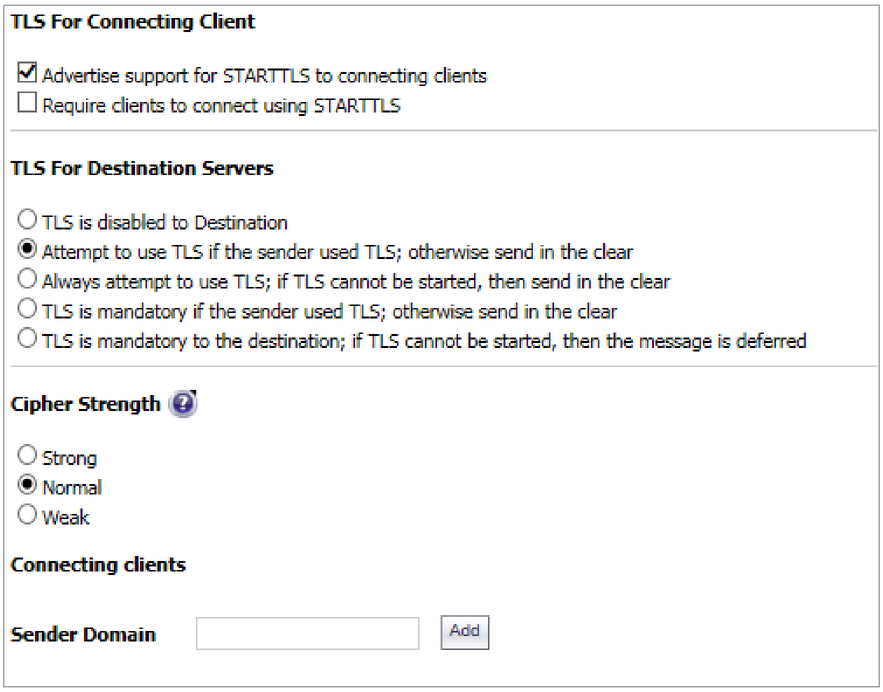
Use this text instead of a host name in the SMTP banner:
(Blank means use host name.)

Reserve the following port:
(This is for miscellaneous internal "localhost to localhost" communication between Email Security components.)
4025
Internal utility port

☑ Enable STARTTLS on this path:
What is this?

Configure SMTP AUTH on this path:
What is this?

- **Use this text instead of a host name in the SMTP banner**—This setting allows you to customize the host name of the server that appears in the heading of the email messages relayed through this path. If left blank, the host name is used.
- **Reserve the following port**—This setting allows you to designate a port for miscellaneous “localhost to localhost” communication between Email Security components.
- **Enable StartTLS on this path**—Select this check box if you want a secure internet connection for email. SonicWall Email Security uses Transport Layer Security (TLS) to provide the secure internet connection. Click the **Configure STARTTLS** button to configure encrypted email communications.



TLS For Connecting Client

☑ Advertise support for STARTTLS to connecting clients
☐ Require clients to connect using STARTTLS

TLS For Destination Servers

○ TLS is disabled to Destination
● Attempt to use TLS if the sender used TLS; otherwise send in the clear
○ Always attempt to use TLS; if TLS cannot be started, then send in the clear
○ TLS is mandatory if the sender used TLS; otherwise send in the clear
○ TLS is mandatory to the destination; if TLS cannot be started, then the message is deferred

Cipher Strength

○ Strong
● Normal
○ Weak

Connecting clients

Sender Domain

a Set the **TLS for Connecting Client**. Choose one of these options:

- **Advertise support for STARTTLS to connecting clients**
- **Require clients to connect using STARTTLS**

b Set the **TLS for Destination Servers**. Choose one of the these options:

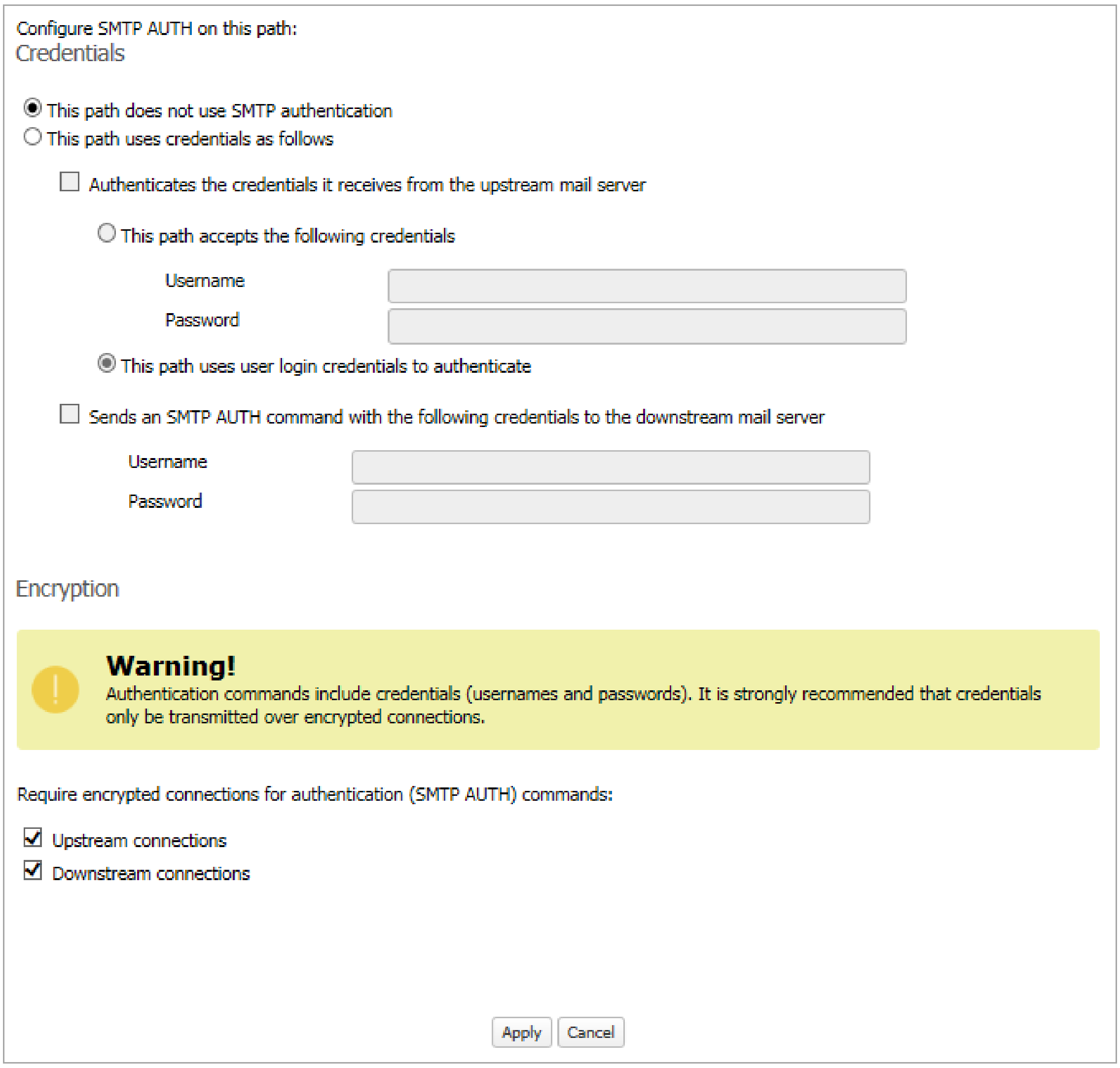
- **TLS is disabled to Destination**
- **Attempt to use TLS if the sender used TLS; otherwise send in the clear**
- **Always attempt to use TLS; if TLS cannot be started, then send in the clear**
- **TLS is mandatory if the sender used TLS; otherwise send in the clear**
- **TLT is mandatory to the destination; if TLS cannot be started, then the message is deferred**

c Set the **Cipher Strength**; select from **Strong**, **Normal** or **Weak**.

d Provide the **Sender Domain** for the Destination servers and select **Add**.

e Select **Apply** when settings are complete.

- **Configure SMTP AUTH on this path**—Authentication provides a way for a mail server to verify the identity of the email sender. During authentication, the sender supplies credentials to the receiving mail server, which may refuse email delivery if the sender's identity cannot be verified.



Configure SMTP AUTH on this path:

Credentials

● This path does not use SMTP authentication

○ This path uses credentials as follows

□ Authenticates the credentials it receives from the upstream mail server

○ This path accepts the following credentials

Username

Password

● This path uses user login credentials to authenticate

□ Sends an SMTP AUTH command with the following credentials to the downstream mail server

Username

Password

Encryption

Warning!
Authentication commands include credentials (usernames and passwords). It is strongly recommended that credentials only be transmitted over encrypted connections.

Require encrypted connections for authentication (SMTP AUTH) commands:

☑ Upstream connections

☑ Downstream connections

Select one of three options:

- **This path does not use SMTP authentication**—This is the default setting, where no authentication is required.

- **This path uses credentials as follows**—This option allows you to perform Server Side Authentication and Client Side Authentication.
  - For Server Side Authentication, check the box for **Authenticates the credentials it received from the upstream mail server** and also choose one of the following:
    - Use **This path accepts the following credentials** if you want to configure a single set of credentials that is used for all email. These credentials can be used to identify a specific customer or server. Provide the username and password to complete the configuration.
    - Use **This path uses user login credentials to authenticate** to require user authentication.
  - For Client Side Authentication (for example, when sending outbound email through an ISP that requires authentication), select **Sends an SMTP AUTH command with the following credentials to the downstream mail server**. Provide the username and password to complete the configuration.
- At the bottom of the window, you can require encryption for both upstream and downstream connections. The default is that both are selected.

△ CAUTION: Authentication commands include credentials like usernames and passwords. To protect them they should only be transmitted over encrypted connections.

Outbound Mail Path Configuration

The outbound path options for both All in One and Split configurations are very similar. The window is divided into several segments with various options for each. Definitions and recommendations are reviewed in the following sections:

- Source IP Contacting Path for Outbound Mail
- Path Listens On for Outbound Mail
- Destination of Path for Outbound Mail
- Advanced Settings for Outbound

The following descriptions apply whether you select **Add Path** or **Edit Path**. To remove a path from the configuration, select the path and click **Delete Path.**

Source IP Contacting Path for Outbound Mail

This section allows you to specify the IP addresses of other systems that are allowed to connect to and relay outgoing mail. Select from the following:

- **Any source IP address is allowed to connect to this path**—Use this setting if you want any sending email server to be able to connect to this path and relay messages. Using this option could make your server an open relay.

△ CAUTION: **This may make an open relay.**

ⓘ **NOTE:** You need to use this setting if you configure your SonicWall Email Security solution to listen for both inbound and outbound email traffic on the same IP address on port 25.

- **Only these IP addresses/FQDNs can connect and relay through this path**—Use this setting if you know the sending email server IP addresses and you do not want any other servers to connect. Separate multiple IP addresses with a comma.

  ⓘ **NOTE:** If your configuration is running in Split mode, and this path is on a remote analyzer, the control center must be able to connect and relay through this path.

Path Listens On for Outbound Mail

This section allows you to 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. The default port 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 to.

Destination of Path for Outbound Mail

Destination of path allows you to specify the destination server to which this pat routes email. You can choose whether to make a path through the SonicWall Email Security, or through one of the following:

- If **Round robin** is specified, email traffic is balanced by sending a portion of the 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 **Failover** 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.

Choose one of these options in the **Destination of Path** section.

- **This is a Proxy. Pass all email to destination server**—This setting configures the path to act as a proxy and relay messages to an upstream MTA. If the upstream server is unavailable, outgoing messages will not be accepted or queued. Note that no queuing or routing are performed.
- **This is a Proxy. Route email in Round-Robin or Failover mode to the following multiple destination servers**—This setting configures the path to act as a proxy and relay messages to a downstream email server. Select Round-Robin to balance the email load by sending a portion of the email flow through each server listed in the text box. Select Failover to send email to the servers listed in the text box only if the downstream server is unavailable. Email is queued if all of the servers listed are unavailable.
- **This is an MTA. Route email using SmartHost to destination server**—This setting is similar to the "This is a Proxy. Pass all email to destination" option, except that outgoing messages are accepted and queued if the upstream MTA is unavailable. These domains should use MX (Mail Exchange) record routing. However, you can list the specific domains that won't use MX record routing.

  You can also specify which domains should route using SmartHost in Round-Robin mode. Provide IP addresses or host names.
- **This is an MTA. Route email using SmartHost in Round-Robin or Failover mode to the following multiple destination servers**—This setting is similar to the previous MTA option, however outgoing messages can be routed to multiple upstream MTAs. Select Round-Robin to balance email load by sending a portion of the email flow through each MTA listed in the text box. Select Failover to send email to the MTAs listed in the text box only if the upstream MTA is unavailable. Email is queued if all of the MTAs listed are unavailable.
- **This is an MTA. Route email using MX record routing. Queue email if necessary**—This setting routes any outbound email messages by standard MX records.

- **This is an MTA. Route email using MX record routing with these exceptions**—This setting routes any outbound email messages by standard MX records. However, email messages sent to the email addresses or domains listed in the configuration table are routed directly to the associated IP address or hostname in Round-Robin mode. Messages are queued if necessary.

Advanced Settings for Outbound

The following settings are optional. When finished configuring settings, click **Apply** to save changes made for the outbound path.

- **Use this text instead of a host name in the SMTP banner**—This setting allows you to customize the host name of the server that appears in the heading of the email messages relayed through this path. If left blank, the host name is used.
- **Reserve the following port**—This designates a port for miscellaneous "localhost to localhost" communication between Email Security components.
- **Enable STARTTLS on this path**—Check this box for a secure internet connection for email. SonicWall Email Security uses Transport Layer Security (TLS) to provide the secure internet connection. Click the **Configure STARTTLS** button to configure encrypted email communications.

    a Set the **TLS for Connecting Client**. Choose one of these options:

    - **Advertise support for STARTTLS to connecting clients**
    - **Require clients to connect using STARTTLS**

    b Set the **TLS for Destination Servers**. Choose one of the these options:

    - **TLS is disabled to Destination**
    - **Attempt to use TLS if the sender used TLS; otherwise send in the clear**
    - **Always attempt to use TLS; if TLS cannot be started, then send in the clear**
    - **TLS is mandatory if the sender used TLS; otherwise send in the clear**
    - **TLT is mandatory to the destination; if TLS cannot be started, then the message is deferred**

    c Set the **Cipher Strength**; select from **Strong**, **Normal** or **Weak**.

    d Provide the **Recipient Domain** for the **Destination servers** and select **Add**.

    e Select **Apply** when settings are complete.

- **Configure SMTP AUTH on this path**—Authentication provides a way for a mail server to verify the identity of the email sender. During authentication, the sender supplies credentials to the receiving mail server, which may refuse email delivery if the sender's identity cannot be verified. Select one of three options:
    - **This path does not use SMTP authentication**—This is the default setting, where no authentication is required.
    - **This path uses credentials as follows**—This option allows you to perform Server Side Authentication and Client Side Authentication.
        - For Server Side Authentication, check the box for **Authenticates the credentials it received from the upstream mail server** and also choose one of the following:
            - Use **This path accepts the following credentials** if you want to configure a single set of credentials that is used for all email. These credentials can be used to identify a specific customer or server. Provide the username and password to complete the configuration.

        - Use **This path uses user login credentials to authenticate** to require user authentication.
    - For Client Side Authentication (for example, when sending outbound email through an ISP that requires authentication), select **Sends an SMTP AUTH command with the following credentials to the downstream mail server**. Provide the username and password to complete the configuration.
- At the bottom of the window, you can require encryption for both upstream and downstream connections. The default is that both are selected.

△ **CAUTION:** Authentication commands include credentials like usernames and passwords. To protect them they should only be transmitted over encrypted connections.

Managing Servers for a Split architecture

A Split architecture is made up of at least one Control Center and one or more Remote Analyzers. A Control Center can perform as the main control center, the search engine server and/or the reporting server. Remote analyzers can process inbound messages, outbound messages or both.

To configure a Split architecture:

1. Navigate to **System Setup | Network > Server Configuration** on the **MANAGE** view.
2. Choose the **Split** option.
3. Designate the server as a **Remote Analyzer** or **Control Center**.
4. If you selected Control Center, select all the additional functions that apply to the server: **Main Control Center**, **Search Engine Server**, or **Reporting Server**.
5. Click **Apply**.
6. Click the **Test Connectivity** button to verify if the server successfully connected to the Control Center. It can take 15 seconds to refresh settings so if the first test fails, try it again.

To add a Remote Analyzer:

1. Click the **Add Server** button in the **Inbound Remote Analyzer Paths** section.
2. Enter the **Remote Analyzer's hostname**.
3. Enter the port number for the field called **Remote Analyzer allows http access on port number**.
4. Check the box if your configuration **Requires SSL**.
5. List the **Hostname in received header**.
6. Click the **Add** button.

    ⓘ **NOTE:** If the network traffic has high volume, it might take some time before the new Remote Analyzer is displayed in the **Input Remote Analyzer** table.

7. Click the **Test Connectivity** button to verify if the server successfully connected to the Control Center. It can take 15 seconds to refresh settings so if the first test fails, try it again.

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.

To add a Control Center:

1. Click **Add Server** in the Control Center section of the Server Configuration window.
2. Enter the **Control Center Hostname**.

3 Enter the port number for the field called **Control Center allows http access on port number**.

4 Click **Add**.

5 Click the **Test Connectivity** button to verify if the server successfully connected to the Control Center. It can take 15 seconds to refresh settings so if the first test fails, try it again.

To delete a Remote Analyzer:

ⓘ **NOTE:** Before deleting a Remote Analyzer, verify that it has no messages in the queue for quarantine.

1 Stop SMTP traffic to the Remote Analyzer by turning off the Email Security Service. Click C**ontrol Panel > Administrative Tools > Services > MlfASG Software > Stop**.

2 After a few minutes, check the last entry in the mfe log on the Remote Analyzer log.

3 Check the mfe log in the Control Center logs directory to ensure the last entry in the mfe log for the Remote Analyzer is there.

4 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.

Configuring Communications for Split Configurations

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

To configure a Remote Analyzer:

1 Log in to each device set up as a Remote Analyzer.

2 Scroll to the **Control Centers** section.

3 Click the **Add Path** button to identify which Control Center this Remote Analyzer can accept instructions from.

4 Enter the hostname of your **Control Center**.

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

Changing Configurations

Only two situations 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

This kind of change has implications for your configuration so reach out to SonicWall Customer Support for help in planning the proper steps. Refer to SonicWall Support for more information.

MTA Configuration

Navigate to the **System Setup | Network > MTA Configuration** screen to configure the Mail Transfer Agent (MTA) settings. You can specify how the MTA handles a case in which Email Security is unable to deliver a message right away.

ⓘ **NOTE:** Most installations do not require any change to the MTA settings.

Topics:

- Mail Transfer Agent Settings
- Rate Limit Settings
- Non-Delivery Reports (NDR)

Mail Transfer Agent Settings

On the MTA Configuration page, you can configure the retry and bounce intervals for the MTA. Messages are bounced if the recipient domain returns a permanent failure (5xxx error code). For transient failures (4xx error codes, indicating a delay), the MTA retries delivery of the message periodically based on the schedule specified.

To configure the Mail Transfer Agent Settings:

1. In the **Retry interval** field, set how frequently the MTA tries to resend the email message after failure.
2. In the **Bounce after** field, set when delayed messages are bounced if they cannot be delivered. When the **Bounce after** time elapses, no further attempts are made to deliver the delayed messages.
3. Choose to **Ignore 8-bit Mime** encoded content by selecting the **On** option button. Select **Off** if you don’t want to **Ignore 8-bit Mime** content.
4. Click **Save** when finished configuring the Mail Transfer Agent Settings.

Rate Limit Settings

The Rate Limiting Settings section is an advanced feature. The MTA automatically minimizes the number of connection it uses. If you are unsure of the impact any changes to these settings will have on your configuration, do not change them.

The default for rate limiting is **0**, which is the same as no limit, for all MX record domains. To limit the number of connections used, enter the new default number you want.

You can also limit the maximum number of simultaneous connections the MTA can open to a specific MX record domain.

ⓘ **NOTE:** The connection limits configured in this section only apply to connections opened by MTA, not connections opened by the SMTP proxy.

To add a specific domain:

1. Navigate to **System Setup | Network > MTA Configuration** on the **MANAGE** view.
2. Scroll to the **Rate Limiting Settings** section.
3. Set a **Default Limit for all MX record domains**. 0 is defined as no limit.
4. To add an override for specific MX record domains, click the **Add Domain** button.
5. Specify the **MX record domain** in the space provided.

6 Specify the **Limit**.

7 To have the subdomains adhere to the rate limit, check the box for **Include subdomains**.

8 Click **Save**.

Non-Delivery Reports (NDR)

When an email cannot be sent due to either a transient delay or a permanent failure, the sender may receive a notification email, or a Non-Delivery Report (NDR), describing the failure. Administrators can use this pane to customize the schedule and contents of the NDR. Permanent NDR may not be disabled, but sending NDR for transient failure is optional.

Topics:

- Transient Failure Settings
- Permanent Failure Settings
- General Settings

Transient Failure Settings

To enable Transient NDR, select the **Send NDR for transient failures** check box. Also specify:

- The **Notification interval** (in days, hours, and minutes)
- The **Email address from which NDR is sent** and **Name from which NDR is sent** (for example, “ericsmith@example.com” and “Eric Smith”)
- A **Subject line tag** for the NDR (for example, “Delay in sending your email”)
- A customized body for the NDR

Permanent Failure Settings

To define the parameters of an NDR for permanent failures, specify:

- The **Email address from which NDR is sent** and **Name from which NDR is sent** (for example, “ericsmith@example.com” and “Eric Smith”)
- A **Subject line tag** for the NDR (for example, “Your email could not be sent.”)
- A customized body for the NDR.

ⓘ **NOTE:** Permanent Failure Settings cannot be disabled.

General Settings

All NDRs include a diagnostic report about the problem that prevented delivery, including the headers of the original message. Permanent NDRs may optionally have the contents of the original message attached. To enable the option to **Attach original message** to the NDR, check the box.

When finished configuring this section, click **Save**.

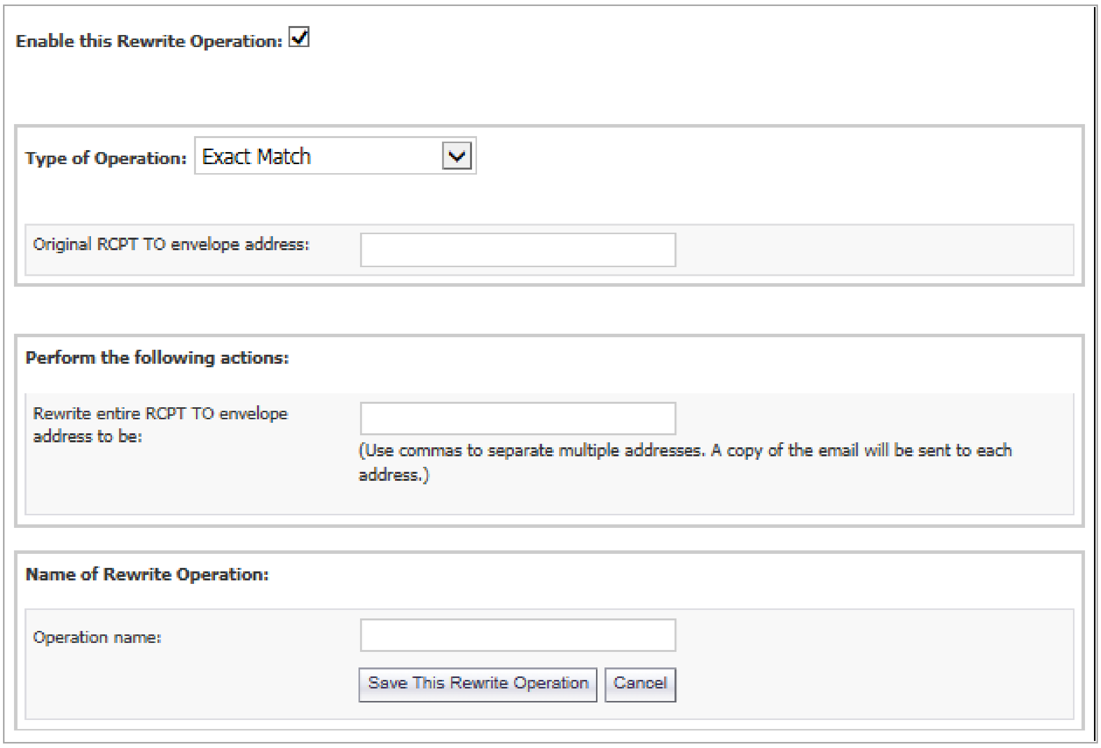
ⓘ **NOTE:** Some mail servers, such as Microsoft Exchange, may send their own NDRs or rewrite the contents of NDRs sent from other products. Please see the Microsoft Exchange administrator's guide for information on integrating this product's NDR functionality with Microsoft Exchange.

Email Address Rewriting

Use this window 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.

To enable the Email Address Rewrite Operations:

1. Navigate to **System Setup | Network > Email Address Rewriting** on the **MANAGE** view.
2. Select either **Inbound** (to rewrite the "To" field) or **Outbound** (to rewrite the "From" field).
3. Click on **Add New Rewrite Operation**.



Enable this Rewrite Operation: ☑

Type of Operation: Exact Match

Original RCPT TO envelope address:

Perform the following actions:

Rewrite entire RCPT TO envelope address to be:

(Use commas to separate multiple addresses. A copy of the email will be sent to each address.)

Name of Rewrite Operation:

Operation name:

4. Check the box for **Enable this Rewrite Operation**.
5. In the **Type of Operation** drop-down menu, select one of the possible options:
   - If **Exact Match** is selected, the operation is triggered by the exact email address (including the domain). The full email address is rewritten. For example, an email sent to billy@corp.example.com could be rewritten so that the address is mandy@example.net.
   - If **Starts With** is selected, the operation is triggered when the starting characters of the full email address (including the domain) match the characters specified. The entire email address including the domain is replaced. For example, if the operation is intended to be triggered by email addresses that start with billy@corp, an email sent to billy@corp.example.net could be rewritten so that the address was mandy@sales.example.com.
   - If **Ends With** is selected, the operation is triggered when the ending characters of the full email address (including the domain) match the characters specified. The entire email address including the domain is replaced. For example, if the operation is intended to be triggered by email addresses that end with .com, an email sent to billy@example.com could be rewritten so that the address was mandy@corp.example.net.
   - If **Domain** is selected, the operation is triggered by a particular email domain. The operation rewrites only the domain portion of the email address. For example, an email sent to

joe@corp.example.com could be rewritten so that the address is joe@example.net. If an asterisk, *, is entered, all domains are matched, and the rewrite operation will be triggered by any domain.

- If **LDAP Rewrite to Primary** is selected, the operation is applied to every inbound email. The operation rewrites the entire email address to be the primary mail attribute in LDAP. For example, an email sent to joe@corp.example.com could be rewritten so that the address is joe@example.com.
- If **LDAP Email List Expansion** is selected, the operation is triggered by the email list you select. Click the Select Email List button to choose an email list to expand. This operation replaces the email list in the envelope with a RCPT TO header for each member of the list. For example, an email sent to sysadmins@corp.example.com could be rewritten so that the addresses in the envelope are joe@example.com, sue@example.com, and malcom@example.com.

6 Enter the text that triggers the rewrite operation in the **Original RCPT TO envelope address** text field. For example, if you want to rewrite a domain from corp.example.com, enter corp.example.com in this section.

7 In the **Perform the following actions** section, enter the text that triggers the rewrite operation in the **Rewrite entire RCPT TO envelope address to be** field. For example, if you want to rewrite a domain from example.com to be example.net, enter example.net here.

8 In the section called **Name of Rewrite Operation**, enter a descriptive name for the operation you created.

9 Click on **Save This Rewrite Operation**. The new operation appears on the respective Inbound or Outbound tab.

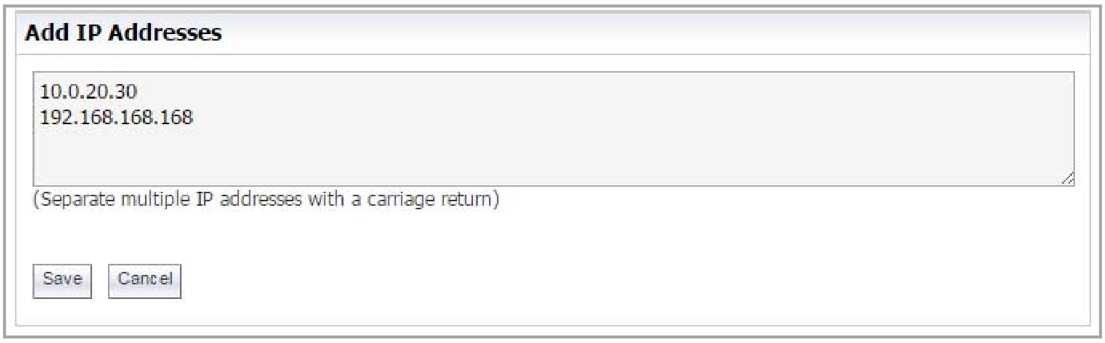
Trusted Networks

When the Email Security is not a “first-touch” server and receives email messages from an upstream server that uses a non-reserved or public IP address, the GRID Network effectiveness may degrade. To avoid this degradation on the GRID Network, users can put public IP addresses on a privatized list to make the address look like it’s part of a trusted network.

To add IP addresses to a Trusted Network:

1 Navigate to **System Setup | Network > Trusted Networks** on the **MANAGE** view.

2 Click the **Add Server** button.


Add IP Addresses

10.0.20.30
192.168.168.168

(Separate multiple IP addresses with a carriage return)

3 Type in the IP addresses you want added. If you want to add multiple IP addresses, put each IP address on a separate line, followed by a carriage return.

4 Click **Save**. The IP addresses appear on the Server List.

Junk Box

You can use the **System Setup | Junk Box** options to define the parameters for junk message management and for Junk Box Summary notification.

Message Management

On the **Set Setup | Junk Box > Message Management** page, you define General Settings, Action Settings, and Miscellaneous setting for managing junk messages.

General Settings

In **General Settings** section, you choose options for saving messages in the junk box and for unjunking messages.

To define General Settings:

1. Choose the **Number of days to store in Junk Box before deleting** from the drop-down list.

   This sets the enterprise-wide policy for how long email messages remain in the Junk Box before being automatically deleted. The options range from 1 day to 180 days. This can be adjusted for an individual user by an administrator or the user, if you allow it. (Refer to User View Setup.)

2. Select one of the following options for **When a user unjunks a message**:
   - Automatically add the sender to the recipient's Allowed List
   - Ask the user before adding the sender to the recipient's Allowed List
   - Do not add the sender to the recipient's Allowed List

3. Scroll to the bottom of the page and select **Apply Changes** if done or select **Reset to Defaults** if you want to return to prior settings.

Action Settings

In the **Action Settings** section, you define how unjunked messages are tagged and delivered to users' inboxes. Review each of the four options, check the box to enable that option and type in the text you want added to the subject line. The table below provide more information on the options.

Unjunked Tagging Option	Notes
Tag unjunked messages with this text added to the subject line	Example of words to be added to the subject line: `[Junk released by User Action]`.
Tag messages considered junk, but delivered because sender/domain/list is in Allowed List with this text added to the subject line	Example of words to be added to the subject line: `[Junk released by Allowed List]`.
Tag messages considered junk, but delivered because of a Policy action with this text added to the subject line:	Example of words to be added to the subject line: `[Junk released by Policy Action]`.
Tag all messaged processed by Email Security for initial deployment testing with this text added to the subject line:	Example of words to be added to the subject line: `[SonicWall` Email Security`]`.

Miscellaneous

The **Miscellaneous** section provide links that take you to message management features for the Anti-Spam, Anti-Phishing, Anti-Virus, and Policies modules.

Miscellaneous Message Management Options	Where link goes
To set spam message management	**Security Services | Anti-Spam > Spam Management**
To set phishing message management	**Security Services | Anti-Phishing**
To set virus message management	**Security Services | Anti-Virus** (both **Inbound** and **Outbound** options)
To set policies for your organization	**Security Services | Policy & Compliance > Filters** (both **Inbound** and **Outbound** options)

Summary Notifications

On the **Set Setup | Junk Box > Summary Notifications** page, you define Frequency Settings, Message Settings, Miscellaneous Settings, and Other Settings for the Junk Box Summary that is sent to users and administrators. The Junk Box summaries list the incoming email that Email Security has quarantined. From these summaries, users can choose to view or unjunk an email if the administrator has configured these permissions. From the **Summary Notifications** page, users can determine the language, frequency, content, and format of Junk Box summaries.

Frequency Settings

To define the frequency settings of the Junk Box Summary:

1. Select the **Frequency of summaries** from the drop-down list. Options range from **Never** to **14 Days**.
2. Select the **Time of day to send summary**. You can select **Any time of day** or specify an hour to send by selecting **Within an hour of** and choosing the hour from the drop down menu.
3. Select the **Day of week to send summary**. You can select **Any day of the week** or select **Send summary on** and specify a day.
4. Specify the **Time Zone** for the Email Security system.
5. Scroll to the bottom of the page and select **Apply Changes** if done.

Message Settings

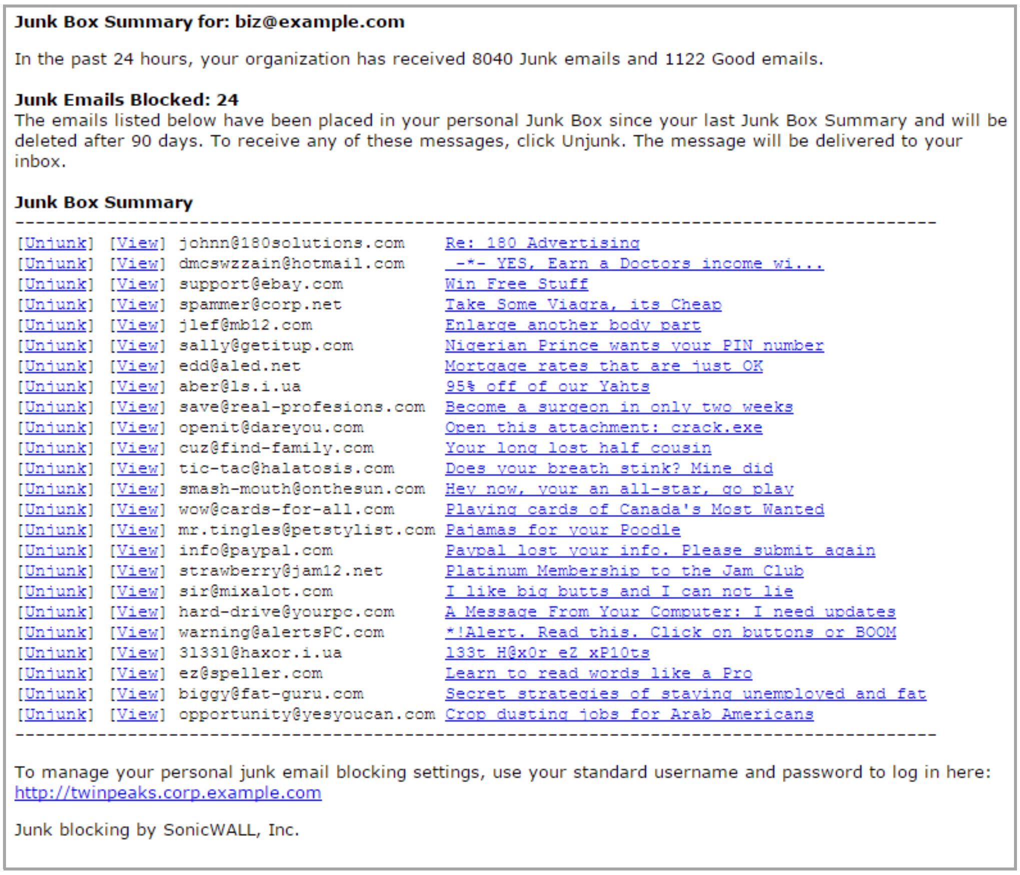
To define the Message Settings for the Junk Box Summary:

1. In **Summaries include** section, chose **All Junk Messages** or **Only likely junk (hide definite junk)** in Junk Box Summaries.

   ⓘ **NOTE:** If **All Junk Messages** is selected, both definite and likely junk messages are included. If **Only likely junk** is selected, only likely junk messages are included in the summary.

2. Select the **Language of summary email** from the drop down list.
3. Check the box to enable **Plain summary** if you want to send junk box summaries without graphics.

The following image shows a Plain Summary:



Junk Box Summary for: biz@example.com

In the past 24 hours, your organization has received 8040 Junk emails and 1122 Good emails.

Junk Emails Blocked: 24
The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days. To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

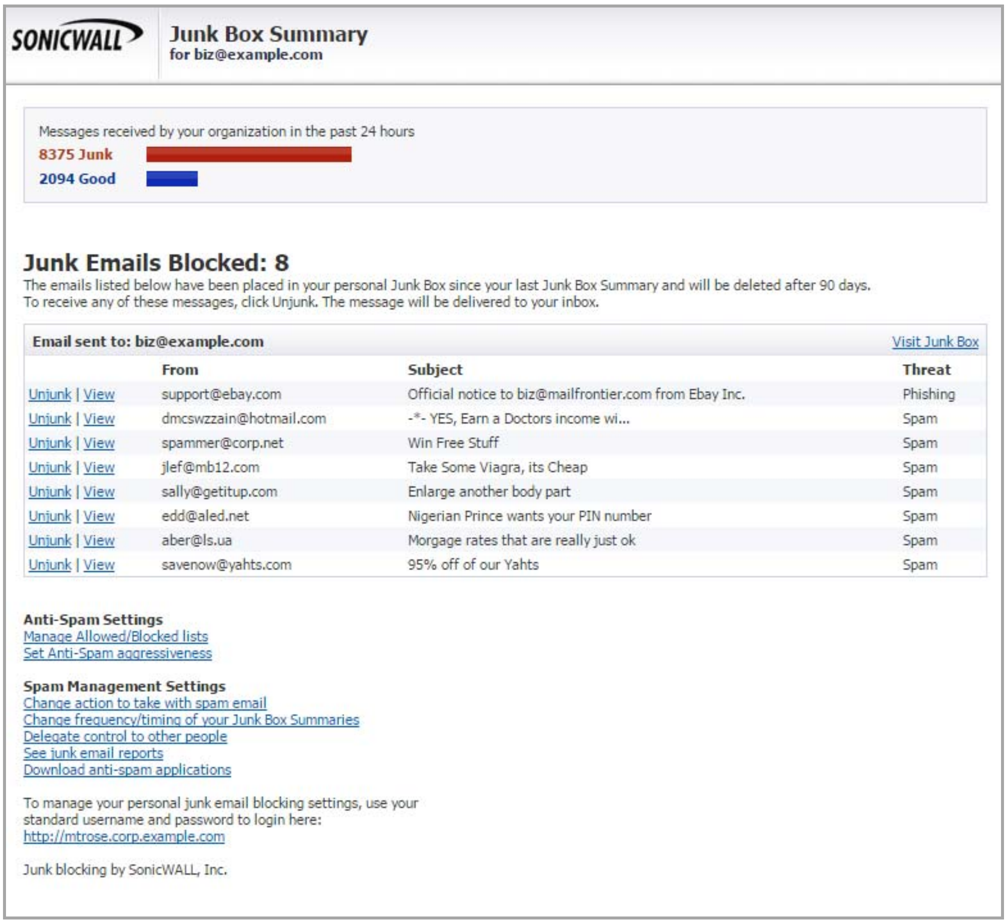
Junk Box Summary

```
------------------------------------------------------------------------------------------
[Unjunk] [View] johnn@180solutions.com    Re: 180 Advertising
[Unjunk] [View] dmcswzzain@hotmail.com     -*- YES, Earn a Doctors income wi...
[Unjunk] [View] support@ebay.com          Win Free Stuff
[Unjunk] [View] spammer@corp.net          Take Some Viagra, its Cheap
[Unjunk] [View] jlef@mb12.com             Enlarge another body part
[Unjunk] [View] sally@getitup.com         Nigerian Prince wants your PIN number
[Unjunk] [View] edd@aled.net              Mortgage rates that are just OK
[Unjunk] [View] aber@ls.i.ua              95% off of our Yahts
[Unjunk] [View] save@real-profesions.com  Become a surgeon in only two weeks
[Unjunk] [View] openit@dareyou.com        Open this attachment: crack.exe
[Unjunk] [View] cuz@find-family.com       Your long lost half cousin
[Unjunk] [View] tic-tac@halatosis.com     Does your breath stink? Mine did
[Unjunk] [View] smash-mouth@onthesun.com  Hey now, your an all-star, go play
[Unjunk] [View] wow@cards-for-all.com     Playing cards of Canada's Most Wanted
[Unjunk] [View] mr.tingles@petstylist.com Pajamas for your Poodle
[Unjunk] [View] info@paypal.com           Paypal lost your info. Please submit again
[Unjunk] [View] strawberry@jam12.net      Platinum Membership to the Jam Club
[Unjunk] [View] sir@mixalot.com           I like big butts and I can not lie
[Unjunk] [View] hard-drive@yourpc.com     A Message From Your Computer: I need updates
[Unjunk] [View] warning@alertsPC.com      *!Alert. Read this. Click on buttons or BOOM
[Unjunk] [View] 31331@haxor.i.ua          133t H@x0r eZ xP10ts
[Unjunk] [View] ez@speller.com            Learn to read words like a Pro
[Unjunk] [View] biggy@fat-guru.com        Secret strategies of staying unemployed and fat
[Unjunk] [View] opportunity@yesyoucan.com Crop dusting jobs for Arab Americans
------------------------------------------------------------------------------------------
```

To manage your personal junk email blocking settings, use your standard username and password to log in here:
http://twinpeaks.corp.example.com

Junk blocking by SonicWALL, Inc.

The following image shows a Graphic Summary:



Junk Box Summary
for biz@example.com

Messages received by your organization in the past 24 hours
8375 Junk
2094 Good

Junk Emails Blocked: 8

The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days.
To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

Email sent to: biz@example.com — Visit Junk Box

	From	Subject	Threat
Unjunk | View	support@ebay.com	Official notice to biz@mailfrontier.com from Ebay Inc.	Phishing
Unjunk | View	dmcswzzain@hotmail.com	-*- YES, Earn a Doctors income wi...	Spam
Unjunk | View	spammer@corp.net	Win Free Stuff	Spam
Unjunk | View	jlef@mb12.com	Take Some Viagra, its Cheap	Spam
Unjunk | View	sally@getitup.com	Enlarge another body part	Spam
Unjunk | View	edd@aled.net	Nigerian Prince wants your PIN number	Spam
Unjunk | View	aber@ls.ua	Morgage rates that are really just ok	Spam
Unjunk | View	savenow@yahts.com	95% off of our Yahts	Spam

Anti-Spam Settings
Manage Allowed/Blocked lists
Set Anti-Spam aggressiveness

Spam Management Settings
Change action to take with spam email
Change frequency/timing of your Junk Box Summaries
Delegate control to other people
See junk email reports
Download anti-spam applications

To manage your personal junk email blocking settings, use your standard username and password to login here:
http://mtrose.corp.example.com

Junk blocking by SonicWALL, Inc.

4 Check the box to **Display junk statistics in summary email.** This includes junk statistics in the Junk Box Summary.

5 Scroll to the bottom of the page and select **Apply Changes** if done.

Miscellaneous Settings

To define the Miscellaneous Settings for the Junk Box Summary:

1 Check the box to enable **Send Junk Box Summary to delegates**. This send summary emails sent directly to a user’s delegates. Users with delegates no longer receive summary emails.

2 Select one of the options for **Enable “single click” viewing of messages**. You can select from the following:

- Off—The “single click” viewing of messages setting is not enabled.
- View messages only—Users are able to preview messages without having to type their name or password.
- Full Access—Users can click any link in a Junk Box Summary and are granted full access to the particular user’s settings.

3 Check the box to **Enable Authentication to Unjunk** if you want to require authentication for unjunking messages in the Junk Box Summary.

4. Check the box **Only send Junk Box Summary emails to users in LDAP** to only include LDAP users as recipients of the Junk Box Summary emails. With this setting selected, users not associated with the LDAP do not receive Junk Box Summary emails.
5. To enable authentication for non-LDAP users, click the link. You are automatically directed to the **System Setup | Users, Groups & Organizations > Users** page. For more information regarding LDAP and non-LDAP users, refer to Users.
6. Scroll to the bottom of the page and select **Apply Changes** if done.

Other Settings

To define the Other Settings for the Junk Box Summary:

1. Choose **Email address from which summary is sent**. Select one of the following:
   - **Send summary from recipient's own email address**
   - **Send summary from this email address** and specify the email address in the space provided.
2. Specify the **Name from which summary is sent** in the field provided.
3. Specify the **Email subject** in the space provided.
4. Specify the **URL for user view** in the space provided. The Junk Box Summary includes this URL so users can easily view quarantined emails, unjunk quarantined emails, and to log in to the Email Security system.
5. Click the **Test Connectivity** button to verify the URL specified in the URL for User View field properly connects.
6. Select **Apply Changes** if done. Select **Revert** if you want to fall back to the previously save definitions.

13

Anti-Spam

Email Security 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. This chapter reviews the configuration information for Anti-Spam:

- Spam Management
- Address Books
- Anti-Spam Aggressiveness
- Languages
- Black List Services
- Spam Submissions

Administrators 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 Management

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 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 have a higher priority than a user’s.

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, Email Security analyzes the messages’ headers and contents and uses collaborative thumb-printing to block email that contains junk.

Use **Security Services | Anti-Spam > Spam Management** to select options for dealing with Definite Spam and Likely Spam. The default setting for Definite Spam and Likely Spam is to quarantine the message in the user’s Junk Box.

To manage messages marked as definite spam or likely spam:

1 Choose one of the following responses for messages marked as **Definite Spam** and **Likely Spam**:

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user's mailbox was unavailable (for example, not found or rejected for policy reasons).
Store in Junk Box (recommended for most configurations)	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	Forward the email message for review to the specified email address. For example, you could Send to `postmaster`."
Tag With	The email is tagged with a term in the subject line, for example `[SPAM]`. Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Add X-Header	This option adds an X-Header to the email with the key and value specified to the email message. The first text field defines the X-Header. The second text field is the value of the X-Header. For example, a header of type X-`EMSJudgedThisEmail` with value `DefiniteSpam` results in the email header as: `X-EMSJudgedThisEmail:DefiniteSpam`.

2 Select the **Accept Automated Allowed List** check box to allow automated lists that are created by User Profiles to prevent spam.

With this feature enabled, User Profiles analyze the recipients of emails from members of your organization and automatically added them to Allowed Lists. This helps reduce the false positives, which are good email messages judged as junk. This feature can be configured globally, for particular groups, or for specific users. SonicWall recommends enabling this feature.

ⓘ **NOTE:** If this check box is unchecked in the Corporate, Group, or User windows, User Profiles have no effect.

3 Select the **Skip spam analysis for internal email** check box to exclude internal emails from spam analysis, resulting in a reduced amount of false positives. If you are routing internal mail through the Email Security product, SonicWall recommends that you enable this feature.

4 Select the **Allow users to delete junk email** check box to allow users to control the delete button on individual junk boxes.

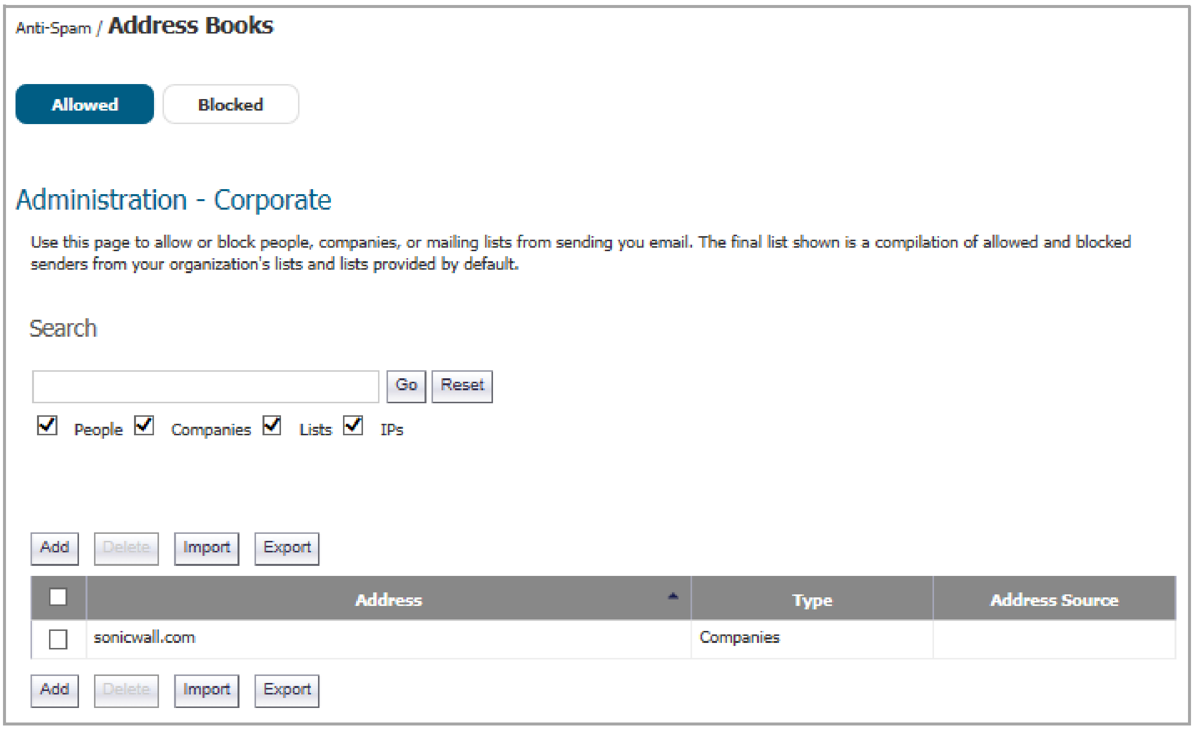
ⓘ **NOTE:** Leave this check box not selected if you have an extended away/out of the office message turned on so that your auto-reply does not automatically place all recipients on your Allowed list.

5 Click **Apply Changes** to save; selecting **Revert** allows you to fall back to the prior settings.

Address Books

From **Security Services | Anti-Spam > Address Books** you can create an address book of people, companies, mailing list or IP addresses who are allowed to or are blocked from sending email to you. Select the **Allowed** or **Blocked** button to view the respective type of address.

If you attempt to add your own email address or your organization's domain, SonicWall Email Security displays a warning. A user's email address is not automatically added to the allowed list because spammers sometimes use a recipient's own email address. Leaving the address off the allowed list does not prevent users from emailing themselves, but their emails are evaluated to determine if they are junk.



Anti-Spam / Address Books

Allowed | Blocked

Administration - Corporate

Use this page to allow or block people, companies, or mailing lists from sending you email. The final list shown is a compilation of allowed and blocked senders from your organization's lists and lists provided by default.

Search

Go | Reset

☑ People ☑ Companies ☑ Lists ☑ IPs

Add | Delete | Import | Export

□	Address	Type	Address Source
□	sonicwall.com	Companies	

Add | Delete | Import | Export

Using the Search Field

To search for an address:

1 Enter all or part of the email address in the Search field. For example, entering sale displays `sales@domain.com` as well as `forsale@domain.com`.

2 Narrow your search by selecting the **People**, **Companies**, **Lists**, or **IPs** check box(es) below the Search field.

3 Click **Go** to perform the search.

Adding People, Companies, Lists, or IPs

To add people, companies, lists, or IPs to the Allowed or Blocked lists:

1. From the **Security Services | Anti-Spam > Address Books** page, click the **Allowed** or **Blocked** tab.
2. Click the **Add** button.
3. Select the list type (**People**, **Companies**, **Lists**, **IPs**) from the drop-down menu.
4. Enter one or more address, separated by carriage returns.
5. Select **Add** to complete.

When adding addresses, consider the following:

- 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.
- Email Security warns you if you attempt to add your own email address or your own organization.
- Email addresses are not case-sensitive; Email Security converts the address to lowercase.
- 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; 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.
- Email Security does not support adding top-level domain names such as .gov or .abc to the Allowed and Blocked lists.
- Mailing list email messages are handled differently than individuals and domains because Email Security looks at the recipient's address rather than the sender's. Because many mailing list messages appear spam-like, entering mailing list addresses prevents mis-classified messages.

Deleting People, Companies, Lists, or IPs

To delete people, companies, lists, or IPs from your Address Books:

1. From the **Security Services | Anti-Spam > Address Books** page, click the **Allowed** or **Blocked** tab.
2. Select the check box next to the address or addresses you want to delete.
3. Click the **Delete** button.

Importing and Exporting the Address Book

You can import an address book of multiple addresses to create our Allowed or Blocked lists. Note that users and secondary domains should be added prior to importing their respective address books.

The Address Book file for import must follow specific formatting to ensure successful importing:

- <TAB> delimiter between data
- <CR> to separate entries

Each address book entry must include each of the following:

- **Identifier**—Specified as <email address / primary domain>
- **Domain / List / Email**—Specified as D / L / E

- **Allowed / Blocked**—Specified as A / B
- **Address List**—Specified as abc@domain.com, example.com

For example:

```
EmailID<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
Domain<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
```

To import an Address Book:

1. From the **Security Services | Anti-Spam > Address Books** page, click the **Import** button on either the **Allowed** or **Blocked** tabs.
2. Click the **Browse...** button.
3. Select the correct file from your system.
4. Click the **Import** button.

To export the Address Book:

1. Select the **Export** button.
2. Save the file to your local system.

Anti-Spam Aggressiveness

The **Security Services | Anti-Spam > Anti-Spam Aggressiveness** page allows you to tailor the SonicWall Email Security product to your organization's preferences. Configuring this window is optional.

SonicWall Email Security recommends using the default setting of Medium unless you require different settings for specific types of spam blocking. Be sure to select **Apply Changes** to save the settings or select **Reset to Defaults** to go back to the prior settings.

Topics:

- Configuring Grid Network Aggressiveness
- Configuring Adversarial Bayesian Aggressiveness
- Unjunking spam
- Category settings

Configuring Grid Network Aggressiveness

The GRID Network Aggressiveness technique determines the degree to which you want to use the collaborative database. Email Security maintains a database of junk mail identified by the entire user community. You can customize the level of community input on your corporate spam blocking. Selecting a stronger setting makes Email Security more likely more responsive to other users who mark a message as spam.

Use the following settings to specify how stringently Email Security evaluates messages:

- If you choose **Mildest**, you will receive a large amount of questionable email in your mailbox. This is the lightest level of Anti-Spam Aggressiveness.

- If you choose **Mild**, 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 through unwanted email from your personal mailbox.
- If you choose **Medium**, you accept Email Security's spam-blocking evaluation.
- If you choose **Strong**, 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.
- If you choose **Strongest**, Email Security heavily filters out spam. This creates an even higher probability of good email messages in your Junk Box.

Configuring Adversarial Bayesian Aggressiveness

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 the following settings to specify how stringently SonicWall Email Security evaluates messages:

- If you choose **Mildest**, you will receive a large amount of questionable email in your mailbox. This is the lightest level of Anti-Spam Aggressiveness.
- If you choose **Mild**, 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 through unwanted email from your personal mailbox.
- If you choose **Medium**, you accept Email Security's spam-blocking evaluation.
- If you choose **Strong**, 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.
- If you choose **Strongest**, Email Security heavily filters out spam. This creates an even higher probability of good email messages in your Junk Box.

Unjunking spam

Select the **Allow users to unjunk spam** check box if you want to enable users to unjunk spam messages. If left unchecked, users cannot unjunk spam messages.

Category settings

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

For each type of spam:

- Choose **Mildest** to be able to view most of the emails that contain terms that relate to these topics.
- Choose **Mild** to be able to view email that contains terms that relate to these topics.
- Choose **Medium** to cause Email Security to tag this email as likely junk.
- Choose **Strong** to make it more likely that email with this content is junked.
- Choose **Strongest** to make it certain that email with this content is junked.

For example, if you don’t want to receive any email with sexual content, select **Strong**. If you are less concerned about receiving other categories, select Mild.

You can also select the **Allow Unjunk** check box to allow users to unjunk specific types of spam.

Languages

From the **Security Service | Anti-Spam > Languages** page, you can **Allow All**, **Block All**, or enter **No Opinion** on email messages in various languages. If you select **No opinion**, Email Security judges the content of the email message based on the modules that are installed. After configuring Language settings, click the **Apply Changes** button.

> **NOTE:** Some spam email messages are seen in English with a background encoded in different character sets such as Cyrillic, Baltic, or Turkish. This is done by spammers to bypass the anti-spam mechanism that only scans for words in English. In general, unless used, it is recommended to exclude these character sets. Common languages such as Spanish and German are normally not blocked.

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. Email Security can be configured from the **Security Services | Anti-Spam > Black List Services** page to query these lists and identify spam originating from any of their known spam addresses.

> **NOTE:** SonicWall Email Security performance may vary if you add Black List Services because each email is placed on hold while the BLS service is queried.

Adding to the Black List

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 added.

Email from Sources on the Black Lists Services

Select 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.

> **IMPORTANT:** By enabling this option, you can increase the risk of false positives, and you may not receive some legitimate email.

Spam Submissions

The **Security Services | Anti-Spam > Spam Submissions** page allows you 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 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.

Topics:

- Managing Spam Submissions
- Probe Accounts
- Managing Mis-Categorized Messages
- Managing Mis-Categorized Messages
- Forwarding Mis-Categorized Email
- Configuring Submit-Junk and Submit-Good email accounts

Managing Spam Submissions

To manage spam submissions:

1 Navigate to **Security Services | Anti-Spam > Spam Submissions** on the **MANAGE** view.

2 Enter an **Email address for Submitting Missed Spam** in the text field. 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** in the text field. 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 Email Security. For example, you might create a probe email account with the address `mailto:probeaccount1@your_domain.com`.

> ⓘ **IMPORTANT:** 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 never receives another email - good or junk - again, because all email sent to that address is redirected to the SonicWall corporation's data center.

5 Click the **Apply Changes** button.

Probe Accounts

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

Configure the Probe Email Account fields to allow any email sent to your organization to create fictitious email accounts from which mail is sent directly to SonicWall for analysis. Adding this junk email to the set of junk email messages that Email Security blocks enhances spam protection for your organization and other users. If you configure probe accounts, the contents of the email will be sent to SonicWall for analysis.

Managing Mis-Categorized Messages

When an email message is mis-categorized, the following actions are taken:

- For false negatives, Email Security 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, Email Security 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.) If the sender email is the user's own email address, the address is not added to the allowed list, because spammers send email pretending to be from the user. Email sent to and from the same address will always be evaluated to determine if it is junk.

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 Mis-Categorized Email

You must set up your email system so that email messages sent to the this_is_spam@es.your_domain.com and not_spam@es.your_domain.com pass through Email Security. The email addressed to these accounts must pass through the Email Security system so that it can be analyzed. Using a domain that does not route, such as "fixit.please.com", is recommended.

A problem can arise if the user sends an email to this_is_spam@es.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 the Email Security system. The most common solution is included below as an example.

To forward the missed email to Email Security for analysis:

1 Add the this_is_spam and not_spam email addresses as `this_is_spam@es.your_domain.com` and `not_spam@es.your_domain.com` into the Email Security Junk Submission text field.

2 Create an A and an MX record in your internal DNS that resolves `es.your_domain.com` to your Email Security server's IP address.

3 Tell users to forward mail to `this_is_spam@ES.your_domain.com` or `not_spam@ES.your_domain.com`.The mail goes directly to the Email Security servers.

Configuring Submit-Junk and Submit-Good email accounts

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

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

Users must forward their mis-categorized email directly to these addresses after you define them so that the Email Security system can learn about mis-categorized messages.

14

Anti-Spoofing

SonicWall Email Security solution allows you to enable and configure settings to prevent illegitimate messages from entering your organization. Spoofing consists of an attacker forging the source IP address of a message, making it seem like the message came from a trusted host. By configuring SPF, DKIM, and DMARC settings, your Email Security solution runs the proper validation and enforcement methods on all incoming messages to your organization. This chapter provides configuration information specific to Anti-Spoofing, including:

- Inbound SPF Settings
- Inbound DKIM Settings
- Inbound DMARC Settings
- Inbound DMARC Report Settings
- Outbound DKIM Settings

The Anti-Spoofing feature works in an order of precedence, where features at the top of the page are of a lower priority than features towards the bottom of the page. Generally, a message is subjected to SPF, DKIM, and DMARC if all are enabled. The results from DKIM validation will take precedence over the results from SPF validation, and DMARC validation results will take precedence over DKIM validation results.

Inbound SPF Settings

The **Security Services | Anti-Spoofing > Inbound** tab features SPF (Sender Policy Framework) validation for inbound email messages. SPF is an email validation system designed to prevent email spam by verifying that sender IP addresses are valid. SPF records, which are published in the DNS records, contain descriptions of the attributes of valid IP addresses. SPF is then able to validate against these records if a mail message is sent from an authorized source. If a message does not originate from an authorized source, the message fails. You can configure the actions against messages that fail.

Two types of SPF failures include:

- **SPF HardFail**—The SPF has determined that the host is *not* allowed to send messages and does not allow those messages through to the recipient.
- **SPF SoftFail**—When a SPF soft fail occurs (the system determines that the sending host is probably not authorized to send messages), mail messages from senders in the Allow list are not sent through to the recipient. This feature is enabled by default.

To enable SPF:

1 To **Enable SPF validation for incoming messages**, check the box.

2 For hard failures, configure the action to take:

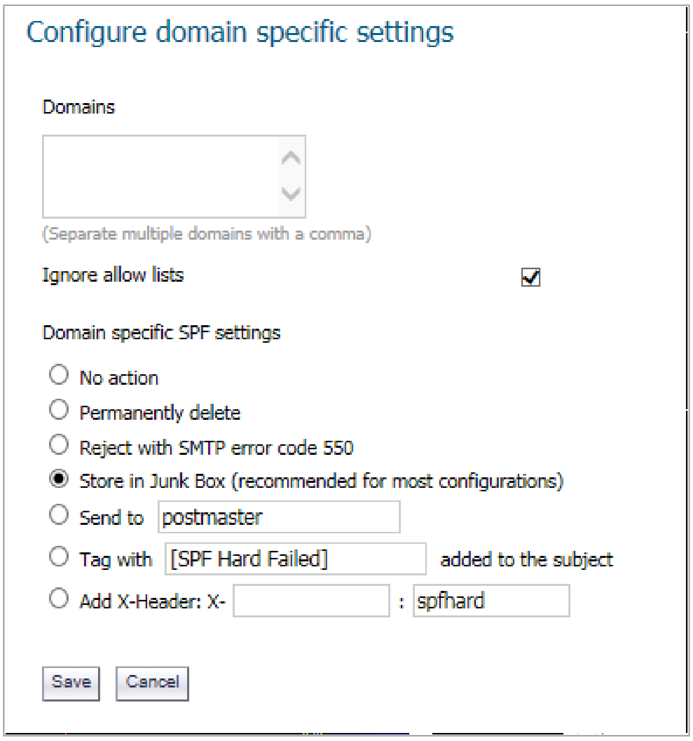
   a Decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

   b Select an action to take for messages marked as **SPF hard fail**. Actions to Take for Hard Failures describes the options.

Actions to Take for Hard Failures

No Action	No action is taken against messages marked as SPF hard fail.
Permanently delete	Messages marked as SPF hard fail are permanently deleted.
Reject with SMTP error code 550	Messages marked as SPF hard fail are rejected with an SMTP error code 550.
Store in Junk Box (recommended for most configurations)	Messages marked as SPF hard fail are stored in the Junk Box. This is the recommended setting for most configurations.
Send to [field]	Messages marked as SPF hard fail are sent to the user specified in the available field. For example, you can send to `postmaster`.
Tag with [field] added to the subject	Messages marked as SPF hard fail are tagged with a term in the subject line. For example, you may tag the messages `[SPF Hard Failed]`.
Add X-Header: X-[field]:[field]	Messages marked as SPF hard failed add an X-Header to the email with the key and value specified to the email message. The first text field defines the X-Header. The second text field is the value of the X-Header. For example, a header of type `X-EMSJudgedThisEmail` with value `spfhard` results in the email header as: `X-EMSJudgedThisEmail:spfhard`.

   c Click **Add Domain** if you want to define specific actions for an identified domain.



Configure domain specific settings

Domains

(Separate multiple domains with a comma)

Ignore allow lists ☑

Domain specific SPF settings

○ No action
○ Permanently delete
○ Reject with SMTP error code 550
● Store in Junk Box (recommended for most configurations)
○ Send to postmaster
○ Tag with [SPF Hard Failed] added to the subject
○ Add X-Header: X- : spfhard

d List the domains in the **Domains** field. Separate domains with a comma.

e Select one of the actions for a hard failure. Refer to Step b above for definitions of the options.

f Click **Save**.

3 For soft failures, decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

4 Click on **Apply Changes**.

Inbound DKIM Settings

DKIM (Domain Keys Identified Mail) uses a secure digital signature to verify that the sender of a message is who it claims to be and that the contents of the message have not been altered in transit. A valid DKIM signature is a strong indicator of a message's authenticity, while an invalid DKIM signature is a strong indicator that the sender is attempting to fake his identity. For some commonly phished domains, the absence of a DKIM signature can also be a strong indicator that the message is fraudulent. Users benefit from DKIM because it verifies legitimate messages and prevents against phishing. Remember that DKIM does not prevent spam - proper measures should still be taken against fraudulent content.

To configure DKIM signature settings:

1 Navigate to **Security Services | Anti-Spoofing > Inbound** on the **MANAGE** view, and scroll down to the section labeled **DKIM Settings**.

2 To enable DKIM, select the **Enable DKIM validation for incoming messages** check box.

3 Decide if you want to **Ignore allow lists** when a failure occurs. A check ignores the allowed lists and unchecked uses the lists.

4 Choose the action to take for messages marked as **DKIM signature failed**. The options are the same as those listed in Actions to Take for Hard Failures. In the **Tag with** field, you can use text to indicate a DKIM failure.

5 Click **Add Domain** if you want to define specific actions for an identified domain.

   a List the domains in the **Domains** field. Separate domains with a comma.

   b Select one of the actions for a hard failure. Refer to Actions to Take for Hard Failures above for the options.

   c Decide if **Domain** is **required to have DKIM signature**. A check requires the signature and unchecked doesn’t require it.

   d Click **Save** to configure domain specific settings.

6 Click on **Apply Changes** to save the DKIM definitions.

Inbound DMARC Settings

DMARC (Domain-based Message Authentication, Reporting & Conformance) is a policy that works in tandem with SPF and DKIM to fully authenticate incoming and outgoing email messages. A DMARC policy allows a sender to indicate that his emails are protected by SPF and/or DKIM, and also tells a receiver what to do if neither of those authentication methods passes, such as junk or reject the message.

To configure DMARC settings:

1 Navigate to **Security Service | Anti-Spoofing > Inbound** on the **MANAGE** view, and scroll down to the section labeled **DMARC Settings**.

2 Select the **Enable DMARC judgment for incoming messages** check box.

   NOTE: To use DMARC, you must also enable DKIM and SPF.

3 Select the **Enable DMARC Policy Enforcement for incoming messages** check box.

4 In the field provided, **Exclude these sender domains**, enter any sender domains (for example, sonicwall.com or gmail.com) you want excluded from DMARC policy enforcement. Multiple domains can be entered and should be separated by a comma.

5 Choose whether to **Enable DMARC Outgoing Reports.**

   Once DMARC is enabled, outgoing reports are automatically sent. You can configure an **Outbound Path for RUA delivery** of the reports by clicking the provided link (**System Setup | Network > Server Configuration**).

6 If you want to override reporting attributes for a specific domain, select **Add Domain**:

   a Enter the domain name to send DMARC reports to. You have the option of using ‘*’ as a value for the domain field. Consider the following:

      - A configuration created with the domain name * is considered the default domain.
      - If the domain is not provided, DMARC uses configuration settings from the * domain.
      - If no * domain is added, then a hard-coded default value, such as postmaster@domain, is used as the Sender ID.

   b Enter the email address from which the report originates in the field called **Report From: address**.

   c Optionally add any **Notes** regarding this domain.

      NOTE: The RUA is the aggregated report for domains with published domain records. Reports are sent daily.

   d Select **Save**

7 Click on **Apply Changes** to save the DMARC definitions.

Inbound DMARC Report Settings

You can configure DMARC incoming report settings by clicking the **Add Domain** button in the **DMARC Reports Settings** section. DMARC Incoming Reports are collected and processed only for the domains added.

To set up the DMARC reports:

1 Navigate to **Security Service | Anti-Spoofing > Inbound** on the **MANAGE** view, and scroll down to the section labeled **DMARC Report Settings**.

2 Select **Add Domain**.

3 Enter the **Domain** name for DMARC incoming reports.

4 Check the box to override reports being sent to the RUA email address specified in the DNS record. An example from the DNS record is `rua=mailto:aggrep@yourcompany.com`.

5 **I**f you selected the **Override DNS RUA Email Address**, specify the **RUA Email Address** to which the reports should be sent. Multiple addresses can be entered and should be separated by a comma.

> ⓘ **NOTE:** The RUA is the aggregated report for domains with published domain records. Reports are sent daily.

6 Click **Save** to save the report definition.

7 Select **Apply Changes** to update the report settings.

ⓘ **NOTE:** You can select the **Refresh** button to refresh the data in report domains table.

Outbound DKIM Settings

Set up the DKIM signature options for the outbound mail.

To set up DKIM settings on the outbound path:

1 Navigate to **Security Service | Anti-Spoofing > Outbound** on the **MANAGE** view.

2 Click the **Add Configuration** button. The DKIM Outbound Configuration page displays:

3 To define the **Settings for DKIM Signature**, complete the fields as described below:

Domain	Enter the **Domain** name.
Identity of Signer	Enter an **Identity of Signer**. Select the **Same as domain** check box to use the specified Domain name as the Identity of Signer.
Selector	Enter a value for the **Selector**. The selector is used to differentiate between multiple DKIM DNS records within the same organization (for example, `feb2014.domainkey.yourorganization.com`.
List of Header fields for Signing	Check the **Sign all standard headers** box to include all headers, or specify the headers in the designated field. Separate multiple headers with a colon (for example, `from:to:subject`).

4 To set up the Public Private key pair for SKIM Signing, complete the fields as described below:

Generate Key Pair	If you want to generate key pair for the DKIM signing, select **Generate key pair**. Specify the Key Size from the values in the drop down list, then click the Generate Key Pair button.
Key Size	Specify the **Key Size** from the values in the drop down list, then select the **Generate Key Pair** button.
Import existing public-private key pair	Choose Import existing public-private key pair, if you want to use an existing pair. Click on **Browse...** to **Upload Public key** and click on **Browse...** to **Upload Private key**. Type in the **Passphrase for private key.** Use only alphanumeric characters.

5 Click the **Save** button to finish. The signature is added to the DKIM Signature Configurations list.

Generating DNS Record

Once a domain has been successfully added to the DKIM Signature Configurations table, you can generate a DNS Record.

To generate a DNS record:

1 Under the DNS Record column for the domain you want to generate a record for, click the **Generate** button.

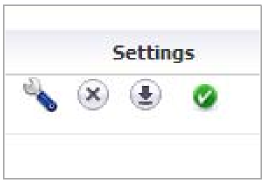
2 Set the following options on the Generate DNS Record page:

- **Domain**—This field auto-populates with the Domain you entered when adding a new configuration. This field cannot be edited.
- **Selector**—This field auto-populates with the Selector you entered when adding a new configuration. This field cannot be edited.
- **Public Key**—This field populates with the Public Key for your DNS record. You can copy and paste from this field.
- **Domain is testing DKIM**—Select the check box to enable testing DKIM for this domain.
- **Subdomains required to have their own DKIM keys**—Select the check box to enable the requirement for all subdomains to have their own DKIM keys.

3 Click the **Generate DNS Record** button to save the settings and generate your DNS record.

Managing Outbound DKIM Settings

The Settings column of each domain listed in the DKIM Signature Configurations table has the following icons:



- **Edit**—Click this icon to edit the DKIM Signature settings. Note that not all fields are editable.
- **Delete**—Click this icon to delete the DKIM Signature.
- **Download**—Click this icon to download the Public Key for this DKIM Signature.
- **Status**—The status icon notifies you if the DKIM Signature is enabled (green icon) or disabled (gray icon).

15

Anti-Phishing and Anti-Virus

The Anti-Phishing page and Anti-Virus features protect your organization from email messages with fraudulent content and inbound email viruses and prevent your employees from sending viruses with outbound email..

Topics:

- Anti-Phishing
- Anti-Virus

Anti-Phishing

Topics:

- Phishing Overview
- Configuring Phishing Protection

Phishing Overview

Two audiences are targeted for fraudulent phishing schemes:

- *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 Website 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.

Configuring Phishing Protection

To configure Email Security for phishing:

1 Navigate to **Security Service | Anti-Phishing** on the **MANAGE** view of your Email Security solution.

2 Select which action to take for messages identified as **Definite Phishing**. For more information about available actions, see the following table:

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user's mailbox was unavailable (for example, not found or rejected for policy reasons).
Store in Junk Box (default setting)	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	Forward the email message for review to the specified email address. For example, you could "Send To [postmaster]."
Tag With	The email is tagged with a term in the subject line, for example [PHISHING] or [LIKELYPHISHING]. Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Add X-Header	This option adds an X-Header to the email with the key and value specified to the email message. The first text field defines the X-Header. The second text field is the value of the X-Header. For example, a header of type "X-EMSJudgedThisEmail" with value "Fraud" results in the email header as: "X-EMSJudgedThisEmail:Fraud"

3 Select which action to take for messages identified as **Likely Phishing**. These are the same as for **Definite Phishing**.

4 Select the A**llow users to unjunk phishing messages** check box if you want to allow users to unjunk fraudulent messages.

5 To send copies of fraudulent email messages to a person or people designated to deal with them, enter the recipients' email addresses in the test box for **Send copies of emails containing phishing attacks to the following email addresses**. Separate multiple emails addresses with a comma.

6 Click **Apply Changes**.

Anti-Virus

Topics:

- Inbound Anti-Virus Protection
- Outbound Anti-Virus Protection

Inbound Anti-Virus Protection

Anti-Virus protection can be configured on the **Inbound** and **Outbound** paths. You are able to define separate actions for **Definite Viruses** and **Likely Viruses**.

To configure Anti-Virus protection on the inbound path:

1 Navigate to **Security Services | Anti-Virus** on the **MANAGE** view and select **Inbound**.

> ⓘ | **NOTE:** If you have licensed more than one virus-detection engines, they all work in tandem.

2 Choose one of the actions in **Actions to take for Definite Viruses and Likely Viruses** to take in response to a **Definite Virus**.

Actions to take for Definite Viruses and Likely Viruses

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user’s mailbox was unavailable (for example, not found or rejected for policy reasons). **NOTE:** When Capture analysis confirms a definite virus or likely virus, the message is quarantined—even if the reject action is selected—and any attachments are stripped. The quarantine preserves a record of the action and the message is recoverable if needed, rather than being lost.
Store in Junk Box (default setting)	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	Forward the email message for review to the specified email address. For example, you could Send To `postmaster`.
Tag With	The email is tagged with a term in the subject line, for example `[VIRUS]`. Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Add X-Header	This option adds an X-Header to the email with the key and value specified to the email message. The first text field defines the X-Header. The second text field is the value of the X-Header. For example, a header of type X-`EMSJudgedThisEmail` with value “Virus” results in the email header as: X-`EMSJudgedThisEmail:Virus`

3 Choose one of the actions in **Actions to take for Definite Viruses and Likely Viruses** to take in response to a **Likely Virus**. Change the text fields, if needed, to define the response appropriately.

4 In the Miscellaneous section, select the **Allow Users to Unjunk Viruses** check box to allow users to view messages with viruses in the Junk Box.

The virus is removed before the user accesses the message. This setting allows both Viruses and Likely Viruses to be unjunked.

5 If you want to turn off or disable any specific virus engines, check the appropriate box.

> ⓘ **NOTE:** Disabling a virus engine causes the SMTP service to restart on the Control Center and Remote Analyzers.
>
> **NOTE:** Currently, only Kaspersky can be disabled.

6 Click **Apply Changes**.

Outbound Anti-Virus Protection

Use this page to guard your organization from accidently sending malicious viruses

Topics:

- General Settings
- Zombie Protection Settings
- Flood Protection

General Settings

The general settings apply to all users.

To define the General Settings:

1 Navigate to **Security Services | Anti-Virus** on the **MANAGE** view and select the **Outbound** button.

2 Choose one of the actions in **Actions to take for Definite Viruses and Likely Viruses** to take in response to a **Definite Virus**.

Actions to take for Definite Viruses and Likely Viruses

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user’s mailbox was unavailable (for example, not found or rejected for policy reasons).
Store in Junk Box (default setting)	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	Forward the email message for review to the specified email address. For example, you could Send To `postmaster`.

3 Choose one of the actions in **Actions to take for Definite Viruses and Likely Viruses** to take in response to a **Likely Virus**.

4 Scroll down to the bottom of the page and select **Apply Changes**.

Zombie Protection Settings

Unauthorized software may be running on a computer within your organization and sending out junk email messages with spam, phishing, virus, or other unauthorized content. This scenario could happen if your organization was subjected to a virus attack called Trojans or a user downloaded something 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.

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 enable Zombie Protection:

1 Navigate to **Security Services | Anti-Virus** on the **MANAGE** view and select the **Outbound** button.

2 Check the box to **Enable Zombie and Spyware Protection**.

3 Use the Monitoring for Zombie and Spyware Activity section to configure several alerts to notify the administrator. The following alerts can be sent:

- **Email is sent from an address not in LDAP**
- **More than (specify number) messages are identified as possible threats** (within the last hour)
- **More than (specify number) messages are sent by one user** (within the last hour)

4 Set the actions to take when emails are sent by zombies. Zombie Protection Options describes the available Action and Miscellaneous Settings for the Zombie Protection feature.

Zombie Protection Options

Action	Description
Action for messages leaving your organization that are identified as spam, phishing attacks, or other threats	Select one of the following settings: **Allow Delivery**—Allows the delivery of the message without interference. **Permanently Delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved. **Store in Junk Box**—Stores messages with potential threats in the outbound Junk Box.
Action for messages leaving your organization in which the "From" address is not in LDAP	Select one of the following settings: **Allow any "From" address**— Allows messages from all email addresses. Note that this is the only option you are able to use if you have not configured LDAP. **Permanently delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved. **Store in Junk Box**—Stores messages from unknown senders in the Junk Box.

Zombie Protection Options

Action	Description
Activate/Deactivate Outbound Safe Mode preventing any dangerous attachments from leaving your organization	Outbound Safe Mode blocks all emails with potentially dangerous attachments from leaving your organization. When there is a new virus outbreak and one or more of your organization's computers is affected, the virus can often propagate itself using your outbound email traffic. Outbound Safe Mode also minimizes the possibility of new virus outbreaks spreading through your outbound email traffic.
When Outbound Safe Mode is on, take this action for any message with dangerous attachments	If you have enabled Outbound Safe Mode, select one of the following actions when a message with dangerous attachments is received: **Permanently delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved. **Store in Junk Box**—Stores messages from unknown senders in the Junk Box.
Automatically turn Outbound Safe Mode on and alert administrators every 60 minutes that Safe Mode is on if	These settings do not take any action other than alerting the administrator of a potential zombie infection. Select any of the check boxes to send and alert to the administrator if: • **Email is sent from an address not in the LDAP (within the last hour)** • **More than (specify number) messages are identified as possible threats within the last hour** • **More than (specify number) messages are sent by one user within an hour**
Specify senders that will not trigger alerts or actions	Enter email addresses in this box that you want exempt from Zombie Protection. (This list might include any email addresses that are not in LDAP and email addresses that are expected to send a lot of messages.)

Flood Protection

The Flood Protection feature supports Zombie Protection by automatically blocking specified users from sending outbound mail when it exceeds the specified Message Threshold.

To enable Flood Protection:

1. Navigate to **Security Service | Anti-Virus** on the **MANAGE** view and click the **Outbound** tab.
2. Scroll down to the **Flood Protection** section.
3. Click the **Enable Flood Protection** check box.
4. Configure the following settings:
   - **Message Threshold**—Specify the amount of outbound messages (between 1-10,000) that are sent by a single sender. Then, specify the interval (in hours) by selecting a value from the drop down list. The Flood Protection service activates when a sender has exceeded the amount of messages sent within the specified interval of hours.

- **Alert sender when threshold is crossed**—Enable this option to alert the sender that he/she has exceeded the organizational threshold. Note that as a result, outbound emails are now affected.
- **Action on outbound message from Flood Senders**—Select one of the following options to determine what action is taken on outbound messages from flood sender(s):
  - **Permanently delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved.
  - **Store in Junk Box**—The message moves to the Junk Box and flagged as 'likely virus' with the category name 'flood_protection.' The administrator is able to unjunk the message, which is then delivered from the outbound path.
  - **None**—No action is taken; messages go through as usual.
- **Flood Protection Senders Exception List**—Found under the Miscellaneous section, specify the list of outbound senders that are exempt from the Flood Protection rule.
- **Flood Senders List**—Users that exceeded the specified Message Threshold values are added to this table by Email Address and the time which the Flood Sender was found exceeding the threshold. To remove a user from the Flood Senders List, select the check box next to the email address(es) you wish to remove, then click the **Delete** button.

5 When finished configuring the **Flood Protection** settings, click the **Apply Changes** button.

16

Capture, Encryption and Connections

Topics:

- Capture ATP
- Encryption Service
- Connection Management

Capture ATP

Capture ATP performs the following functions:

- Scans suspected messages.
- Renders a verdict about the message.
- Takes action based on what the administrator configures for that verdict.

ⓘ **NOTE:** All three anti-virus options (McAfee, Kaspersky, and Cyren) also need to be licensed to enable the Capture ATP license.

Unlike the anti-virus engines that check against malware signatures stored locally, messages for Capture ATP are uploaded to the back end cloud servers for analysis. These messages are typically advanced threats that evade identification by traditional static filters. They need to be identified by their behavior, and thus need to be run in a highly instrumented environment. Capture ATP accepts a broad range of file types to analyze.

The process for engaging Capture ATP is outlined below:

1. Inbound email is first scanned by the other anti-virus plug-ins.
   - If a threat is detected, then the appropriate action is taken (discard, junk, tag, etc.).
   - If the service is enabled, all the anti-virus plug-ins return a *no threat* result, and the message contains an eligible attachment, the email is sent to Capture ATP for analysis.
2. The attachment is uploaded to the Capture server and quarantined in the Capture Box.
3. Capture ATP performs the analysis and returns a verdict.
4. Further analysis is performed and Email Security applies the policy based on the final disposition of the message.

Capture ATP status and settings can be managed at **Security Services | Capture ATP** on the **MANAGE** view. Refer to Capture ATP Logs for information on uploading a file for analysis.

Basic Setup Checklist

The Basic Setup Checklist shows the status of the various licenses required for Capture ATP. For each item listed, a red X indicates no subscription or an expired one. A green check indicates the license is active or a service is functional.

The items tracked in the checklist include:

- Status of Capture ATP functionality. A link is provided to test connectivity between your appliance and the back end server where the captured file is analyzed.
- Status of the required anti-virus licenses.
- Status of the base license.
- Status of the anti-spam license.

ⓘ | **NOTE:** For each active item, a link for managing licenses is provided.

Blocking Behavior

Files that are not blocked or excluded by traditional Email Security services are sent to Capture ATP for analysis. If the Capture analysis returns a malicious judgment, Email Security applies the actions defined by the **Anti-Virus** options. A link is provided so you can jump immediately to the **Anti-Virus** page and view the settings for inbound and outbound traffic.

ⓘ | **IMPORTANT:** When Capture analysis confirms a definite virus or likely virus, the message is quarantined and any attachments are stripped. This action occurs even if the anti-virus settings specify a reject action. The quarantine preserves a record of the action and the message is recoverable if needed.

Exception Management

Exception Management provides the flexibility for you to define those unique situations in your environment where you don't want certain types of files transferred to Capture ATP for analysis.

In the upper part of the Exception Management section, specify the maximum file size of attachments that can be transferred to Capture ATP for analysis. The default and recommended option is a maximum file size of 10 MB. You can opt for larger file sizes, but the trade-off is the possibility of processing delays for likely good email.

Click on **Submit** once you define the maximum file size.

In the lower part of the Exception Management section, specify the file types, people, companies, mailing lists or IP addresses whose attachments are not be sent to Capture ATP for analysis.

To define the exceptions:

1. Select **Add exception**.
2. Choose the exception type at the top of the window:
   - Person from email
   - List to email
   - Company to/from domains
   - IP Address to/from IP addresses
   - Attachment file type

3 Enter the details in the text box. Enter only one element, email address or domain per line. If you chose **Attachment file type**, select the file type from the drop down list provided.

4 Click on **Add**.

Click on **Clear Filters** to remove all the filters defined in the table.

Within the table, you can sort and filter the exceptions. Click in the heading for the column you want to sort in ascending or descending order. The order is indicated by the small arrowhead in the heading field.

To filter data in the table:

1 Click on the drop down option in the column heading you want to filter.

2 Check the box by **Filters**.

3 Type the search string in the text box, and the table adjusts to show the results of the filtering.

4 Uncheck the box to remove the filter and the table returns to its prior view.

Encryption Service

The Encryption Service feature works in tandem with Email Security as a Software-as-a-Service (SaaS), which provides secure mail delivery solutions. The mail messages that have [SECURE] as part of the Subject are encrypted and securely delivered to the recipient via the Encryption SaaS.

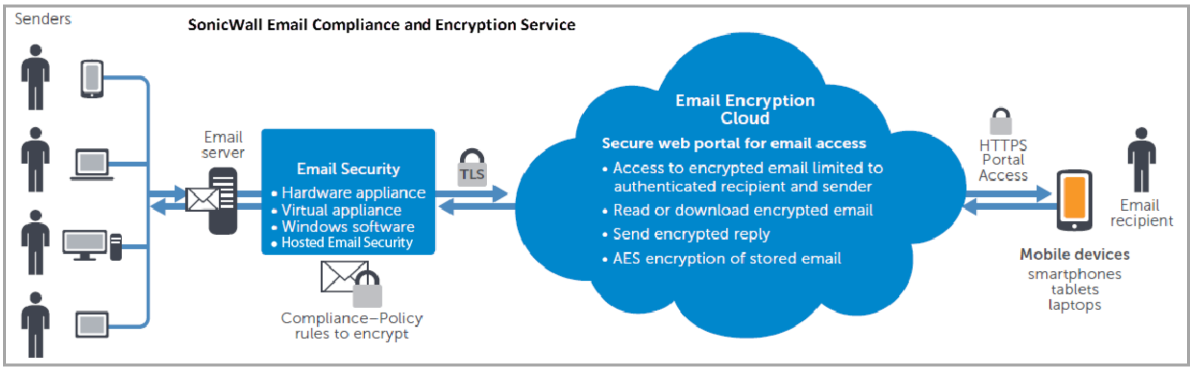
A few things to consider when using the SonicWall Encryption Service:

- The customer is responsible for protecting user passwords and using care in spelling email addresses when sending emails, especially emails containing sensitive information.
- Encrypted emails automatically expire after 30 days and are not recoverable.
- The subject lines of email messages are not encrypted and should not include electronic protected health information (ePHI) or confidential information.

Topics include:

- Encryption Service Overview
- Licensing Email Encryption Service
- Enabling the Secure Mail Policy
- Configuring Encryption Service

Encryption Service Overview


Senders
SonicWall Email Compliance and Encryption Service
Email server
Email Security
• Hardware appliance
• Virtual appliance
• Windows software
• Hosted Email Security
TLS
Compliance–Policy rules to encrypt
Email Encryption Cloud
Secure web portal for email access
• Access to encrypted email limited to authenticated recipient and sender
• Read or download encrypted email
• Send encrypted reply
• AES encryption of stored email
HTTPS Portal Access
Email recipient
Mobile devices
smartphones
tablets
laptops

The Encryption Service works with both outbound and inbound email messages. The Encryption Service must first be licensed through the **License Management** page on the **MANAGE** view. The administrator can then enable the default policy filter that allows sending secure email via the Encryption Service. After adding the necessary sender domains and public IP addresses, the administrator can then add users that are licensed to use Encryption Service.

Outbound messages flow in the following order:

1 A user in an organization sends a secure email message. It is sent through the exchange email server of the organization.

2 The message is then processed by Email Security. Email Security recognizes the message as Secure Mail based on the auto sender domains or any other policy set to **Route to Encryption Service**.

3 The message is sent from the Email Security appliance via TLS to the SonicWall Email Encryption Cloud. The Email Encryption Cloud determines if this is a secure message based on the auto sender domains or any other policy set to 'Route to Encryption Service.'

4 The Email Encryption Cloud then sends a notification email to the recipient. This email includes a URL to the secure message.

5 The Secure Mail recipient clicks the URL and is required to log into the Email Encryption Cloud to retrieve the message. Once the recipient views the message, the sender gets a notification mail from Email Encryption Cloud indicating that the secure message has been viewed.

Licensing Email Encryption Service

Because Encryption Service is a subscription service, you must purchase a license by logging in to your MySonicWall account or by contacting your SonicWall reseller.

ⓘ **NOTE:** The Encryption Service subscription license must match the Email Protection Subscription (Anti-Spam and Anti-Phishing) user account. If not, you receive an error message.

To license the Email Encryption Service:

1 Navigate to the **Licence Management** page of your SonicWall appliance.

2 Select **Manage Licenses**.

3 Log in to your MySonicWall account with your username and password and select **Submit**.

4 Click on the **Activate** or **Try** link to activate Email Encryption Service.

5 Enter the **Email Encryption Service Activation Key** in the text field provided.

6 Select the **Data Center nearest to you** from the drop down list.

7 Enter the **Company Name**.

8 Add the **Admin Email Address**.

9 Enter the **Auto Sender Domains**. If entering more than one domain, separate them with a comma.

   ⓘ **NOTE:** Be sure you own and control these domains before setting them up as the Auto Sender Domains.

10 Click on the **Submit** button and the licensing information is updated.

11 Navigate to **Security Services | Encryption Services** to verify that the settings you just entered are shown in the **Settings** section.

Enabling the Secure Mail Policy

To begin using the Secure Mail Service, you must first enable the default outbound policy to Send Secure Mail. Emails that satisfy the set conditions are encrypted to received secure emails from Encryptions Service without getting flagged as SPF failures, the corresponding inbound policies have to be enabled too.

To enable Outbound Secure Mail:

1. Navigate to **Policy & Compliance > Filters** on the **MANAGE** view.
2. Click the **Outbound** tab.
3. Locate the **PGP: Deliver Encrypted Msg (Delivers Encryped Message to External Recipient)** filter, and select the **Edit** button.
4. Check the box to **Enable this filter**. You can either keep the default settings or edit the settings to customize this filter.
5. When finished configuring the settings, scroll to the bottom and click **Save This Filter**.

ⓘ **NOTE:** The **Policy & Compliance > Filters** page allows you to drag-and-drop filters, changing the precedence order of policies, which may be useful for your specific corporate needs. For more information regarding policies, refer to the chapter on Policy & Compliance.

To enable Inbound Secure Email:

1. Navigate to **Policy & Compliance > Filters** on the **MANAGE** view of your SonicWall appliance.
2. Click the **Inbound** tab.
3. Locate the **PGP: Decrypt (Sends Encrypted Inbound Message to PGP Universal Server for Decryption)** filter, and select the **Edit** button.
4. Check the box to **Enable this filter**. You can either keep the default settings or edit the settings to customize this filter.
5. When finished configuring the settings, select **Save This Filter**.

Configuring Encryption Service

Once you have successfully licensed the Email Encryption Service and enabled the Secure Mail outbound policy, you can configure the settings for the service.

Topics:

- Settings
- Allowed IP List
- User View Setup

Settings

To configure the Encryption Service settings:

1. Navigate to **Security Services | Encryption Service** on the **MANAGE** view.
2. Under the **Account Management Settings** section, click the **Refresh** button to synchronize the account management settings from Encryption Service.

3 Select **Reset Credentials** button to reset and create new credentials. The credentials are used to authenticate the Secure Mail Server Email gateway.

4 Under the **Settings** heading, edit the **Company Name**, if needed.

5 Enter the **Auto Sender Domains** in the space provided. A user account is automatically created for the mail sent from these domains.

> ⓘ **NOTE:** Be sure you own and control the domains listed here.

6 Check the box if you want to **Allow the Encryption Service to route email replies directly to your organization's Email Server over a secure channel**.

> ⓘ **NOTE:** The TLS has to be enabled on your inbound paths on the **System Setup | Server** page.

7 Select **Apply Changes** when finished.

Allowed IP List

These settings define your email servers to the software.

To define IP addresses:

1 **Enter the list of public IP addresses** for the systems that deliver mail outside your organization. Put each entry on its own line, separated by a carriage return.

2 **Enter a list of public IP addresses and the associated domains in your organization that receive mails directly from Encryption Services.** If not specified, MXRecord is used to deliver mails to the organization. Separate each entry with a carriage return.

3 Select **Apply Changes**.

User View Setup

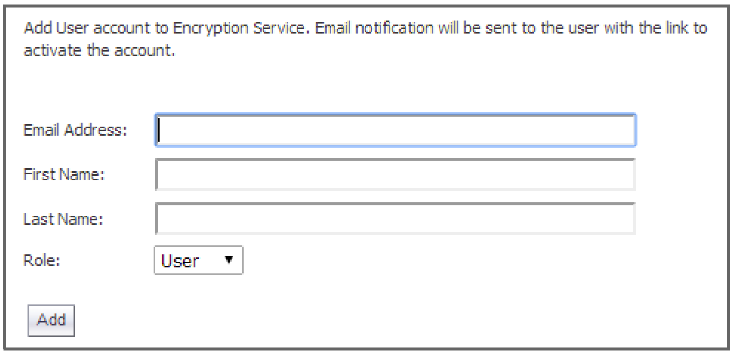
SonicWall recommends that the administrator should add users to the Encryption Service. If any mail messages are sent to the Email Encryption Cloud from a sender account not already created, the Email Encryption Cloud automatically creates a Secure Mail sender account, as long as the domain in the email address is one of the Auto Sender domains.

Adding a New User

To add a new user to the Encryption Service:

1 Navigate to the **Security Services | Encryption Service** page.

2 Scroll down to the **User View Setup** section, and click the **Add** button.


Add User account to Encryption Service. Email notification will be sent to the user with the link to activate the account.

Email Address:	
First Name:	
Last Name:	
Role:	User ▼

3 Enter the following fields:

- **Email Address**—Enter the email address for the user.
- **First Name**—Enter the first name of the user.
- **Last Name**—Enter the last name of the user.
- **Role**—Select the role of the user from the drop down list. The available options are User or Admin.

4 Click **Add** to finish. The new user displays in the User View Setup list.

ⓘ **NOTE:** You may need to click the **Refresh** button to synchronize user accounts and settings from the Secure Email Encryption server if it does not automatically display.

Updating an Existing User

To update the information of an existing user:

1 Navigate to **Security Services | Encryption Services** and scroll down to **User View Setup**.

2 Select the check box corresponding to the user you want to update.

3 Click the **Update** button.

4 Edit the **First Name**, **Last Name**, or **Role**.

ⓘ **NOTE:** You cannot update the **User Email Address**.

5 Click **Update** to save changes made and update the user information.

Delete an Existing User

To delete an existing from the list:

1 Navigate to **Security Services | Encryption Services** and scroll down to **User View Setup**.

2 Find the user you want to delete and check the box by his or her name.

3 Select the **Delete** button.

Adding an Existing User

If you have LDAP configured, you can add existing users to the Secure Email Encryption Service.

To add existing users:

1. Navigate to **Security Services | Encryption Services** and scroll down to **User View Setup**.
2. Click the **Add Existing Users** button.

   A list of users displays based on what you have configured for your LDAP directory. You can search for an existing user by email address in the search field.
3. Select the user you wish to add, then click the **Add** button. The new user displays in the User View Setup list.

Importing Users

If you would like to add multiple users, you can import a .txt list of users to be added to the Secure Email Encryption Service.

The .txt file must use a <TAB> delimiter between the primary email address, first name, last name, and role of each user. You must use <CR> to separate entries. See the following example:

```
primary_email@company.com<TAB>firstname<TAB>lastname<TAB>admin<CR>
primary_email@company.com<TAB>firstname<TAB>lastname<TAB>user<CR>
```

The primary email address is mandatory, while the other fields are optional.

To import users:

1. Navigate to **Security Services | Encryption Services** and scroll down to **User View Setup**.
2. Click the **Import Users** button.
3. Click the **Choose File** button to select the file containing the list of users.
4. Click **Import**.

Exporting Users

To export the list of Encryption Service users:

1. Navigate to **Security Services | Encryption Services** and scroll down to **User View Setup**.
2. Click the **Export Users** button. The list exports a .txt file and saves it to your local system.

Cobranding and Reporting

The Encryption Service allows you the option to customize features on the management console. You can also customize reports from the Encryption Service.

The following are Cobrand and Reporting settings you can configure through the Encryption server portal:

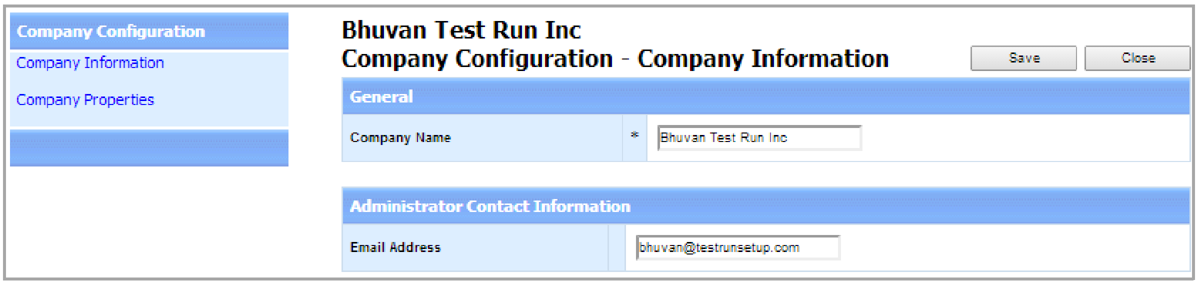
- Company and User Type Properties
- Cobrand Management Console
- Message Tracking Report
- User Logon Report
- User Reports by Message Size, Volume, Date, and Summary
- Total View Report

Company and User Type Properties

You can edit your organization’s information on the **Company Configuration > Company** page. The following fields are editable:

- **Company Name**—This is the company name specified on the **License Management** page once licensing the Encryption Service is completed.
- **Email Address**—This is the administrator’s email address specified on the **License Management** page once licensing the Encryption Service is completed.

The **Company Configuration > Company Properties** page allows you to edit the **Automatically Create Sender Accounts** setting. Select one of the following options: **Off**, **On**, or **Off Send Plain Text**.



Bhuvan Test Run Inc
Company Configuration - Company Information

General

Company Name * Bhuvan Test Run Inc

Administrator Contact Information

Email Address bhuvan@testrunsetup.com

Cobrand Management Console

The **Cobrand Management Console** page allows you to edit your organization’s existing cobrand settings or create a new cobrand.

To edit an existing cobrand or create a new cobrand:

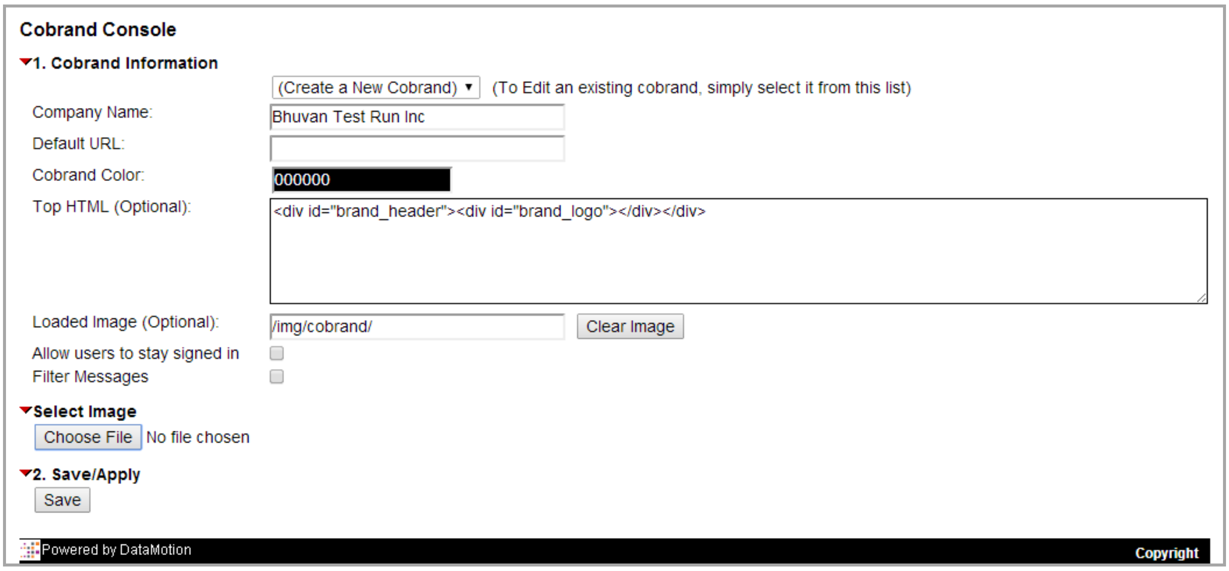
1 Under the Cobrand Information section, select **Create a New Cobrand** from the drop down list to create a new cobrand. To edit an existing cobrand, select it from the drop down list.

2 Specify the following cobrand settings:

   - Company Name—A descriptive name that is associated with the cobrand and is displayed in the drop down list for editing.
   - Default URL—The URL where users are directed when they click the cobrand image. Note that you must include the protocol/scheme (“http://”) in the URL.
   - Cobrand Color—The web color used for the login panel, top and bottom ribbon bars (menu and status bars) for Web pages on the server portal. The web color is identified with 6-character hexadecimal number, commonly used with HTML, CSS, and other applications. You can also identify the cobrand color using the Color Selector box that displays upon editing the hexadecimal number.
   - Top HTML (Optional)—Allows you to specify a block of HTML coding to be used in place of the cobrand image in the page header. The HTML can contain text, links, graphics, and columns, or follow an HTML style sheet.
   - Note that if the Top HTML field contains boilerplate code, do not delete it unless you intend to replace it with customized HTML.
   - Loaded Image (Optional)—Displays the database server path and internal filename for the uploaded cobrand image. Click the Clear Image button to immediately remove the image from the cobrand.
   - Allow users to stay signed in—Select the check box to enable, and then specify the amount of time for users to stay signed in.

- Filter Messages—Allows you to limit the messages that users see in their mailbox to messages related to the cobranded company. If enabled, the Secure Mail recipient’s mailbox only displays messages from or to the cobranded company, as long as the recipient accesses the server using the notification email link.
- Select Image—Select a cobrand image, such as an organization or company logo, that displays at the top of all the server portal pages. This is an efficient and easy way to create professional branding without requiring the use of HTML. Click the Choose File button to select the image you want assigned to the cobrand.

3 Click the **Save** button to save your changes and apply the cobrand to your organization.



Cobrand Console

1. Cobrand Information

(Create a New Cobrand) ▾ (To Edit an existing cobrand, simply select it from this list)

Company Name: Bhuvan Test Run Inc

Default URL:

Cobrand Color: 000000

Top HTML (Optional):

```
<div id="brand_header"><div id="brand_logo"></div></div>
```

Loaded Image (Optional): /img/cobrand/ Clear Image

Allow users to stay signed in □

Filter Messages □

Select Image

Choose File No file chosen

2. Save/Apply

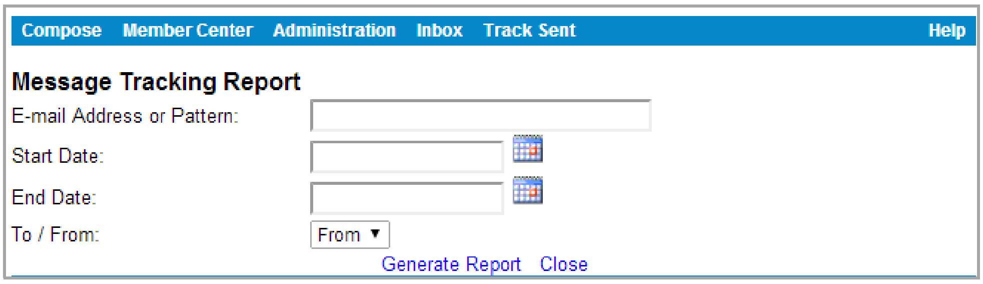
Save

Message Tracking Report

Use the Message Tracking Report to search through email addresses and subject lines of encrypted messages (message bodies are not included in the search).

To generate a Message Tracking Report:

1 Click the **Message Tracking Report** link from the Secure Mail Encryption Service portal.



Message Tracking Report

E-mail Address or Pattern:

Start Date:

End Date:

To / From: From ▾

2 Enter the search parameters into the **Email Address** or **Pattern**, **Start Date**, and **End Date** fields. The **To/From** drop down list specifies whether to search for the parameters in the To or From field of email messages.

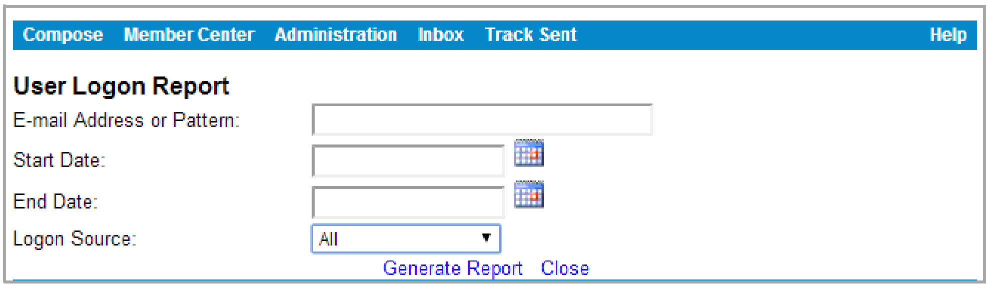
3 Click **Generate Report** link. The report displays all messages matching the specified criteria.

User Logon Report

The User Logon Report generates reports about user log on activity. You can search activity based on specific users, defined time frames, and also how the user logged into the service.

To generate a User Logon Report:

1 Click the **User Logon Report** link from the Secure Mail Encryption Service portal.



User Logon Report

E-mail Address or Pattern:

Start Date:

End Date:

Logon Source: All

Generate Report Close

2 Enter the search parameters into the **Email Address** or **Pattern**, **Start Date**, and **End Date** fields. The **Logon Source** drop down list specifies which service the user accessed. The default is **All**, which includes every service the user may have used.

3 Click the **Generate Report** link. The report generates all log on events for the user, based on the specified criteria.

User Reports by Message Size, Volume, Date, and Summary

There are several types of user reports, each of which can be filtered for sent or received messages (or both) for each user. These reports are summaries of user statistics, differing from the more detailed reports such as the Message Tracking Report.

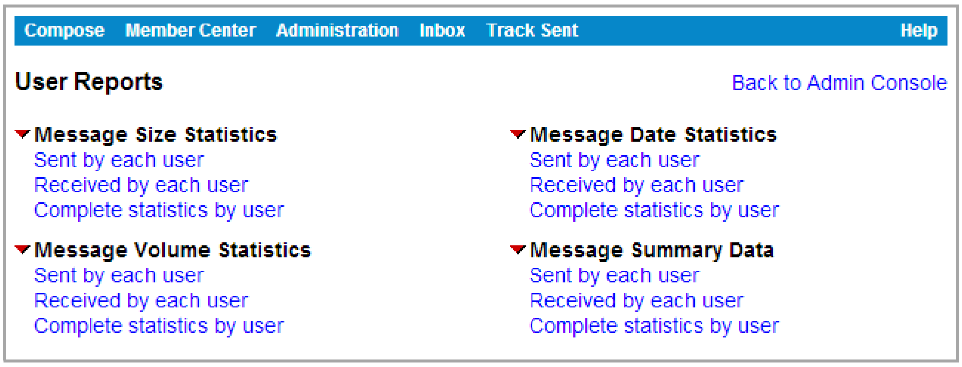
Types of user reports describes the types of reports that can be generated:

Types of user reports

Report Type	Description
Message Size Statistics	Shows the size of messages sent and received by each user
Message Date Statistics	Shows when messages have been sent by the user (first and last messages for each user)
Message Volume Statistics	Shows the number of messages sent/received by the user
Message Summary Data	Shows the fields of other statistics reports on one screen

To access any User Report:

1 Click the **User Reports by Message Size, Volume, Date, and Summary** link from the Encryption Service portal.



User Reports

Back to Admin Console

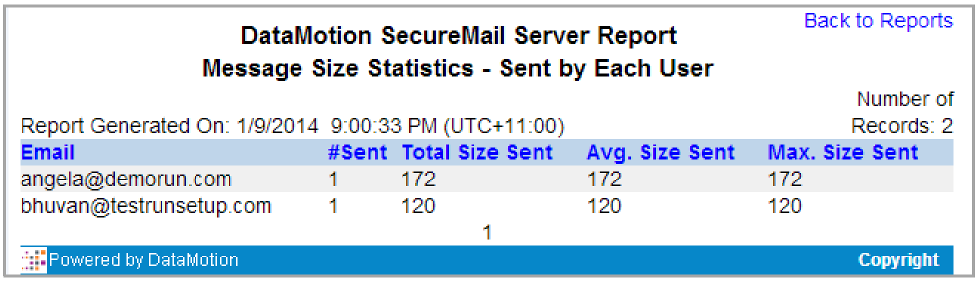
Message Size Statistics
Sent by each user
Received by each user
Complete statistics by user

Message Volume Statistics
Sent by each user
Received by each user
Complete statistics by user

Message Date Statistics
Sent by each user
Received by each user
Complete statistics by user

Message Summary Data
Sent by each user
Received by each user
Complete statistics by user

2 Click on the Report to view the information.


Back to Reports

DataMotion SecureMail Server Report
Message Size Statistics - Sent by Each User

Report Generated On: 1/9/2014 9:00:33 PM (UTC+11:00)

Number of Records: 2

Email	#Sent	Total Size Sent	Avg. Size Sent	Max. Size Sent
angela@demorun.com	1	172	172	172
bhuvan@testrunsetup.com	1	120	120	120

1

Total View Report

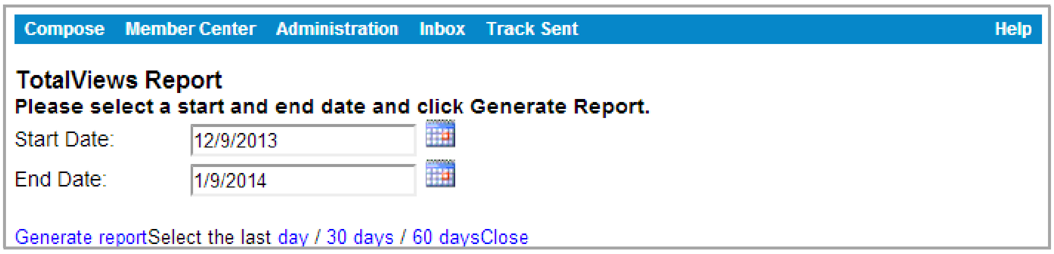
The **Total View Report** provides complete tracking of all messages sent through the Encrypted Service. The report contains a record of every messages sent along with the tracking data for the message (and attachments) in a single report. This report is provided as a CSV file that includes the following fields:

- Message ID
- Date
- From Email
- To Email
- Subject
- Notification Timestamp
- Message Status (Opened / Not Opened)
- Message Open Time
- Attachment Name
- Attachment (Accessed /Not Accessed)
- Attachment Open Time

ⓘ **NOTE:** Each message and every attachment within a message is reported separately. For example, a message to two recipients with two attachments generates four rows of data: Two for each recipient, with one attachment listed on each line per recipient.

To generate a Total View Report:

1. Click the **Total View Report** link from the Encryption Service portal.
2. Specify the **Date range** for the report. For more efficiency, you can click one of the quick links: Last **day**, **30 days**, or **60 days**. This automatically selects the specified time period.
3. Click the **Generate Report** link.
4. Click the **Download Report** link to save the CSV file to your local system. Click **Select Different Dates** to return to the previous screen and conduct a new search with different dates.



TotalViews Report

Please select a start and end date and click Generate Report.

Start Date: 12/9/2013

End Date: 1/9/2014

Generate reportSelect the last day / 30 days / 60 daysClose

Connection Management

SonicWall Email Security uses collaborative techniques as one of many tools to block junk messages. The collaborative database incorporates thumbprints of junked email from SonicWall Anti-Spam Desktop and users. Your server uses the HTTP protocol to communicate with a SonicWall data center to download data used to block spam, phishing, viruses, and other evolving threats.

The **Security Services | Connection Management** page includes the following subsections:

- Intrusion Prevention
- Quality of Service
- Manually Edit IP Address Lists

△ CAUTION: **The Connection Management page provides advanced features. SonicWall recommends that you not make any changes to these features if you are unsure of the impact the changes can have on your configuration.**

Intrusion Prevention

Intrusion Prevention comprises protection from Directory Harvest Attacks (DHA) and Denial of Service (DoS). Spammers stage DHAs to get a list of all users in your directory, making unprotected organizations vulnerable to increased attacks on email and other data systems. A Denial of Service (DoS) attack aims at preventing authorized access to a system resource or delaying system operations and functions for legitimate users.

ⓘ **NOTE:** Your LDAP must be configured before Intrusion Prevention can be configured.

Directory Harvest Attack (DHA) Protection

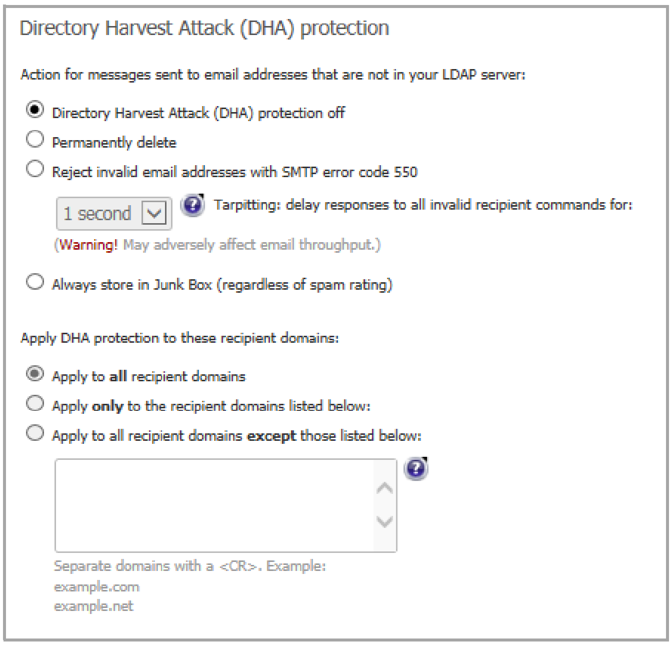
DHA can threaten your network in a number of ways:

- 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 an email address, 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 provide 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.
- Exposes users to fraudulent email masquerading as good email. DHA can perpetuate fraudulent email messages by giving malicious hackers the ability to target your users individually and by name.

ⓘ **NOTE:** User must be configured before directory protection can be configured.

To configure Directory Harvest Attack (DHA) protection:

1 Navigate to **Security Services | Connection Management**.



Directory Harvest Attack (DHA) protection

Action for messages sent to email addresses that are not in your LDAP server:

● Directory Harvest Attack (DHA) protection off
○ Permanently delete
○ Reject invalid email addresses with SMTP error code 550
1 second Tarpitting: delay responses to all invalid recipient commands for:
(Warning! May adversely affect email throughput.)
○ Always store in Junk Box (regardless of spam rating)

Apply DHA protection to these recipient domains:

● Apply to **all** recipient domains
○ Apply **only** to the recipient domains listed below:
○ Apply to all recipient domains **except** those listed below:

Separate domains with a <CR>. Example:
example.com
example.net

2 Define the **Action for messages sent to email addresses that are not in your LDAP server**. Choose one of the four options defined in the following table.

Actions for non-LDAP email addresses

Setting	Action	Result
Directory Harvest Attack (DHA) Protection Off	Processes all messages the same, whether email address is in LDAP or not. No action is taken on messages.	No directory protection.
Permanently Delete	All email messages 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.
Reject Invalid Email Addresses with SMTP error code 550	SMTP clients that specify invalid recipients are rejected with and SMTP error code 550 (also know as being tarpitted)	Responses to invalid recipient commands are delayed for some time period to slow down the rate that they can attack an organization's mail system. (See Caution below.)
Always Store in Junk Box (regardless of spam rating)	Email that is sent to an invalid address is stored in the Junk Box. Email Security does not process the email to determine if it is spam or another form of unwanted email.	Email Security recommends this option to protect the confidentiality of your directory population.

△ CAUTION: Enabling tarpitting protection uses your system resources (CPU, memory) and may slow down your server which can adversely affect throughput.

3 Define the options to **Apply DHA protection to these recipient domains**. The following table describes the available actions for DHA protection to recipient domains:

Actions for DHA protection

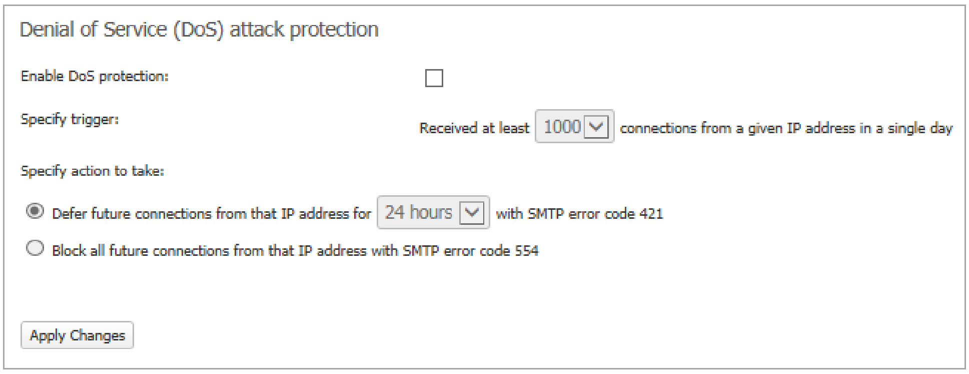
Option	Result
Apply to all recipient domains SonicWall recommends that most organizations choose Apply to all recipient domains.	Applies DHA protection to all recipient domains.
Apply only to the recipient domains listed below	Applies DHA protection to the recipient domain(s) listed in the text field. If listing multiple domains, separate them with a carriage return so they appear on different lines.
Apply to all recipient domains except those listed below Enter each domain on a separate line in the text box.	Applies DHA protection to all recipient domains except for those listed. If listing multiple domains, separate them with a carriage return so they appear on different lines.

Denial of Service (DoS) Attack protection

The Denial of Service Attack Protection adds an extra level of security to thwart an attack. DoS attacks can threaten your network in the following ways:

- Bandwidth consumption. The available bandwidth of a network is flooded with junkmail addressed to invalid recipients.
- Resource starvation. The mail servers of an organization are overwhelmed trying to process the increased volume of messages coming from infected computers, which leads to the mail servers to run out of resources (CPU, memory, storage space).

> **IMPORTANT:** To use the DoS Attach Protection feature, your SonicWall Email Security appliance must be the first destination for incoming messages. If you are routing mail to your Email Security appliance from an internal mail server or using an MTA, do not use DoS Attack Protection.



Denial of Service (DoS) attack protection

Enable DoS protection: □

Specify trigger: Received at least 1000 connections from a given IP address in a single day

Specify action to take:

● Defer future connections from that IP address for 24 hours with SMTP error code 421

○ Block all future connections from that IP address with SMTP error code 554

To configure Denial of Service (DoS) attack protection:

1. Navigate to the **Security Services | Connection Management** window.
2. Select the **Enable DoS protection** check box.
3. **Specify trigger** by selecting the number of connections to allow from a given IP address. in a single day
4. **Specify action to take** if the maximum number of connections is exceeded by selecting one of the following options:
    - **Defer future connections from that IP address for <*XX*> hours with SMTP error code 421**, where *XX hours* is an option selected from the drop down menu.

- **Block all future connections from that IP address with SMTP error code 554**.

5 Click the **Apply Changes** button.

Quality of Service

From the **Security Services | Connection Management** page, navigate to the Quality of Service section. The following sections describe how to configure the Quality of Service components:

- Throttling
- Connections
- Messages
- Miscellaneous
- Delayed Connection Management

Throttling

This section allows you to set specific thresholds to limit the sending ability of suspicious clients by limiting offensive IP addresses. Some examples of thresholds include:

- one connection per hour
- one message per minute for the next 24 hours
- ten recipients per message

To configure the Throttling (flow control) feature:

1 Navigate to the **Security Service | Connection Management** screen and scroll down to **Quality of Service**.

2 Select the check box to **Enable Throttling**.

3 Set **Specify trigger** by choosing the following options from the drop down menus

  - Specify the trigger number from pre-defined values. They range from **10** to **7000**.
  - Specify event type: **Connections**, **Messages**, or **Recipient Commands** from a given IP address
  - Specify the percentage of invalid emails to recipients. This setting only applies when **Recipient Commands** is selected.

4 Choose one of the following to **Specify an action to take**:

  - **Defer future connections from that IP address for <*XX*> hours with SMTP error code 421**, where *XX hours* is an option selected from the drop down menu.
  - **Block all future connections from that IP address with SMTP error code 554**.
  - Limit a future event type, for some number events per interval over a period of time by setting the following drop down menus:
    - Specify the event type: choose from **Connections**, **Messages**, or **Recipient Commands**
    - Number of events: options range from **1** to **60**.
    - Interval: predefined values range from **1 minute** to **24 hours**.
    - Period: predefined values range from **1 hour** to **1 year**.

5 Click the **Apply Changes** button.

ⓘ **NOTE:** Some scenarios can be implemented with either Denial of Services Attack Protection or Throttling settings. You can choose to throttle mail from clients above one threshold and choose to block clients above a second threshold.

Connections

In the **Connections** section, you can impose a limit on the number of simultaneous inbound and outbound connections that your Email Security server can accept. On the inbound path, this value limits the number of simultaneous connections external hosts can make to the Email Security appliance or software. On the outbound path, this value limits the number of simultaneous connections internal hosts can make to the Email Security to deliver messages. When the connections limit is exceeded, the Email Security sends a transient failure message (421 error code).

To set the connection limits:

1. Navigate to the **Security Service | Connection Management** screen and scroll down to **Quality of Service | Connections**.
2. Specify a number to **Limit number of inbound connections**. You can input a number between 0 and 5000. SonicWall recommends **250**. A **0** means no limit.
3. Specify a number to **Limit number of outbound connections.** You can input a number between 0 and 5000. SonicWall recommends **250**. A **0** means no limit.
4. Scroll down and click on **Apply changes**.

Messages

In the Messages section, you can limit messages based on number of recipients or message size.If too many recipients are specified in a message, Email Security sends a transient failure message (4xx error code). If the message size limit is exceeded, Email Security sends a permanent failure message (5xx error code).

Specify the **Limit number of recipients** and **Limit message size (in bytes)** in the fields provided. These values apply to both inbound and outbound paths.

To set the message parameter limits:

1. Navigate to the **Security Services | Connection Management** screen and scroll down to **Quality of Service | Messages**.
2. Specify a number to **Limit number recipients**. A **0** in that field means no limit.
3. Specify the number of bytes to **Limit message size**. A **0** in that field means no limit.
4. Scroll down and click on **Apply changes**.

Miscellaneous

In the **Miscellaneous** section, you can enable a series of specific connection management settings. Bounce Address Tag Validation (BATV) reduces the number of unauthorized Non-Delivery Reports (NDR) delivered to your organization. Greylisting discourages spam without permanently blocking a suspicious IP address. By disabling strict MAIL FROM checking, you can reduce the load on the downstream server, and you can drop SMTP connections based on using the GRID Network IP reputation. You can also disable checks for IP addresses of unauthenticated mail senders.

To set the miscellaneous settings:

1. Navigate to the **Security Services | Connection Management** screen and scroll down to **Quality of Service | Miscellaneous**.
2. Select the **Bounced Address Tag Validation (BATV)** check box to enable the feature. Refer to Bounce Address Tag Validation (BATV) for details about how BATV works.
3. Select the **Greylisting** check box to enable the feature. Refer to Greylisting for details on how Greylisting works.

   ⓘ **IMPORTANT:** Greylisting is useful only for Email Security servers running the "first touch" server, or the server receiving email directly from the Internet. SonicWall recommends disabling Greylisting if Email Security is not first touch.

4. Select the **Disable strict MAIL FROM checking** check box.

   By default, this feature enforces the SMTP specification with regard to the Reverse Path, which is the MAIL FROM field or Envelope From field. This feature reduces the load on the downstream server (for example, Microsoft Exchange), as well as reduces the amount of junk email allowed into the system.

5. Select the **Grid Network IP Reputation** check box to drop SMTP connections based on IP reputation. Refer to Grid Network IP Reputation for details on the Grid Network IP Reputation works.

   ⓘ **IMPORTANT:** This feature is useful only for SonicWall Email Security servers running as "first touch" servers. SonicWall recommends disabling the Grid Network IP Reputation feature if Email Security is not first touch.

6. Check the box if you want to **Disable checks for IP addresses of unauthenticated mail senders**.
7. Click the **Apply Changes** button.

Bounce Address Tag Validation (BATV)

BATV protects your organization by adding a signature to all outbound mail. When an NDR arrives, BATV checks for a valid signature. If the signature does not exist or does not pass the security check, then Email Security rejects the NDR. If the signature is authentic and the NDR is valid, Email Security continues analyzing the NDR.

BATV is not enabled by default. Although BATV is a powerful tool to eliminate invalid messages, some configurations on other mail servers may cause the BATV system to reject legitimate messages. The user who sent out the message is not notified that the message did not reach the intended recipient. Some reasons for false positives may include:

- LDAP upstream of SonicWall Email Security
- Null reverse paths instead of "From" fields
- Divergent SonicWall Email Security configuration
- Incorrect or altered reverse mail paths

Greylisting

When Greylisting is enabled, Email Security assumes that all new IP addresses that contact it are suspicious and requires those addresses to retry before it will accept the email. The Greylist is the list of IP addresses that have contacted the Email Security once, and have been sent a request to retry the connection. The Greylist is cleared and restarted every night; thus, if the connection is not retried before the Greylist is restarted, that server is asked to retry the connection again when it sends a retry of the initial connection request.

SonicWall Email Security also keeps track of the MTAs that have successfully retried the connection and are now deemed to be responsible MTAs. These IP addresses are added to a separate list. Connections from MTAs on this list are accepted without further retry requests, but the data from the connection is subjected to the rigorous checking performed by Email Security on all incoming mail.

The benefits of enabling Greylisting include:

- Increased effectiveness. Less spam received into the gateway translates to less spam delivered to the Inbox.
- Better performance, Greylisting reduces the volume of traffic at the gateway, as well as traffic to the downstream (for example, the Exchange server). As a result of the reduced volume, valuable system resources are freed up (such as sockets, memory, network utilization, etc.) allowing SonicWall Email Security to process more good mail in the same amount of time.
- Storage requirements. With the increasing focus on archiving, Greylisting reduces the amount of junk that gets stored in an archive, saving valuable resources.

If Greylisting is enabled, the Source IP Address is cross-checked against the Email Security Connection Management components in the following order:

Allowed List	If an IP address is on this list, it gets a free pass through Connection Management. Note the message is still subject to plug-in chain processing.
Blocked List	This IP address is already blocked from connecting to Email Security/
Deferred List	Connections from this IP address are already configured to be deferred.
DoS	Checks to see if the IP address has crossed the DoS threshold, and if so, takes the appropriate action.
Throttling	Checks to see if the IP address has crossed the throttling threshold, and if so, takes the appropriate action.
Responsible MTA List	This IP address has already been through and passed the Greylisting filter.
Greylist	The IP address is added to the Greylist if this is first time the IP address has contacted the Email Security.

Grid Network IP Reputation

The Grid Connection Management with Sender IP Reputation feature is the reputation a particular IP address has with members of the SonicWall Grid Network. When a connection is received from a known bad IP address, the error “554 No SMTPd here” is given, and the SMTP session is rejected.

If IP Reputation is enabled, the source IP addresses is checked in the following order:

Allowed List	If an IP address is on this list, it gets a free pass through Connection Management. Note the message is still subject to analysis by the Email Security server as usual.
Blocked List	This IP address is already blocked from connecting to Email Security server.
Reputation List	If the IP address is not in the previous lists, the Email Security server checks with the GRID Network to see if this IP address has a bad reputation.
Deferred List	Connections from this IP address are deferred. A set interval must pass before the connection is allowed.
DoS	If the IP address is not on the previous lists, the Email Security server checks to see if the IP addressed has crossed the DoS threshold. If it has, the server uses the existing DoS settings to take action.
Throttling	Checks to see if the IP address has crossed the throttling threshold, and if so, takes the appropriate action.

Not Greylist	This IP address has already been through and passed the grey-list filter. Note that this feature applies to the GRID Network IP Reputation only if it enabled.
Greylist	The IP address is added to the Greylist if this is first time the IP address has contacted the Email Security.Note that this feature applies to the GRID Network IP Reputation only if it enabled.

Delayed Connection Management

Delayed Connection Management provides the option to delay dropping a connection that has been judged malicious. Delaying the connection allows more information to be gathered about the sender until all recipients are known.

The default is to reject connections as soon as possible, which also allows better performance. If you opt to delay dropping connections by selecting after all recipients are known, which ensures better tracking, additional logging and auditing could impose on I/O burden on the Email Security server.

To set the Delayed Connection Management:

1. Navigate to the **Security Services | Connection Management** screen and scroll down to **Quality of Service | Delayed Connection Management**.
2. Select one of the options for **Rejected connections**:
   - **as soon as possible (better performance)** is the default.
   - **after all recipients are known (better tracking)** enables the delay.
3. Click on **Apply Changes** to finalize your choice.

Manually Edit IP Address Lists

This section allows you to manage the list of IP addresses to allow, defer, block, or throttle. Navigate to the **Security Services | Connection Management** screen, then scroll down to the **Manually Edit IP Address Lists** section. Click on the appropriate button to edit the list.

Allowed List	When an IP address is added to the Allowed list, Email Security continues to check for spam and phishing attacks in messages from that IP address. To add an IP address to the list or edit the existing list, click the Edit Allowed List button. Enter the IP address, then click the Add New IP Address button when finished. To delete an IP address from the list, select the check box of the IP address you wish to delete, then click the Delete Checked IP Addresses button.
Deferred List	In the case of a connection from a deferred IP address, the transient message is “421 4.4.5 Service not available, connection deferred.” To add an IP address to the list or edit the existing list, click the Edit Deferred List button. Enter the IP address, then click the Add New IP Address button when finished. To delete an IP address from the list, select the check box of the IP address you wish to delete, then click the Delete Checked IP Addresses button.

Blocked List

When the server receives a connection from an IP address on a blocked list, the Email Security responds with a “554 No SMTP service here” error message, and reject the TCP/IP connection.”

To add an IP address to the list or edit the existing list, click the Edit Blocked List button. Enter the IP address, then click the Add New IP Address button when finished. To delete an IP address from the list, select the check box of the IP address you wish to delete, then click the Delete Checked IP Addresses button.

Throttled List

When the SMTP server receives a connection from an IP address on this list, Email Security responds with the error message “421 4.4.5 Service not available, too many connections due to throttling” and drops the TCP/IP connection.

To add an IP address to the list or edit the existing list, click the Edit Throttled List button. Enter the IP address and the amount of hours to throttle for, then click the Add New IP Address button when finished. To delete an IP address from the list, select the check box of the IP address you wish to delete, then click the Delete Checked IP Addresses button.

17

Reporting

In the **Reporting** section of the **MANAGE** view allows you to different kinds of reporting:

- Configure Known Networks is where you define known network groups to use as filters for DMARC reports.
- Scheduled Reports is where you customize and schedule delivery of reports through email.

Configure Known Networks

Configure Known Networks is a specific filter for DMARC reports. The **Add** button allows you to create new server groups by adding IP addresses and associating them to a **Server Group Label** you define. The Server Group Labels *my servers* and *external trusted servers* can be edited, but you are not allowed to delete them. They are system defined and are typically used as follows:

my servers	Usually made up of the list of company-owned IP addresses
external trusted servers	Lists the IP addresses of company-trusted external servers and customers

To add a Server Group Label:

1. Navigate to **Reporting | Configure Known Networks**.
2. Select **Add**.
3. Type the label name in **Server Group label** field.
4. Enter the IP addresses of the servers you want to include in that group. If listing multiple servers, put each on a separate line.

   ⓘ | **NOTE:** The **IP Address** field allows IPv4 CIDR and IPv6.

5. Select **Add** to save the group.

To edit a Server Group Label:

1. Navigate to **Reporting | Configure Known Networks**.
2. Select **Edit** on the line next to the group label you want to edit.
3. Edit or remove the IP addresses that you want to change.
4. Select **Save** to keep the changes.

To delete a Server Group Label:

1 Select **Delete** on the line next to the group label you want to remove.

2 Click **Yes** to confirm that you want to delete that Server Group Label.

To export the Known Networks file:

1 Click on **Export**. The file is downloaded locally.

To import the Known Networks file:

1 Set up the file prior to importing it.

Email Security only supports importing XML files. If starting new, use the following template as a sample to create the file correctly.

NOTE: my servers and **external trusted servers** are required even they have no IP data for them.

--XML sample data--

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="no"?>
<known_networks date="20140224232207" lastupdatedby="xxxxx"
writeversion="1">

<known_network name="my servers">
<ipaddress>204.14.232.70</ipaddress>
<ipaddress>209.167.231.144</ipaddress>
</known_network>

<known_network name="external trusted servers">
<ipaddress>204.14.232.70/24</ipaddress>
<ipaddress>209.167.231.144</ipaddress>
</known_network>

<known_network name="saiyer server">
<ipaddress>10.20.202.12</ipaddress>
<ipaddress>209.85.220.175</ipaddress>
<ipaddress>216.82.243.196</ipaddress>
</known_network>

<known_network name="bhuvan server">
<ipaddress>10.223.232.43</ipaddress>
<ipaddress>195.229.241.85</ipaddress>
<ipaddress>2001:558:fe14:43:76:96:62:16</ipaddress>
<ipaddress>209.167.231.144</ipaddress>
<ipaddress>209.167.231.144/24</ipaddress>
<ipaddress>67.115.118.12</ipaddress>
<ipaddress>67.115.118.12/24</ipaddress>
<ipaddress>67.115.118.12/32</ipaddress>
</known_network>

<known_network name="jzhang servers">
<ipaddress>10.202.202.43</ipaddress>
<ipaddress>195.229.241.85</ipaddress>
<ipaddress>2001:558:fe14:43:76:96:62:16</ipaddress>
<ipaddress>209.167.231.144/24</ipaddress>
<ipaddress>67.115.118.12</ipaddress>
<ipaddress>67.115.118.12/32</ipaddress>
```

```
</known_network>
</known_networks>
```

-------------------------------------XML sample data--

2 Navigate to **Reporting | Configure Known Networks**.

3 Select **Import**.

4 Select one of the following modes:

- Merge mode only imports the data that differs from the current data.
- Overwrite mode replaces the current data with the data in the importing XML files. You are asked to confirm that you want to overwrite current data.

5 Select **Browse...** and navigate to the new XML file you want to import.

6 Click on **Import**.

Scheduled Reports

You can have Email Security reports emails to you regularly. You can choose the type of report, a time span the data covers, the list of recipients, and so forth.

Data in the scheduled reports is displayed in the time zone of the server where the data is stored (either an All in One or a Control Center), just like the reports on the **MONITOR** view. Scheduled report emails are sent according to the time zone on that system as well.

To add a a scheduled report:

1 Navigate to **Reporting | Scheduled Reports** on the **MANAGE** view.

1 Select the **Add New Scheduled Report** button.

2 Select **Which report** from the drop-down list.

3 Select **Frequency of report email** from the drop-down list. Options range from **1 Day** to **30 Days**.

4 For **Time of day to send report**, select one of the following options:

- **Any time of day**
- **Within an hour of** <*choose time from drop down menu*>.

5 For **Day of week to send report**, select one of the following:

- **Any day of the week**
- **Send report on** <*choose day from drop down menu*>.

6 Select **Language of report email**.

7 Select **Report has data for the last** <*choose time period from drop down menu*>. Options range from **1 Day** to **180 Days**.

8 For **Report lists results by**, choose for the results to be listed by the **Hour** or by the **Day**.

9 Choose the **Report Format**: **JPEG**, **CSV**, or **PDF**.

10 Type the **Name from which report is sent**.

11 Type the **Email Address From Which Report is Sent**.

12 Type in the email addresses for the **Recipients of Report Email**. Separate multiple email addresses with a comma.

13 Type in the domains for the field **Reports shows email sent to these domains**. Separate multiple domains with a comma. If left blank, the report shows email sent to all domains.

14 Specify the **Report Name**.

15 Select **Save Scheduled Report** when finished. The reports appears in the Reports table.

Part 5

Appendixes

- Interface Map
- SonicWall Support

A

Interface Map

Beginning with Email Security 9.1, the interface has been enhanced so commands align under the key functions of **MONITOR**, **INVESTIGATE**, and **MANAGE**. Related commands on the left-hand menu are grouped under a divider labels for easier navigation. Refer to the following table to see how the classic interface maps to the enhanced interface.

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
Report & Monitoring	Reports	Dashboard	MONITOR			Dashboard
Report & Monitoring	Reports	Connection Management Reports	MONITOR	Event Summaries		All Event Connections
Report & Monitoring	Reports	Anti-Spam Reports	MONITOR	Event Summaries		Anti-Spam
Report & Monitoring	Reports	Anti-Spoof Reports	MONITOR	Event Summaries		Anti-Spoof
Report & Monitoring	Reports	Anti-Phishing Reports	MONITOR	Event Summaries		Anti-Phishing
Report & Monitoring	Reports	Anti-Virus Reports	MONITOR	Event Summaries		Anti-Virus
Report & Monitoring	Reports	Directory Protection	MONITOR	Event Summaries		Directory Harvest
Report & Monitoring	Reports	Capture ATP Reports	MONITOR	Event Summaries		Capture ATP
Report & Monitoring	Reports	Policy Management Reports	MONITOR	Policy & Compliance		Policy
Report & Monitoring	Reports	Compliance Reports	MONITOR	Policy & Compliance		Compliance
Report & Monitoring	Reports	Encryption Service Reports	MONITOR	Policy & Compliance		Encryption
Report & Monitoring	Monitoring	Real-Time System Monitor	MONITOR	Appliance Health		Live Monitor
Report & Monitoring	Reports	Performance Metrics	MONITOR	Appliance Health		Performance Metrics
Report & Monitoring	Reports	User Statistics	MONITOR	Appliance Health		LDAP Users
Report & Monitoring	Monitoring	System Status	MONITOR	Current Status		System Status

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
Report & Monitoring	Monitoring	MTA Status	MONITOR	Current Status		MTA Status
Junk Box Management		Junk Box	INVESTIGATE			Junk Box
	(new feature)		INVESTIGATE	Email Continuity		Inbox
	(new feature)		INVESTIGATE	Email Continuity		Outbox
	(new feature)		INVESTIGATE	Email Continuity		Sent Items
Auditing		Messages	INVESTIGATE	Logs		Message Logs
Auditing		Connections	INVESTIGATE	Logs		Connections Logs
Capture ATP		Status	INVESTIGATE	Logs		Capture ATP Logs
Reports & Monitoring	DMARC Reports	DMARC Reports	INVESTIGATE	Tools		Run DMARC Reports
System		Audit Trail	INVESTIGATE	Tools		Audit Trail
System		Diagnostics	INVESTIGATE	Tools		Diagnostics
System		License Management	MANAGE			License Management
System		Advanced	MANAGE			Firmware Update
System		Manage Backups	MANAGE		Backup & Restore	Manage Backups
System		Schedule Backup	MANAGE		Backup & Restore	Schedule Backup
System		FTP Profiles	MANAGE		Backup & Restore	FTP Profiles
		Downloads	MANAGE			Downloads
Policy & Compliance		Filters	MANAGE	Policy & Compliance		Filters
Policy & Compliance		Policy Groups	MANAGE	Policy & Compliance		Policy Groups
Policy & Compliance	Compliance	Dictionaries	MANAGE	Policy & Compliance	Compliance	Dictionaries
Policy & Compliance	Compliance	Approval Boxes	MANAGE	Policy & Compliance	Compliance	Approval Boxes
Policy & Compliance	Compliance	Encryption	MANAGE	Policy & Compliance	Compliance	Encryption
Policy & Compliance	Compliance	Record ID Definitions	MANAGE	Policy & Compliance	Compliance	Record ID Definitions
Policy & Compliance	Compliance	Archiving	MANAGE	Policy & Compliance	Compliance	Archiving
System		Administration	MANAGE	System Setup	Server	Administration

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
System		LDAP Configuration	MANAGE	System Setup	Server	LDAP Configuration
System		Updates	MANAGE	System Setup	Server	Updates
System		Monitoring	MANAGE	System Setup	Server	Monitoring
System		Host Configuration	MANAGE	System Setup	Server	Host Configuration
System		Advanced	MANAGE	System Setup	Server	Advanced
System		User View Setup	MANAGE	System Setup	Customization	User View Setup
System		Branding	MANAGE	System Setup	Customization	Branding
System	Certificates	Generate/ Import	MANAGE	System Setup	Certificates	Generate/ Import
System	Certificates	Generate CSR	MANAGE	System Setup	Certificates	Generate CSR
System	Certificates	Configure	MANAGE	System Setup	Certificates	Configure
Users, Groups & Organizations		Users	MANAGE	System Setup	Users, Groups & Organizations	Users
Users, Groups & Organizations		Groups	MANAGE	System Setup	Users, Groups & Organizations	Groups
Users, Groups & Organizations		Organizations	MANAGE	System Setup	Users, Groups & Organizations	Organizations
System	Network Architecture	Server Configuration	MANAGE	System Setup	Network	Server Configuration
System	Network Architecture	MTA Configuration	MANAGE	System Setup	Network	MTA Configuration
System	Network Architecture	Email Address Rewriting	MANAGE	System Setup	Network	Email Address Rewriting
System	Network Architecture	Trusted Networks	MANAGE	System Setup	Network	Trusted Networks
Junk Box Management		Junk Box Settings	MANAGE	System Setup	Junk Box	Message Management
Junk Box Management		Junk Box Summary	MANAGE	System Setup	Junk Box	Summary Notifications
Anti-Spam		Spam Management	MANAGE	Security Services	Anti-Spam	Spam Management
Anti-Spam		Address Books	MANAGE	Security Services	Anti-Spam	Address Books
Anti-Spam		Anti-Spam Aggressiveness	MANAGE	Security Services	Anti-Spam	Anti-Spam Aggressiveness
Anti-Spam		Language	MANAGE	Security Services	Anti-Spam	Language
Anti-Spam		Black List Services	MANAGE	Security Services	Anti-Spam	Black List Services

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
Anti-Spam		Spam Submissions	MANAGE	Security Services	Anti-Spam	Spam Submissions
		Anti-Spoofing	MANAGE	Security Services		Anti-Spoofing
		Anti-Phishing	MANAGE	Security Services		Anti-Phishing
		Anti-Virus	MANAGE	Security Services		Anti-Virus
Capture ATP		Settings	MANAGE	Security Services		Capture ATP
		Encryption Service	MANAGE	Security Services		Encryption Service
System		Connection Management	MANAGE	Security Services		Connection Management
Reports & Monitoring	DMARC Reports	Configure Known Networks	MANAGE	Reporting		Configure Known Networks
Reports & Monitoring		Scheduled Reports	MANAGE	Reporting		Scheduled Reports

B

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Legend

⚠ **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

△ **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

ⓘ **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Email Security Administration
Updated - February 2018
Software Version - 9.1
232-004190-00 RevA

Copyright © 2018 SonicWall Inc. All rights reserved.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements. Select the language based on your geographic location to see the EUPA that applies to your region.

Open Source Code

SonicWall is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035