SOPHOS

Cybersecurity made simple.

Sophos Email Appliance
Configuration Guide
1 Setup and Configuration Guide

The purpose of this guide is to assist you with the basic configuration steps in the Sophos™ Email Appliance Setup Wizard and some essential post-configuration tasks.

Introduction

The guide assumes that you have already completed all of the steps in your appliance’s Setup Guide. While the guide contains enough information to prepare the Email Appliance for live email traffic, it should not be considered a substitute for the product documentation. For complete instructions on configuring and managing the Email Appliance, see the product’s online documentation.

The Setup Wizard prompts you to configure settings in five main categories:

- System Settings
- Network Configuration
- Register and Update
- Mail Routing
- Anti-Virus/Spam Settings

Although the wizard allows you configure many of the Email Appliance’s essential components, additional configuration options are available in the management console, which launches automatically when you exit the wizard. The "Post-Installation Configuration/Integration" section of the guide covers many of the configuration options that become available once activation is complete.

Of the remaining two sections, one describes how alias maps can be used to create associations between email addresses that can be applied for policy filtering and user preferences. The final section offers a summary of the system maintenance options.
2 Product Overview

The Sophos Email Appliance offers reliable gateway protection while allowing effective and efficient management. The Email Appliance’s compact and easy-to-manage format is designed to provide integrated threat protection.

Key Features

- **On-Board Quarantine**: The email quarantine resides on the same appliance as the mail-filtering software, translating into minimal infrastructure requirements, easy message-handling, and a low overall cost.

- **Powerful Message Tracking**: An advanced search function for tracking messages in system logs and the quarantine means that it’s easy to find and retrieve messages or trace their routing.

- **Powerful Dashboard**: Offers quick and comprehensive appliance management, monitoring and reporting, making it easy to execute common tasks and run key reports.

- **Built-In Hardware Redundancy [ES4000, ES5000 and ES8000]**: With dual hard disks, power supplies and processors, administrators can be confident that vital email systems will run without interruption.

- **Clustering Capability**: Two or more Email Appliances can be configured to back up a primary Email Appliance for uninterrupted operation and added security against the loss of configuration data.

Threat Protection

- **Reliable Protection Against Viruses, Spam, Spyware and Other Malware**: Single-vendor solution for better performance of all mission-critical functions and one source for updates and 24/7 support.

- **Powered by SophosLabs™**: Proactive protection from an industry-leading worldwide network of threat detection and analysis labs helps keep networks safe and clean 24/7, with reduced costs of disinfection and repair.

- **Optimized Operating System and Mail Transfer Agent**: The entire infrastructure is tuned to work seamlessly with the Email Appliance software.

- **Preset Policy Choices**: The ability to easily choose from several standardized email policy rule sets means that less time is spent on system setup and administration.

- **Real-Time Remote System Monitoring**: Sophos continuously monitors the system health and status of all installed appliances, helping to guarantee that your appliance is always up to date and functioning properly.

- **On-Demand Remote Assistance**: Customer-enabled secure (SSH) connection provides Sophos Technical Support with direct access to individual appliances for specific troubleshooting.

- **Superior Support**: Web-based, email and live telephone support available 24/7/365.
Software Features

Built for reliable operation, high-performance message throughput, and secure email scanning at the gateway, the Email Appliance software features are as follows:

- Powerful web management interface
- Personalized End User Web Quarantine
- Optimized operating system and high performance MTA
- Denial of Service (DoS) and Directory Harvest Attack (DHA) Protection
- High-performance mail-filtering engine
  - Anti-virus
  - Anti-spam
  - Content filtering
- Secure, self-managed on-board message quarantine
- Self monitoring
- Self updating

Powerful Web Management Interface

The Email Appliance’s web management interface is designed to be comprehensive, powerful and effective. The Dashboard displays the status of the system, including mail flow, software, and threat updates. It also offers rapid access to other management functions.

Personalized End User Web Quarantine

The quarantine reduces the administrative load by giving end users the ability to manage their own quarantines, activate their quarantine email summaries, and customize their own allowed and blocked senders lists.

Optimized Operating System and High-Performance MTA

The infrastructure is tuned to work seamlessly with the Email Appliance software, providing an integrated, hardened and reliable system.

DoS/DHA Protection

With one click, an administrator can enable protection against denial of service (DoS) and directory harvest attacks (DHA), securing the gateway with enterprise-level protection.

High-Performance Email Filtering

Anti-Virus
The Email Appliance uses the same Sophos Anti-Virus™ engine found in all Sophos products. Combined with its email policy tests for both inbound and outbound email, the Email Appliance protects against both viruses and potentially dangerous attachments.

**Anti-Spam**

Using multiple spam identification techniques, the Sophos anti-spam engine maintains a high capture rate and minimal false positives. SophosLabs continuously monitors and updates threat definitions for the anti-spam and anti-virus engines. The Email Appliance’s engines are capable of receiving threat definition updates every five minutes.

**Content Filtering**

The Email Appliance further extends email security with inbound and outbound content filtering. Administrators can manage content based upon simple keywords as well as sophisticated pattern matching.

**Self-Managed On-Board Message Quarantine**

Email-borne threats are held at the gateway inside the Email Appliance’s secure, self-managed quarantine. The quarantine automatically expires enough of the oldest messages to ensure that the quarantine does not exceed 70% of capacity and expires any messages older than 30 days.

**Self-Monitoring**

The Email Appliance constantly monitors its hardware, operating system, software, and applications. It reports and alerts on conditions that concern administrators. The monitoring system alerts the designated administrators and Sophos Technical Support of any critical conditions.

**Self-Updating**

The Email Appliance can update each of its software components. Maintenance time frames can be scheduled to apply these updates. Critical and non-critical updates supplied by Sophos are downloaded and installed in the next maintenance period. Optionally, you can defer non-critical updates beyond the scheduled maintenance period.

### Message Capacity

<table>
<thead>
<tr>
<th>Model</th>
<th>ES150</th>
<th>ES1100</th>
<th>ES5000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Message Capacity (per hour)</td>
<td>55900</td>
<td>108000</td>
<td>389000</td>
</tr>
<tr>
<td>Legitimate Message Capacity (per hour)</td>
<td>6800</td>
<td>13000</td>
<td>54000</td>
</tr>
</tbody>
</table>

**Environment Overview**

The Email Appliance is designed to function as an email gateway for a network. Incoming mail is relayed by the Email Appliance to internal mail servers or mail relays after being scanned for viruses, spam, and other specified content. Outgoing mail can be sent through the Email Appliance to an outbound relay or directly to the internet.
In the simple configuration example pictured here, incoming mail is filtered by the Email Appliance and then passed directly to a mail server for retrieval by clients. Outbound mail is sent from the clients to the mail server and then routed to the Email Appliance for delivery to external addresses. Alternatively, clients could use the Email Appliance itself as the their outbound SMTP relay. The Email Appliance would then pass local mail back to the mail server and pass external mail out to the internet.
3 Installing a Virtual Appliance

Optionally, you can deploy one or more appliances as virtual machines using VMware. These appliances can be clustered with other virtual appliances or Sophos Email Appliances. If you are not deploying virtual appliances, skip this section and proceed to “Initial Configuration”.

Prerequisites

- VMware ESX Server 3i
- VMware Infrastructure Client

Since virtual appliances use a 32-bit operating system, you should allocate no more than 4 GB of memory when creating an image.

Need to explain how to allocate the size of the image (20 GB by default).

To ensure the functionality of the Sophos Email Appliance, configure your network to allow access on the ports listed below. Some ports are required only for specific situations, such as when you enable directory services or when the appliance is part of a cluster.

### External Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
<th>Service</th>
<th>Protocol</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>22</td>
<td>Remote assistance</td>
<td>SSH</td>
<td>TCP</td>
<td>[Required] Between appliance and esa-ssh.sophos.com</td>
</tr>
<tr>
<td>25</td>
<td>Mail transfer</td>
<td>SMTP</td>
<td>TCP</td>
<td>[Required] Between appliance and internet/intranet</td>
</tr>
<tr>
<td>80</td>
<td>Software downloads</td>
<td>HTTP</td>
<td>TCP</td>
<td>[Required] Between appliance and internet</td>
</tr>
<tr>
<td>123</td>
<td>Network time synchronization</td>
<td>NTP</td>
<td>UDP</td>
<td>[Required] Between appliance and NTP server (e.g. pool.ntp.org)</td>
</tr>
<tr>
<td>443</td>
<td>Registration</td>
<td>HTTPS</td>
<td>TCP</td>
<td>[Required] Between appliance and esa-reg.sophos.com</td>
</tr>
<tr>
<td>444</td>
<td>Feedback</td>
<td>HTTP</td>
<td>TCP</td>
<td>Between appliance and sophos.com</td>
</tr>
<tr>
<td>10443/443</td>
<td>SPX Secure Email Portal</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Between appliance to internet (configurable)</td>
</tr>
<tr>
<td>32224</td>
<td>Time-of-Click (ToC) Protection</td>
<td>HTTP</td>
<td>TCP</td>
<td>Inbound from internet to appliance</td>
</tr>
</tbody>
</table>

### Internal Connections

<table>
<thead>
<tr>
<th>Port</th>
<th>Function</th>
<th>Service</th>
<th>Protocol</th>
<th>Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>20, 21</td>
<td>FTP backup</td>
<td>FTP</td>
<td>TCP</td>
<td>Between appliance and FTP server</td>
</tr>
<tr>
<td>24</td>
<td>Clustering</td>
<td>SSH</td>
<td>TCP/UDP</td>
<td>Between clustered appliances</td>
</tr>
<tr>
<td>25</td>
<td>Mail transfer</td>
<td>SMTP</td>
<td>TCP</td>
<td>[Required] Between appliance and internet/intranet</td>
</tr>
<tr>
<td>Port</td>
<td>Function</td>
<td>Service</td>
<td>Protocol</td>
<td>Connection</td>
</tr>
<tr>
<td>-------</td>
<td>-----------------------------------------</td>
<td>---------</td>
<td>----------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>53</td>
<td>DNS services</td>
<td>DNS</td>
<td>UDP</td>
<td>Between appliance and DNS server</td>
</tr>
<tr>
<td>161</td>
<td>SNMP monitoring</td>
<td>SNMP</td>
<td>TCP/UDP</td>
<td>SNMP monitoring server(s) to appliance</td>
</tr>
<tr>
<td>162</td>
<td>SNMP traps</td>
<td>SNMP</td>
<td>TCP/UDP</td>
<td>Appliance to SNMP monitoring server(s)</td>
</tr>
<tr>
<td>389, 3268, (636, 3269)</td>
<td>Directory services synchronization</td>
<td>LDAP(S)</td>
<td>TCP</td>
<td>Between appliance and directory server</td>
</tr>
<tr>
<td>443/10443 (redirect from 80)</td>
<td>End User Web Quarantine</td>
<td>HTTPS</td>
<td>TCP</td>
<td>Between appliance and intranet (configurable)</td>
</tr>
<tr>
<td>5432</td>
<td>Database functions</td>
<td>Encrypted SQL</td>
<td>TCP/UDP</td>
<td>Between clustered appliances</td>
</tr>
<tr>
<td>18080</td>
<td>Admin UI and clustered UI functions</td>
<td>HTTPS</td>
<td>TCP</td>
<td>[Required] Between appliance and intranet</td>
</tr>
<tr>
<td>8888</td>
<td>Delay Queue</td>
<td>DB Sync</td>
<td>TCP</td>
<td>Inbound/outbound Delay Queue database sync between clustered appliances</td>
</tr>
</tbody>
</table>

### Changing the Disk Size

1. Click the red “stop” icon on the toolbar. You are prompted to confirm that you want to power off. Click Yes. The progress is displayed in the Recent Tasks window.

2. Select Inventory > Virtual Machine > Edit Settings. The Virtual Machine Properties dialog box is displayed.


4. From the New Size drop-down list, select a number in GB that the virtual appliance will occupy on the ESX server.

5. Click OK.

6. On the toolbar, click the green arrow icon to power on the appliance. The status is displayed in the Recent Tasks window.

### Changing Memory Allocation

1. Click the red “stop” icon on the toolbar. You are prompted to confirm that you want to power off. Click Yes. The progress is displayed in the Recent Tasks window.

2. Select Inventory > Virtual Machine > Edit Settings. The Virtual Machine Properties dialog box is displayed.

3. On the Hardware tab, select Memory.

4. Use the slider or directly edit the number in the MB text box. Do not exceed 4GB of memory because that is the maximum the operating system of the virtual appliance can use.
5. Click **OK**.

6. On the toolbar, click the green arrow icon to power on the appliance. The status is displayed in the **Recent Tasks** window.

**Related concepts**

*Initial Configuration* (page 9)
4 Initial Configuration

Follow the steps in this section in the order shown to complete initial activation and configuration of the Email Appliance. Once activation is successfully completed, the step-by-step Setup Wizard launches. Using the wizard, you can configure the time zone and networking elements of the Email Appliance. The appliance registers with Sophos to retrieve the latest software and threat definitions from Sophos. You can then set the initial mail routing and filtering options.

4.1 Activating the Email Appliance

1. Using a supported web browser, connect to: https://172.24.24.172
   
   The Activation page is displayed.

   ![Activation Page]

   Enter the activation code emailed to you by Sophos:

   e.g. 0AYEXT-3KXO4Q-XNAWF2-DID0034JBDIEF9922F8928F829910222

   Start a 30-day limited functionality trial

   Contact Sophos Sales to get an activation code to start a fully functional evaluation or to purchase a license

2. Enter the activation code contained in an email message from Sophos, or if you are installing the appliance as a 30-day trial, click Try Now.
   
   The login page is displayed.
3. Enter an administrator username.
4. Enter and confirm an administrator password.
5. Click Login.
   Configuration begins with acceptance of the license agreement. Once you have accepted the agreement, the wizard’s Network Interface page is displayed.

4.2 Network Interface

The Email Appliance’s network settings and name servers are configured on the Network Interface page of the wizard.
To configure network interface settings:

1. In the **Network settings** section, do one of the following:
   - **To configure network settings with DHCP**: Accept the default DHCP option.
   - **To configure a static IP address**:
     a) In the **IP Address** text box, enter the address for the appliance.
     b) In the **Default Gateway** text box, enter the address of an external gateway server.
     c) In the **Network Mask** text box, enter the mask (for example, 255.255.0.0).
     d) [Optional] Click **Advanced** to open the **Additional Network Routes** dialog box, and configure an alternative gateway for traffic that is not routed through the default gateway.

2. From the **Speed and duplex** drop-down list, accept the **Auto** option. (If you select another setting from the drop-down list, it must match the speed of your managed switch to ensure that the Email Appliance operates correctly.)

3. In the **Name servers** section, do one of the following:
   - Select **Obtain DNS servers automatically**.
• Select **Specify the DNS servers**. Then, in the **Primary DNS IP** text box, enter a DNS IP address. Optionally, enter secondary and tertiary addresses.

4. Click **Next** to proceed to the wizard’s **Hostname and Proxy** configuration page.

### 4.3 Hostname and Proxy

You must assign a hostname for the Email Appliance. Additionally, if you plan to connect to the internet via a proxy server, you must assign a server address and port number for that server.

1. In the **Fully qualified hostname** text box, enter the host and domain name for the Email Appliance. An example entry is shown beneath the text box.

2. In the **Proxy server configuration** section, do one of the following:
   - If you plan to connect to the internet directly, accept the default setting.
   - If you plan to connect to the internet via a proxy, select **Connect through a proxy server**, specify a **Server Address** using a hostname or IP address, and specify a **Port**. Optionally, assign a username and password for the proxy server.

3. Click **Next** to proceed to the wizard’s **Network Connectivity** page.
4.4 Network Connectivity

With network configuration complete, the Email Appliance will now apply and test the network configuration and its connection to Sophos. If there are any errors, you will be prompted to review and modify the network configuration.

Note
Before proceeding, it is important to ensure that your appliance’s ethernet ports are not connected to the same network. If they are connected to the same network, you will see a warning that the network interfaces are cross-wired.

When the test has completed successfully, click **Next** to proceed to the wizard’s **Software Updates** page.
4.5 Register and Update

The Email Appliance will now use the activation code to register with Sophos. Once registered, the Email Appliance is authorized to receive threat definitions and software updates.

• To register the appliance:
  a) In the **Activation code** text box, enter the code provided by Sophos. (If you are installing the appliance as a 30-day trial, this text box is not displayed.)
  b) Click **Register**.
     If registration is successful, a message is displayed in the status bar.
  c) Click **Next**.

• To get the latest threat definitions and software updates:
  a) Click **Update**.
b) Click **Reboot**.
c) Following the reboot, click **Next** to proceed to the wizard’s **Clustering** page.

### 4.6 Clustering

**Note**
This is an optional step. If you do not intend for this appliance to be part of a cluster, click **Next** to proceed to the wizard’s **Time Zone** page.

Configuring clustering is only an option if you have two or more Sophos appliances. The appliances must also have identical software versions, be connected to the same network, and have the ability to communicate via port 24 over both UDP and TCP.

To configure clustering:

1. Select the **I would like this appliance to become part of a Sophos Email Appliance cluster** check box.
2. Enter the **IP or hostname** of another appliance.
3. Click **Next**.
   Messages are displayed, indicating that clustering has been configured.
4. If you want a paper copy of the configuration summary, click **Print**. Then click **Finish**.
   The Email Appliance Dashboard is displayed.

### 4.7 Time Zone

1. From the drop-down list, select the appropriate time zone for your region.
2. In the **Network Time Server** text box, enter the hostname of the Network Time Protocol (NTP) server from which you want to read the precise time of day or accept the default entry. This text box cannot be blank.

3. Click **Next** to proceed to the wizard’s **Mail Delivery Servers** page.

### 4.8 Mail Delivery Servers

In this step you define the internal mail server(s) that the Email Appliance can use to route incoming email.

To specify mail delivery servers:

1. In the **Address** text box, enter the name(s) of the mail delivery server(s).
2. Leave the **Port** set as **25**.
3. Set the **DNS Type** to **A** or **MX**.

**Note**

DNS type “A” means that the appliance will query the value in the **Hostname** field by address, conducting an “A” record query. The other option is “MX”, which results in an MX query of the value in the **Hostname** field. Most internal mail transfer agents have no specific MX record of their own so it is usually preferable to select **A**.

4. Click **Add** after each entry.
   Entries are displayed in the **Mail Delivery Servers** list. To remove a server from the list, select the check box beside the entry, and click **Delete**.

5. When you have finished adding servers, click **Next** to proceed to the **Incoming Mail Domains** page of the wizard.
4.9 Incoming Mail Domains

In this step you define the machines to which inbound mail for specific domains will be routed.

To specify incoming mail domains:

1. In the **Domain name** text box, enter the domain for which the Email Appliance will accept mail.

2. On the **Sub-domains** drop-down list, select **Yes** or **No**, depending on whether you want the host to accept mail bound for sub-domains as well.

3. On the **Deliver to host** drop-down list, enter the IP address of the machine.

4. Click **Add** after each entry.

   Entries are displayed in the **Mail accepting domains** list. To remove an entry from the list, select the check box beside the entry, and click **Delete**.

5. When you have finished adding servers, click **Next** to proceed to the wizard’s **Internal Mail Hosts** page.
4.10 Internal Mail Hosts

Mail relays are the hosts permitted to use the Email Appliance to relay email to the internet. To specify internal mail hosts:

1. In the text box for mail relays, enter the fully qualified hostname or IP address.

2. Click Add after each entry to add the hostname or IP address to the Internal host list. To delete a mail host, select the check box beside the entry, and click Delete.

3. When you have finished adding servers, click Next to proceed to the wizard’s Anti-Virus Settings page.

4.11 Anti-Virus Settings

You can accept the default anti-virus settings, or configure advanced settings for inbound and outbound mail. The default anti-virus settings discard viruses, add a warning banner to encrypted
and unscannable attachments, quarantine suspicious attachments before removing them, and add a warning banner.

To configure anti-virus settings:

1. Choose one of the following basic configuration options for anti-virus filtering:
   - To accept the default settings: Leave Default Anti-Virus Settings selected, and click Next to proceed directly to the wizard’s Anti-Spam Settings page.
   - To configure advanced settings: Select Advanced Configuration, and click Next to proceed to the configuration pages for inbound and outbound anti-virus settings.

There are five threat categories that apply to both inbound and outbound messages:

- **Viruses**: Messages containing known viruses. By default, messages containing viruses are discarded for all users. A notification is not sent and no banner is added.

- **Unscannable Attachments**: Messages with attachments that cannot be scanned (for reasons other than encryption). By default, unscannable attachments are delivered to all users. A banner is added advising users that the message is not guaranteed to be virus-free and should not be opened unless it is an expected message.

- **Encrypted Attachments**: Messages with attachments that could not be scanned specifically because of encryption. By default, encrypted attachments are delivered to all users. A banner is added advising users that the message is not guaranteed to be virus-free and should not be opened unless it is an expected message.

- **Suspect Attachments**: Messages with attachment types that are likely to contain viruses. By default, for all users, messages with suspect attachments are quarantined, the attachments are removed, and the messages are delivered. A banner is added advising users that potentially dangerous attachments were identified and removed. A list of attachment types can be configured by clicking the Suspect Attachments link.

- **Restricted Attachments**: Allows administrators to create a customized policy for blocking messages with specific kinds of attachments. By default, for all users, messages with restricted attachments are quarantined, the attachments are removed, and the messages are delivered. A banner is added advising users that potentially dangerous attachments were identified and removed. A list of attachment types can be configured by clicking the Restricted Attachments link.

2. On the Anti-Virus Inbound Advanced and Anti-Virus Outbound Advanced pages, from the Take action drop-down list, select an action for each threat category. Different actions are available for each threat category, depending on the severity of the threat (for example, the Deliver and Reject actions are not available for the Viruses rules).
   - **Deliver**: Deliver the message intact to the recipient.
   - **Quarantine**: Isolate the message in a quarantine.
   - **Reject**: Discard the message and send a “bounce-back” message to the sender advising that the message has been disallowed.
   - **Discard**: Discard the message without notice.
   - **Quarantine and deliver**: Send a copy of the message to the quarantine and deliver a copy to the recipient.
   - **Quarantine, drop file(s) and deliver**: Send a copy of the message to the quarantine and deliver a copy to the recipient with the relevant attachments removed.
   - **Drop file(s) and deliver**: Deliver the message to the recipient with the relevant attachments removed.
   - **Tag subject and deliver**: Deliver the message to the recipient with a modified subject that indicates the threat.
Figure 1: Anti-Virus Inbound Advanced
3. Select Notify and Banner settings for each threat category by clicking the hyperlinked text in the Notify and Banner columns. Configure using the options available in the pop-up dialog boxes.
   - **Notify**: Copy a specified recipient using Cc or Bcc, as specified in the Notify dialog box, whenever this policy rule is triggered. If instead you select the Redirect to option, the notification is delivered to the specified address only. If such a notification is added to a threat category (e.g. Encrypted Attachments) for which the action involves delivery, the message itself is also redirected to the specified recipient. The original intended recipients receive nothing. You can add a notification message for each of the three Notify options. Viruses are automatically removed from redirected messages.
   - **Banner: [Inbound messages only]** Attach disclaimers or other notifications to messages to alert users. Banners can be customized for each policy rule.

4. Click **Next** to move from Anti-Virus Inbound Advanced to Anti-Virus Outbound Advanced. When you have finished configuring advanced anti-virus settings, click **Next** to proceed to the wizard's Anti-Spam Settings page.
4.12 Anti-Spam Settings

For evaluation or full implementation, the appliance can be configured in one of three anti-spam modes: Passthrough mode, Pilot mode, and Full mode. The first two modes are intended for testing only.

To configure anti-spam settings:

1. Select one of the three modes:

   - **Passthrough mode** [Default]: In this mode, you can use the results to gauge the Email Appliance’s effectiveness. End users will not be aware that the Email Appliance is in operation, yet it will gather spam statistics and copy identified spam to the quarantine. While in Passthrough mode, the Email Appliance still actively identifies and blocks email-borne virus and malware threats.

   - **Pilot mode**: This mode allows you to filter messages for a select group of users. This way, you can test the effectiveness of the appliance on a small set of email addresses before deploying the appliance for a larger group of end users. You enter the email addresses for the test group using the **Group Editor** dialog box.

     **Important**
     If you select either **Passthrough mode** or **Pilot mode** for testing, you must modify the policy when testing is complete to make full use of the appliance’s spam protection. See the “Anti-Spam” section of the Policy documentation for more information.

   - **Full mode**: This setting prepares the appliance for production mode, with the default anti-spam rules applied for all users.
2. Choose one of the following basic anti-spam configuration options:
   - *To accept the default settings:* Leave **Enable default anti-spam settings** selected, and click **Next** to proceed directly to **Appliance Alerting**.
     
     Or

   - *To configure advanced settings:* Select **Advanced Configuration**, and click **Next** to proceed to the configuration page for advanced anti-spam settings.

The **Anti-Spam Inbound Advanced** page allows you to configure different actions for messages with high and medium spam scores.
3. Using the Take Action drop-down lists for **High Spam Scores** and **Medium Spam Scores**, select from the following list of actions:

   - **Continue Processing**: Message continues to be processed by the policy.
   - **Deliver Immediately**: Deliver the message intact to the recipient.
   - **Quarantine**: Isolate the message in a quarantine.
   - **Discard**: Discard the message without notice.
   - **Quarantine, tag subject and continue**: Send a copy of the message to the quarantine, and tag the subject line of the message with the specified text, after which the Email Appliance will continue to process the message.
   - **Tag subject and continue**: Tag the subject line of the message with the specified text, after which the Email Appliance will continue to process the message.

4. When you have finished configuring advanced anti-spam settings, click **Next** to proceed to **Appliance Alerting**.
4.13 Appliance Alerting

The Email Appliance is a mail relay that requires its own postmaster address. However, this can be aliased to another address in the domain. Also, quarantine email summaries will use the postmaster address as their sender’s address.

The Email Appliance is a self-monitoring appliance that sends email notifications of system warnings and critical events to administrators and Sophos Technical Support. Notifications are sent to the email addresses specified in the Alert Recipients list.

1. To configure the postmaster account: In the Enter a postmaster address text box, enter the postmaster email address to alias the postmaster account of this relay to the postmaster account of the email domain it is routing. The quarantine email summaries will use the postmaster address as their sender’s address.
2. To configure alert recipients:
   a) In the **Local alert contacts** text box, enter the recipient email addresses.
   b) Click **Add** after each entry.
      Entries are displayed in the list of alert contacts.
      • To remove an alert recipient from the list, select the check box beside the entry, and click **Delete**.
3. When you have finished adding notification addresses, click **Next** to proceed to the wizard’s *Appliance Support Contact* page.

### 4.14 Appliance Support Contact

The *Appliance Support Contact* page prompts you to provide information that Sophos Technical Support can use to contact you if there is ever a critical problem.

To provide contact information to Sophos Technical Support:

1. Select the **Activate Appliance Support Alerts** check box. The grayed out features below become available.
2. For **Critical alerts**, provide the **Name** and **Email** of the person who should receive these messages.
3. For **Non-critical alerts**, provide the **Name** and **Email** of the person who Sophos should contact.
**Note**

A *non-critical alert* indicates a transient error that Sophos would like to investigate. These alerts do not indicate a problem with web filtering.

4. Click **Next** when you are finished.
   The initial configuration is now complete, and you can view a summary of your settings on the final page of the wizard.

**Related tasks**

Summary Page  (page 30)

### 4.15 Summary

The **Summary** page allows you to review and, optionally, modify settings configured in the wizard.

You should confirm that all of the settings displayed on this page are correct.
• If you need to change or update any of the settings, click the **Edit** button in the appropriate section to access associated configuration items.

**Note**
If you have not provided **Appliance Contact Support** information, contact support information will be not be displayed in the **Appliance Alerting** section of the summary page.

• When you have finished reviewing the settings, click **Finish** to proceed to the **Configuration Homepage**.

**Related concepts**
**Post-Installation Configuration/Integration**  (page 32)
5 Post-Installation Configuration/Integration

Activation and initial configuration bring the Email Appliance to a state where it can filter and deliver mail; however, it can be further integrated with, and customized for, a specific environment. Enabling features such as the Email Appliance’s directory services, user preferences, and advanced mail-routing functionality allow the Email Appliance to integrate more closely into a given environment and offer functionality beyond standard mail-filtering and delivery.

Immediately after you exit the setup wizard, the Dashboard tab of the appliance’s administrative interface is displayed.

To view and edit the list of post-installation tasks:

1. In the System Console section, click Post Configuration Checklist.

   The Configuration Homepage is displayed.

   On the Quick Tasks sidebar are number of items, some of which have “close” (x) buttons beside them. Each item is also accompanied by an icon that indicates whether a task is complete (green check mark) or incomplete (yellow exclamation mark).

2. Click on a task description to open the configuration page for that task.

3. When you have finished configuring a task, click Configuration on the Navigation bar to return to the Configuration Homepage.

4. Click the “x” button to remove a task from the Quick Tasks list.

When these changes have been made, or if no changes are necessary, these items can be cleared by clicking the “x” to the right of each link. Once all the tasks have been cleared, the Post-Configuration Checklist link on the Dashboard tab disappears.
5.1 Testing Appliance Mail Flow

Once you have finished setting up your Email Appliance as described in the Configuration Guide, it is recommended that you confirm its effectiveness by sending test messages.

The method of testing depends on how your network is configured and how you plan to put your appliance(s) into production.

If you have already configured your network to route mail through an appliance, you can send test messages to and from an external email client (for example, Gmail). If, however, the appliance is configured but not yet integrated with your network, you can still use an internal mail client to deliver test messages through the appliance. The two test options are illustrated below.
Testing a Fully Networked Appliance

1. External Mail Client
2. Internet
3. Email Appliance
4. Mail Delivery Agent (For example, Microsoft Exchange Server)
5. Internal Mail Client

To confirm that your Email Appliance is processing mail, you can send a test message from an account (1) outside of your network and check the recipient inbox (5) and the mail logs to see if it was received and if it was routed through the appliance (3). You can then confirm that the appliance is routing mail to locations outside of your network by sending a message from an internal email client (5) and performing the same checks.
Testing a Pre-Deployment Appliance

To confirm that your Email Appliance is processing mail, you can send a test message from a mail client configured to route mail through the appliance (1) to a recipient address belonging to an appliance user group (4). Then check the recipient account and the mail logs to verify that the message was processed and delivered.

5.1.1 Testing Mail Flow on a Fully Networked Appliance

The following procedure assumes that you have set up your Email Appliance as described in the Configuration Guide. If your organization has a firewall, you must also have configured access on all of the essential ports described in the Setup Guide.

Note
If you have yet to integrate the Email Appliance into your network, use the “Testing Mail Flow Before Deployment” procedure instead.

To test mail flow on a fully networked appliance:

1. From an email account outside of your network (for example, a Gmail account), send a test message to an internal address that is configured to have mail filtered by the Email Appliance. This allows you to confirm that the appliance is successfully routing incoming mail to destinations within your network.

   It is recommended that you give the message a subject that can be easily spotted when you search the mail logs in the next step.
2. To confirm that the message has been delivered:
   a) Check the internal email account to verify that the message was received.
   b) Inspect the mail logs for an entry that corresponds with your test message. On the Search tab, on the Search In sidebar, select Mail Logs, and click Search.

3. From an internal email account configured to route mail through the Email Appliance, send a test message to an external email address. This allows you to confirm that the appliance is successfully routing mail to destinations outside of your network.
   It is recommended that you give the message a subject that can be easily spotted when you search the mail logs in the next step.

4. To confirm that the message was received:
   a) Check the external account to verify that the message was received.
   b) Inspect the mail logs for an entry that corresponds with your test message. On the Search tab, on the Search In sidebar, select Mail Logs, and click Search. For more about searching mail logs, see “Search” in the product documentation.

**Related tasks**
Testing Mail Flow Before Deployment (page 36)

**Related information**
Configuration of Ports
Email Appliance Configuration Guide
Search

### 5.1.2 Testing Mail Flow Before Deployment

The following procedure assumes that you have set up your Email Appliance as described in the Configuration Guide. If you want to test the appliance before it is fully integrated with your network, you can send test messages as described below.

**Note**
If you have already integrated the Email Appliance into your network, use the “Testing Mail Flow on a Fully Networked Appliance” procedure instead.

To test mail flow before deployment:

1. From an email client configured to route mail through the Email Appliance, send a test message from an internal email account to an address belonging to an appliance user group. This confirms that the appliance is successfully processing mail.
   It is recommended that you give the message a subject that can be easily spotted when you search the mail logs in the next step.

2. To confirm that the message has been delivered:
   a) Check the recipient account to verify that the message was delivered.
   b) Inspect the mail logs for an entry that corresponds with your test message. On the Search tab, on the Search In sidebar, select Mail Logs, and click Search. For more about searching mail logs, see “Search” in the product documentation.

**Related tasks**
Testing Mail Flow on a Fully Networked Appliance (page 35)
5.2 Configuring Directory Services

Note
This section only applies if you plan to use the Email Appliance in conjunction with an LDAP server. Although Active Directory is the most common, the Email Appliance can be integrated with other LDAP implementations. If you will not be using any form of LDAP, proceed to Configuring User Preferences.

Directory Services integration enables the mapping of users and groups defined on an LDAP server to the Email Appliance’s email policy, recipient validation and user authentication. Initially, email policy rules on the Email Appliance are applied globally; however, you can customize those rules and map them directly to groups defined in the Email Appliance or in directory services.

This allows the Email Appliance to integrate with a particular environment more quickly and tightly by taking advantage of existing definitions and making it possible to administer them from one place. In addition, directory services can be used for email recipient validation and authentication for user preferences.

The Email Appliance can automatically detect the directory services schema and configuration parameters, or they can be manually configured.

To configure directory services:

2. Click Add to launch the Directory Services wizard, and use the wizard to configure your directory server(s). See the “Directory Services” documentation for more information.
3. On the Navigation bar, click the Configuration button at the top of the page to return to the Configuration Homepage.
4. Click the ‘x’ button to the right of Directory Services. Now that directory services are set up, you are ready to configure End User Preferences.

5.3 Configuring User Preferences

User preferences allow email recipients to securely manage their quarantined spam, opt in and out of spam checking, and customize their own lists of allowed and blocked senders. Administrators control which of these options, if any, are available to users. For example, it may be prudent in many organizations to prevent users from opting out of anti-spam protection. Administrators can also set the users’ default interface language, the delivery of email quarantine summaries, and the format and delivery frequency of these summaries.

On the Accounts: User Preferences page, you can configure user options, such as whether users have web access to manage their quarantined messages and whether users receive email summaries of their quarantined messages. When the quarantine summary option is enabled, users receive an email message at a regularly scheduled time that lists all messages that were quarantined by the Email Appliance. Users can then respond to the summary message to release or delete their quarantined messages. Users can opt out of receiving email summaries by disabling this feature via the End User Web Quarantine.
Note
Options on the **Accounts: User Preferences** page can be configured individually, but you must click **Apply** after configuring preferences to make the settings take effect.

To configure user preferences:

1. On the **Quick Tasks** sidebar of the **Configuration Homepage**, click **End Users**.
   The **Accounts: User Preferences** page is displayed.
2. Select the **Enable web quarantine access** check box to grant users access to a web page on which they can manage their own quarantined messages and set anti-spam options.
3. Select one of the following authentication options:
   - **Directory services**: You must have directory services server access configured to use this option. For instructions, see the previous section (**Configuring Directory Services**). With this method, users log in by entering an assigned username and password.
   - **Custom list**: Create the list by clicking the associated **Define users** button, which opens the **Email/Password List** dialog box. When using this method, you must supply users with the email/login and password they will need to log in to the End User Web Quarantine.

   With both of these options, users log in by pointing their browsers to the Web Quarantine address (**http://<host>.<domain>**).

Note
If you use multiple LDAP servers that contain duplicate usernames, the Email Appliance will automatically authenticate each user and grant access to the correct End User Web Quarantine account.

4. Select any of the following options that you want to grant to users:
   - **Enable allow/block lists**: Allow users to create and use personalized allow and block lists for hosts and senders.
   - **Allow wildcard usage in allow/block lists**: Let users use wildcards when defining their personalized allow and block lists for hosts and senders.
   - **Allow users to opt-out of spam checking**: Allow users to bypass spam-checking of their messages.

5. On the **Default user interface language** drop-down list, select the users’ preferred language. Users also have the option of personalizing the language via an option in the End User Web Quarantine.

6. Under **Configure end user service**, click **Configure**.

7. In the **Configure End User Web Quarantine** dialog box, select the HTTPS port numbers used by the SPX Secure Email Portal (if enabled) and the Web Quarantine. Choose between ports 443 and 10443. Whichever port you choose for either service, the other available port is automatically selected for the remaining service.

8. Click **OK**.

9. **[Optional]** Configure automated emailing of quarantine summaries:
   a) Select **Enable email quarantine summary** to email users summaries of their quarantined email messages.
   b) Under **Schedule**, click **Configure**.
   c) In the **Advanced Email Quarantine Summary Schedule** dialog box, use the option buttons and drop-down lists to set the appropriate time(s).
d) Click OK.

10. [Optional] To set banner options for email quarantine summaries, select the Add header or Add footer check box, and enter the content for the banner (the note inserted into the top or the bottom of the message body) in the associated text box. By default, the following text is displayed in the Add header text box:

The following messages were quarantined by Sophos because they appear to be spam. To request that a message be released from the quarantine and delivered to you, click the message ID and send the request. If your mail client does not support HTML, reply to this message and delete lines that correspond to messages you do not want approved. To release all messages in the list, simply reply to this message.

11. When finished configuring user preferences, on the Navigation bar, click the Configuration button. You are returned to the Configuration Homepage.

12. Click the ‘x’ button to the right of End Users.

Now that end user preferences are configured, you are ready to proceed to the Internal Mail Hosts/Outbound Proxy task.

5.4 Configuring Internal Mail Hosts/Outbound Mail Proxy

Note
These steps are only required if your organization has outbound mail relays (internal mail hosts) located between the Email Appliance and the internet. If not, you can clear this task and proceed to the Trusted Relays task.

Organizations with more complex email architectures may also require a more advanced internal mail hosts configuration. These organizations may have internal mail hosts between the Email Appliance and the internet. Settings for these outbound relays and the proxy are configured on the Routing: Internal Mail Hosts page.

If your organization routes all outgoing mail through a proxy server, you must also specify the hostname and port of that server on the Routing: Outbound Mail Proxy page.

1. To configure the internal mail host(s):
   a) On the Quick Tasks sidebar of the Configuration Homepage, click Internal Mail Hosts. The Routing: Internal Mail Hosts page is displayed.
   b) In the Internal mail hosts text box, enter the fully qualified hostname or IP address of each machine approved to send email from your organization. Click Add after each entry.

2. [Optional] To configure a proxy server:
   a) On the Quick Tasks sidebar of the Configuration Homepage, click Mail Proxy. The Routing: Outbound Mail Proxy page is displayed.
   b) In the Hostname text box, enter the hostname or IP address, and specify the Port.
   c) In the DNS type drop-down list, select either MX or A.
Note
DNS A records are used for looking up hosts for most types of network connections (HTTP, FTP, etc). MX records are used specifically for email routing and can be used to specify multiple hosts (for example, for failover or load-balancing behavior). If the mail delivery server does not have an MX record in DNS, set DNS Type to A.

d) [Optional] Select **Enforce TLS** if the proxy server requires connection via TLS.

e) [Optional] Select **Authenticate using the following credentials** if the proxy server requires a username/password for authentication. If a username/password is required, it is strongly recommended that you select the check box described in step 5 (**Enforce TLS**). Without TLS enforcement, the information will be sent as plain text.

f) Click **Apply**.

3. On the Navigation bar, click the **Configuration** button.
   You are returned to the **Configuration Homepage**.

4. Click the ‘x’ button to the right of **Internal Mail Hosts** and **Mail Proxy**.
   You are now ready to proceed to the **Trusted Relays** task.

### 5.5 Configuring Trusted Relays

Note
These steps are only required if your organization has inbound mail relays located between the Email Appliance and the internet.

Some organizations have more complex email architectures, requiring more advanced inbound relay configuration. Such organizations may have one or more layers of relays external to the Email Appliance. The Email Appliance uses its trusted relays configuration to deal with such an environment. It is very important to specify any inbound relays that are external to the Email Appliance so that they are correctly factored into anti-spam analysis. Trusted relays are configured on the **Mail Routing: Trusted Relays** configuration page.

To configure trusted relays:

1. In the Quick Tasks sidebar of the **Configuration Homepage**, click **Trusted Relays**. The **Mail Routing: Trusted Relays** page is displayed.
2. In the **IP address** text box, enter the addresses of mail gateway servers that are located between the internet and the Email Appliance. Click **Add** after each entry.
   Entries are displayed in the **Trusted relay list**. To delete a trusted relay, select the check box next to the entry, and click **Delete**.
3. On the Navigation bar, click the **Configuration** button.
   You are returned to the **Configuration Homepage**.
4. Click the ‘x’ button to the right of **Trusted Relays**.
6 Email Security Appliance Policy

Introduction

Mail processing is configured on the Policy pages of the Email Appliance GUI. Email Appliance policy allows management of anti-virus, anti-spam, content, exception lists, and filtering options. Settings for inbound and outbound messages are configured independently. The policy defines what action to take based on the type of threat in the message. It also allows administrators to append notices to messages as banners and notify additional recipients.

The available actions for the different threats vary but may include:

- Deliver
- Quarantine
- Reject
- Discard
- Quarantine and deliver

The Policy sections have different levels of message management and threat protection, depending on the specific type of threat or message category within that policy section. You can also select the user group(s) affected by these settings, and you can select exceptions to the selected group(s).

User Groups

User groups are specified in the Email Appliance to apply different message-filtering options to different sets of users. User groups can consist of manually created groups or groups imported from Active Directory.

Groups defined in Active Directory can be imported by the Email Appliance and used to include or exclude users from specific policy rules. These groups are imported from Active Directory, cached locally on the Email Appliance, and then synchronized hourly. Groups that are manually defined on the Email Appliance can be applied to policy rules in the same manner.

Quarantine

The quarantine stores unwanted (spam or offensive content) or dangerous (virus-infected) messages. The policy can send a message to the quarantine using one of four actions:

- **Quarantine**: The message is sent to the quarantine and not delivered to the recipient.
- **Copy to Quarantine and deliver**: A copy of the message is sent to the quarantine and a copy is sent to the recipient.
- **Copy to Quarantine, drop file(s), and deliver (Anti-Virus)**: A copy of the message is sent to the quarantine, and a copy with the infected attachments removed is sent to the recipient.
- **Copy to Quarantine, tag subject, and deliver (Anti-Spam)**: A copy of the message is sent to the quarantine, and a copy with a modified subject line is sent to the recipient.
Anti-Virus Policy

The Email Appliance uses the Sophos Anti-Virus engine for virus protection. The Email Appliance checks for virus definition updates every 5 minutes. Updates are installed automatically so there is no need for administrative intervention.

Use the Policy: Anti-Virus page to configure the handling of messages containing known viruses, unscannable attachments, encrypted attachments, or suspect attachment types.

Except for the Viruses category, actions can be configured for a specific group in each of these threat categories:

- **Viruses**: Messages containing known viruses.
- **Unscannable Attachments**: Messages with attachments that cannot be scanned (for reasons other than encryption).
- **Encrypted Attachments**: Messages with attachments that could not be scanned specifically because of encryption.
- **Suspect Attachments**: Messages with attachment types that are likely to contain viruses. Click the Suspect Attachments link to configure a list of attachment types.
- **Restricted Attachments**: Allows administrators to create a customized policy for blocking messages with specific kinds of attachments. Click the Restricted Attachments link to configure a list of attachment types.

The threat categories above can be configured using the following options:

- **Take action**: The policy action taken on matching messages. Different actions are available for each rule, depending on the severity of the threat (e.g. the Deliver action is not available for the Viruses rules). These actions are:
  - **Deliver**: Deliver the message intact to the recipient.
  - **Quarantine**: Isolate the message in quarantine. The quarantine reasons used are "Virus", "Encrypted", "Cantscan", "Suspect", relating to the category that quarantined the message.
  - **Reject**: Discard the message and send a “bounce-back” message to the sender, explaining that the message has been disallowed. For outbound viruses only.
  - **Discard**: Discard the message without notice.
  - **Quarantine and deliver**: Send a copy of the message to the quarantine and deliver a copy to the recipient.
  - **Quarantine, drop file(s) and deliver**: Send a copy of the message to the quarantine and deliver a copy to the recipient with the relevant attachments removed.
  - **Drop file(s) and deliver**: Deliver the message to the recipient with the relevant attachments removed.
  - **Tag subject and deliver**: Deliver the message to the recipient with a modified subject that indicates the threat. The subject line is prepended with one of: [ENCRYPTED], [UNSCANNABLE], or [SUSPECT]. Tag and deliver is not an option for viruses.

- **To/From (Inbound and Outbound)**: Selects the users to whom the rule applies. The default value is all users. The Viruses category is not configurable.

- **Except**: Selects exceptions from the To/From list. The default is none.

- **Notify**: Copy additional recipients (using Cc or Bcc) or redirect the message to another address. An optional notification message can be added. Viruses are automatically removed from redirected messages.
• **Add Banner**: Attach disclaimers or other notifications to messages (inbound messages only). Banners can be customized for each policy rule.

The **Global** option enables scanning for viruses inside archives. It is recommended that this feature be enabled because, even though it may increase processing time on messages with large archive attachments, such messages constitute only a small percentage of mail, and the virus engine also has features that will protect it from unreasonably large attachments.

### Anti-Spam Policy

The Email Appliance uses the Sophos Anti-Spam engine for spam protection. The Email Appliance checks for updates to the anti-spam rules, sender reputation, and anti-spam engine every 5 minutes. Updates are installed automatically so there is no need for administrative intervention.

Use the **Policy: Anti-Spam** page to configure how to handle messages classified as spam. The anti-spam engine assigns a spam categorization to each message. The anti-spam engine determines the relative likelihood that a message is spam and classifies it as "not spam", "medium spam", or "high spam".

The **Policy: Anti-Spam** page allows you to handle **Mail with high spam scores** (almost certainly spam) differently from **Mail with medium spam scores** (very likely spam). For both of these message categories, four different actions can be configured. These actions can be applied to selected users and groups. The default is: one action, **Discard**, defined for high spam to all users, and one action, **Quarantine**, defined for medium spam to all users.

Each category (e.g. high spam) and action makes up an anti-spam policy rule. Each policy rule can be configured with the following options:

- **To**: Users to whom the rule applies.
- **Except**: Exceptions from the To list.
- **Take Action**: The policy action taken on the messages. Available actions are:
  - **Deliver**: Deliver the message intact to the recipient.
  - **Quarantine**: Isolate the message in quarantine. Messages are quarantined with the quarantine reason "High Spam" and "Medium Spam," depending on the category in which the action is set.
  - **Discard**: Discard the message without notice.
  - **Tag subject and deliver**: Deliver the message to the recipient with a modified subject indicating that the message contains spam. The subject is prepended with either [SPAM:HIGH] or [SPAM:MEDIUM].
  - **Quarantine, tag subject and deliver**: Send a copy of the message to the quarantine and deliver a copy to the recipient with a modified subject indicating that the message contains spam.

**Note**

It is possible to create overlapping groups in different rules within a spam category. In cases where a particular user or group is defined in more than one rule (where each row on the **Policy: Anti-Spam** page represents a rule), the action for the first matching rule in the list takes precedence. However, in most cases, it should be possible to avoid overlapping rules by specifying smaller sub-groups in the **Except** column.
Additional Policy

The Email Appliance has content options that allow administrators to manage inbound and outbound email with offensive and site-specific content. SophosLabs has engineered the Email Appliance to detect offensive content in both plain text and the obfuscated forms used by spammers or others who are trying to circumvent detection.

Administrators add to the Offensive Language list provided by SophosLabs, and they can configure an additional tests for inbound and outbound keywords. Site-specific content can be configured using both plain text strings and Perl-based regular expressions.

Use the Policy: Additional Policy page to configure handling of messages with offensive language or specified keywords. The Policy: Additional Policy page defines rules for inbound and outbound messages separately. The Global option is used to reject attachments that exceed a maximum size.

Under Inbound content and Outbound content are rules for Offensive Language and Keywords (Inbound and Outbound). The rule name, or part of the rule name is a link that opens the List Editor dialog box, allowing editing of the list used by that rule. The list editor lets you edit both plain text strings and regular expressions.

Each rule can be configured with the following options:

- **To** ("From" in Outbound content): Users to whom the rule applies.
- **Except**: Exceptions from the To list.
- **Take Action**: The policy action taken on the messages. Available actions are:
  - **Deliver**: Deliver the message intact to the recipient.
  - **Quarantine**: Isolate the message in quarantine. The quarantine reasons ‘Offensive’ and ‘Keyword’ are used.
  - **Discard**: Discard the message without notice.
  - **Quarantine and deliver**: Send a copy of the message to the quarantine and deliver a copy to the recipient.
  - **Tag subject and deliver**: Deliver the message to the recipient with a modified subject that indicates which policy rule was violated. The subject line is prepended with ‘[KEYWORD]’ or ‘[OFFENSIVE]’.
- **Notify**: Copy additional recipients (using Cc or Bcc) or redirect the message to another address. An optional notification message can be added.
- **Add Banner**: Attach disclaimers or other notifications to messages (inbound messages only). Banners can be customized for each policy rule.

Allow/Block Lists

Use the Policy: Allow/Block Lists page to configure lists that define which hosts and senders are trusted and which hosts and senders are not trusted. These sources can be entered as IP addresses, domains, or email addresses. Messages from Allowed Hosts/Senders will bypass anti-spam filtering. Messages from Blocked Hosts/Senders are blocked without being scanned for spam or content. Messages from administratively blocked senders are quarantined as spam; that is, the quarantine reason is "spam".
Note
Message relays known to be spam senders are included by the IP Reputation Filtering feature, which can be configured in the Policy: Filtering Options page. Allow/Block lists provide the ability to add information based on the experience of your organization.

Filtering Options

The Email Appliance has advanced filtering options that augment the protection of a gateway or perimeter device. Its position at the gateway gives the Email Appliance the unique opportunity to offer protection against denial of service (DoS) and directory harvest attacks (DHA) and allows early discard of messages from known bad senders. Use the Policy: Filtering Options page to set advanced mail security settings.

IP Reputation Filtering

SophosLabs has spam traps around the world that capture spam for analysis, allowing Sophos to monitor the capture rate and identify senders of spam. Messages from known bad senders can be blocked solely on the basis of sender reputation data from SophosLabs. Three options are available for this feature.

• **Enable connection-level blocking**: Rejects messages from known bad senders as soon as the sender information from the TCP/IP connection is received. This option is recommended when the Email Appliance is the outermost MTA because it significantly improves throughput by blocking spam early in the connection, before any of the message is received.

• **Enable policy-level blocking**: Rejects messages from known bad senders in the email policy. Although this option is slightly less efficient than connection-level blocking, policy-level blocking does still offer significant performance advantages, and the rejection is logged for reporting.

• **Disable blocking**: Disables the use of SophosLabs reputation data. This is not recommended unless your email policy mandates that you may not reject any messages.

Note
If your network has trusted local SMTP relays that relay inbound messages to the Email Appliance, these servers must be entered in the Trusted Relays list and policy-level blocking must be enabled to maximize the effectiveness of this feature.

Perimeter Protection

The Perimeter Protection option enables automatic denial of service (DoS) and directory harvest attack protection (DHA). This option activates MTA-level throttling, which rejects messages from mail relays that exceed the following limits:

• 50 simultaneous connections per relay
• 1000 connection attempts per relay per minute
• 1000 message delivery requests per relay per minute
• 5000 recipient addresses per relay per minute
Messages from such relays are rejected until traffic from that relay drops below the limit. This option should not be enabled in network configurations where the Email Appliance is not at the gateway (i.e. has trusted SMTP relays between the Email Appliance and the internet).

Optional Data Sharing

When enabled, the **Optional data sharing** option provides SophosLabs with data to help improve spam detection. This data could include proprietary, confidential, and user-identifiable content. This data, used solely to improve threat detection, ensures that SophosLabs receives all information that is critical to maintaining the Email Appliance’s defenses against evolving threats. It is highly recommended that you enable this option.

**Note**
By default, the Email Appliance also shares general, non-confidential data that SophosLabs uses to compile statistics about spam and IP reputation filtering. For further details regarding the Email Appliance data-sharing policy, contact your Sophos sales representative.
There is specialized functionality within user groups called alias maps. Alias maps are used to associate one email address with another email address or multiple addresses. Alias maps can consist of manually defined mappings or aliases created in Active Directory.

If email aliases have been created using the Alias map support feature or if email aliases have been configured inside Active Directory and Active Directory alias support is turned on, the Email Appliance applies these aliases for policy filtering and user preferences. For example, if you have an AD alias that redirects mail destined for FirstName.LastName@example.com to shortname@example.com or have manually created an alias that maps FirstName.LastName@example.com to shortname@example.com, the effects are as follows:

- **Policy Filtering**: Instances of FirstName.LastName@example.com are interpreted as shortname@example.com when messages are processed by the policy. Any explicit references to FirstName.LastName@example in the policy are ignored.

- **Quarantine Summaries**: If the Email Appliance is configured to email quarantine summaries, the summaries for FirstName.LastName@example.com are mailed to shortname@example.com only.

- **User Block Lists**: Messages addressed to FirstName.LastName@example.com, which are subsequently blocked, are stored in the Blocked Messages list for shortname@example.com.
8 System Maintenance

System Administration

The Email Appliance supports multiple administrative accounts for maintenance and administration. Accounts are configured as either a system administrator or a help desk administrator. System administrators have access to all system management tasks, including the ability to add or delete administrator accounts. Help desk administrators can access common tasks to offload work from system administrators. When logged in, help desk administrators can view the Dashboard, view and manage quarantined spam messages, generate reports, and access the Help system. (Note: Help desk administrators do not have access to the Sophos Support and About topics in the Email Appliance’s online Help.)

System Updates

The Email Appliance continuously updates the system software as well as the threat definitions used by the anti-virus and anti-spam engines. Threat definitions are applied immediately, while system software updates are applied during administratively configured maintenance periods. The software updates are either non-critical or critical. Critical software updates (e.g. security-related patches) are applied automatically within 24 hours of availability during the update period. Maintenance updates are applied automatically during the update time frame, but only on the days of the week specified by the administrator.

New threat definitions from SophosLabs (including anti-virus, anti-spam, and IP-blocking data) are automatically downloaded and installed every 5 minutes. The Email Appliance will send an alert to specified recipients if, for a period of 2 hours, it cannot contact Sophos to check for updates to the threat definitions. The Email Appliance displays the following information about threat definitions and their update status:

- **Status**: Status of the automatic updates (turns red if the Email Appliance is unable to connect to Sophos).
- **Installed**: Version number of the current threat definitions.
- **Last updated**: Date and time of the most recent update.

System software updates (including critical and maintenance updates) are installed automatically. It is possible to delay installation for a limited time so that the updates may be installed manually, using the **Update Now** button. Updates can also be manually installed prior to an update period. The Email Appliance displays the following information about software updates:

- **Status**: Status of the update scheduler (turns red if the Email Appliance is unable to connect to Sophos).
- **Installed**: Version number of the currently installed software.
- **Available**: Version number of the software currently available on the Sophos update site.
- **Update details**: Version number of the available update (if an update is available).
- **Auto update schedule**: Date and time that an available update will be installed if no manual update is performed. If no update is available, this field is blank.
- **Last updated**: Date and time of the most recent update.
9 Contact Sophos

Sophos Technical Support

If you encounter a problem with your Sophos product or it does not function as described in the documentation, contact Sophos Technical Support: http://www.sophos.com/support/.

Corporate Contact Information

To contact your local Sophos office, see: https://www.sophos.com/en-us/company/contact.aspx
10 Copyrights and Trademarks

Copyright 2000-2019 Sophos Limited. All Rights reserved.

Sophos, Sophos Anti-Virus and SophosLabs are trademarks or registered trademarks of Sophos Limited. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the license terms or you otherwise have the prior permission in writing of the copyright owner.