SOPHOS

simple + secure

Email Security Appliance Help

Contents

About Your Email Appliance

The Sophos™ Email Appliance offers the best and most reliable gateway protection, while setting a new standard for effective and efficient management. Sophos appliances draw on twenty years of experience in enterprise threat management, delivering world-class threat protection in a compact and easy-to-manage format.

The Sophos Email Appliance extends the power and performance of Sophos gateway security software into the appliance form-factor. Sophos appliances provide award-winning integrated threat management and a superior overall customer experience to deliver powerful, effective and reliable gateway solutions for the enterprise.

Email Appliance Features

Enterprise-scale solution for organizations with up to 25,000 users

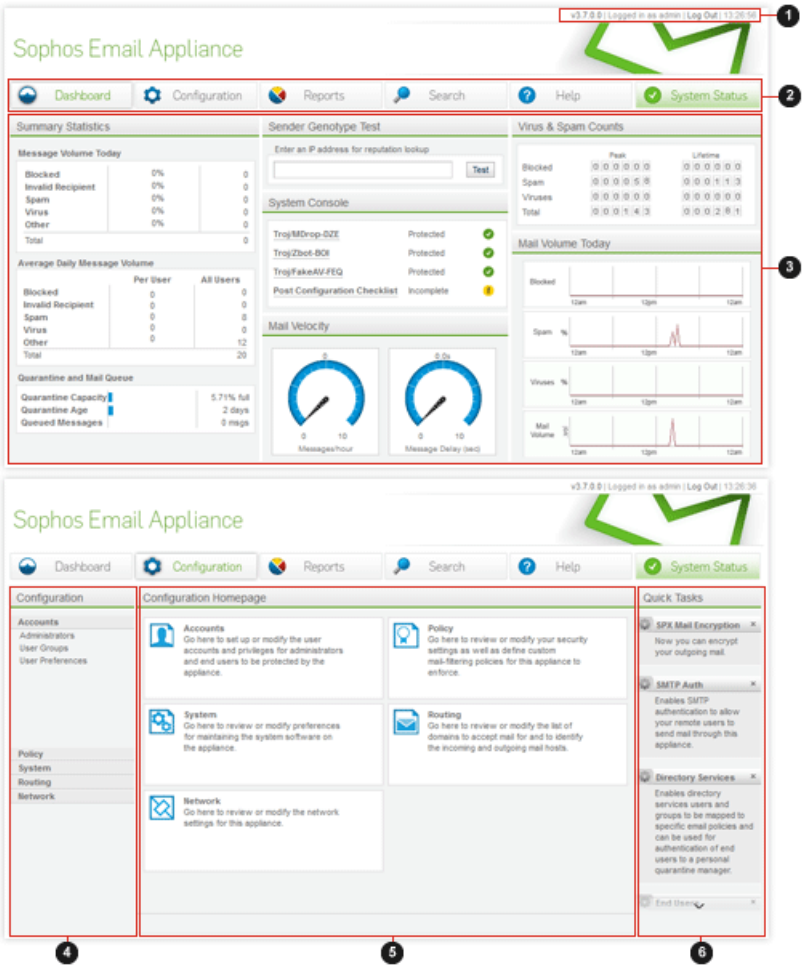
- **On-Board Quarantine**: The email quarantine resides on the same appliance where the mail is filtered, translating into fewer infrastructure requirements, easier message handling, and a lower total cost of ownership.
- **Powerful Message Tracking**: A multi-parameter search capability for tracking messages in system logs and quarantine means that it's easy to find and retrieve messages or trace their routing, with less time spent searching for lost emails.
- **Powerful Dashboard**: Offers quick and comprehensive appliance management, monitoring and reporting, making it easy to execute key tasks and run key reports.
- **Built-In Hardware Redundancy**: The ES4000, ES5000 and ES8000 come with dual hard drives, power supplies and processors. Administrators can be confident that vital email systems will remain running.

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, providing an integrated, hardened, and reliable system.
- **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.
- **Sender Genotype service**: Employs connection management technology to block email from bad senders. Includes traditional IP reputation filtering as well as proactive connection control, which blocks suspicious hosts. Sender Genotype eliminates up to 85% of inbound spam, substantially increasing message throughput without the need for additional infrastructure investments.
- **Real-Time Remote System Monitoring**: Sophos continuously monitors the system health and status of all installed appliances to guarantee that your appliance is always up to date and functioning properly.

- **On-Demand Remote Assistance**: A customer-enabled Secure Shell (SSH) connection provides Sophos Technical Support with direct access to individual appliances for specific troubleshooting.
- **Superior Support**: Award-winning web-based, email and live telephone support available 24/7/365.

The Email Appliance User Interface



The Email Appliance user interface includes the following components:

❶ The Status Information bar shows the following (from left to right):

- **Remote Assistance session established** is displayed while an outbound SSH connection to Sophos Technical Support is open.
- **Version number** of the currently installed software.
- **Logged in as <username>** is displayed, indicating the username of the current user.
- **Log Out** can be clicked to exit from the Email Appliance user interface.
- The current time in 24-hour format.

❷ The Navigation bar is used to access the **Dashboard**, **Configuration**, **Reports**, **Search**, **Help** and **System Status** tabs.

❸,❺ The Content pane displays the pages of the Email Appliance user interface.

❹ The Navigation sidebar only appears on the **Configuration**, **Reports**, and **Search** tabs. Click the links on this sidebar to view the various configuration and reports options in the **Content** pane or, on the **Search** tab's sidebar, fill in the text boxes to perform a search.

❻ The **Quick Tasks** sidebar only appears on the **Configuration** tab. Click any of these links to perform common configuration tasks.

Note: The interface for the Email Appliance is optimized for the latest supported browsers.

Getting Support

Sophos Email Appliances are equipped with advanced monitoring and assistance technologies that deliver a superior customer support experience. Every installed appliance is kept up to date and at its operational peak, with minimal administrative involvement. Using embedded technology, Sophos appliances communicate with Sophos Technical Support every five minutes, automatically receiving anti-virus and anti-spam updates and optionally reporting on hardware health and protection status.

If required, you can send a support request directly from within the Email Appliance. Click the **Help** button. Then, on the sidebar, click **Sophos Support**.

Sophos appliances also feature optional remote assistance via a secure, reverse tunnel SSH connection. This lets customers grant Sophos Technical Support direct remote access to their appliance for faster support resolution. Contact *Sophos Technical Support* before enabling remote assistance.

Note: If you use your appliance in a clustered configuration, the reverse SSH connection will open to whichever system you are currently logged into.

Active monitoring delivers automatic alerts on protection status, license validity and one-click renewal/activation to system administrators.

Hardware Support

All appliances carry a standard Advanced Replacement Warranty. Sophos will initiate the replacement within two hours of a confirmed failure. Next-day delivery (not including delays from international Customs clearing, if required) will occur according to the following cut-offs, Monday through Friday:

Customer Region	Local Cut-off Time
United States, Canada	12:00 (Boston, USA)
United Kingdom, EMEA	12:00 (London, UK)
France and Spain	13:00 (Paris, FR)
Germany, Switzerland and Austria	13:00 (Frankfurt, DE)
Italy	13:00 (Milan, IT)
Asia Pacific	16:00 (Sydney, AU)
Japan	14:00 (Yokohama, JP)
Australia, New Zealand	16:00 (Sydney, AU)

Hardware replacement requests received after the times shown above will be fulfilled on the second subsequent business day.

To contact your local Sophos office, see: *http://sophos.com/companyinfo/contacting/*

Sophos Proactive Monitoring

Proactive Monitoring is a service that can be provided by Sophos to continuously monitor the system health and status of your appliance. If there is ever a need to do so, Sophos will contact you and advise you about what action may need to be taken to ensure the continued smooth functioning of your appliance.

If your Email Appliance indicates that Sophos Proactive Monitoring is disabled, then you are not subscribed to this service. To subscribe to the Sophos Proactive Monitoring service, contact your Sophos representative.

Getting Started

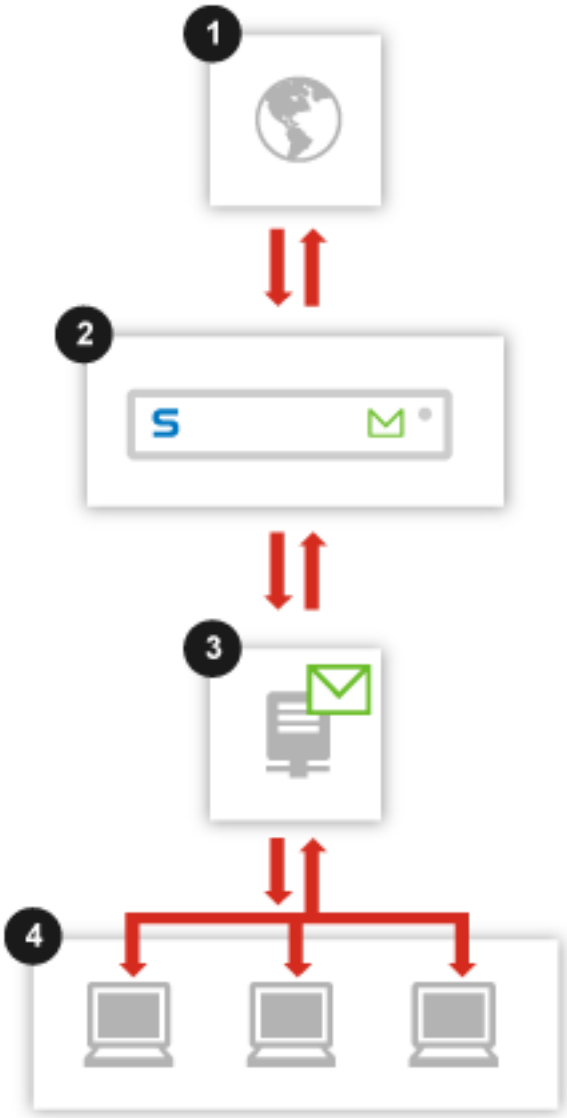
The Email Appliance is an appliance for filtering email. It provides tools for routing incoming and outgoing mail, configuring policies for email processing, monitoring mail flow, and allowing end-user access to a message quarantine.

Mail Routing

The Email Appliance is designed to function as an email gateway for a network. Incoming email is relayed by the Email Appliance to internal mail hubs or 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.

Simple Mail Routing

A simple network configuration could be set up with the Email Appliance at the network gateway as shown.



1. Internet
2. Email Appliance
3. Mail Hub/SMTP Server (for example, MS Exchange)
4. Clients

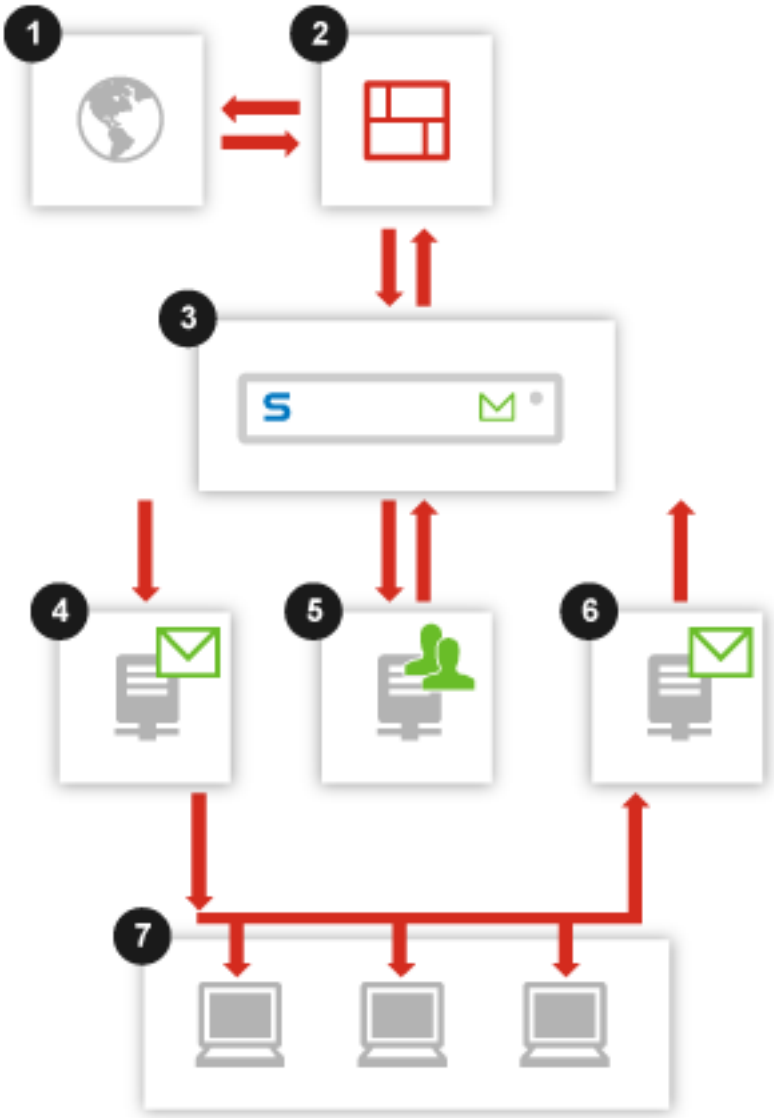
Incoming mail is filtered by the Email Appliance, and then passed directly to a mail hub for retrieval by clients. Outbound email is sent from the clients to the mail hub, and then routed out to the Email Appliance for delivery to external addresses. Alternatively, clients could use the Email Appliance itself as their outbound SMTP relay. The Email Appliance would pass local mail back to the mail hub and external mail out to the internet.

User-based authentication at the gateway helps prevent unwanted messages from entering the network. In the previous configuration example, messages to invalid users are rejected at the mail hub rather than the gateway. Connecting the Email Appliance to a directory services domain controller enables user-based authentication at the gateway.

Mail routing is configured on the **Configuration ➤ Routing** page.

More Complex Mail Routing

In this example, inbound and outbound email are handled by separate servers in the network.



1. Internet
2. Firewall
3. Email Appliance
4. Mail Hub (for example, MS Exchange)
5. Directory Services Domain Controller
6. Outbound SMTP Server
7. Clients

Incoming mail is routed through a firewall to the Email Appliance, and then forwarded to a mail hub where it is retrieved by clients. Outbound email is routed through an SMTP relay before being sent out to the Email Appliance. Local email can be diverted from the outbound SMTP relay directly to the mail hub, or through the Email Appliance for policy filtering. The domain controller provides the Email Appliance with user information, which allows it to reject messages to invalid users at the gateway.

With the exception of quarantined email, messages are not stored on the Email Appliance.

Mail routing is configured on the **Configuration ➤ Routing** page.

Policy

Mail filtering is controlled by policy settings. The main categories of the policy include **Anti-Virus**, **Anti-Spam**, **Data Control**, and **Additional Policy** (such as offensive language and keywords). You can also set **Allow/Block Lists** and **Filtering Options**. Generally, the settings that you can change involve which actions are triggered by specific events, and for what groups of your users the settings are applied.

For example, the **Anti-Virus** page allows you to select—for either inbound and outbound messages—the actions that are taken in response to messages that contain:

- Viruses
- Unscannable Attachments
- Encrypted Attachments

- Suspect Attachments

The actions that you can select vary for the different events, but may include:

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

You can also select the end user group(s) affected by these settings, and you can specify exceptions to the selected group(s).

Similar types of settings are available for **Anti-Spam** and **Additional Policy** filtering, although the details for each vary.

Several policy pages also contain global settings. These settings can have a significant impact on system performance and filtering accuracy. They include:

- On the **Additional Policy** page, you can can configure the content preferences for inbound and outbound mail.
- On the **Allow/Block Lists** page, you can create allow and block lists for hosts and senders that can be used to accept or reject messages from the indicated sources, thus avoiding normal policy processing.
- On the **Filtering Options** page you can:
  - set the stage at which IP reputation filtering is performed.
  - enable protection from denial of service (DoS) attacks.
  - set whether to share aggregate traffic data with SophosLabs to improve your spam protection.

Quarantine

The quarantine stores unwanted (spam) or dangerous (virus infected) messages. The policy can send messages to the quarantine in three ways:

- **Quarantine**: The message is sent to the quarantine and not delivered to the recipient.
- **Quarantine and continue**: A copy of the message is quarantined, then processing of the message continues.
- **Copy to Quarantine, drop file(s), and continue** (Anti-Virus): A copy of the message is sent to the quarantine and a copy, without its infected attachments, is sent to the recipient.

Administrator and User Accounts

The Email Appliance provides different functionality, depending on the type of account. Administrators can access Email Appliance features, as can email users for whom the Email Appliance filters mail. There are two types of administrator account: System administrator and Help desk administrator.

System administrators have full access to the control and monitor functions of the Email Appliance, including its configuration. They can create, and in some cases import, other accounts. A system administrator controls whether users have web access to Email Appliance management capabilities and what features are available to them.

Help desk administrators have a limited subset of the system administrator capabilities. They can:

- view the **Dashboard** tab
- view the **Reports** tab
- search the quarantine and release spam messages from it
- search the logs
- view the **Help**

However, help desk administrators cannot access:

- the **Configuration** tab
- the **System Status** tab
- the **Sophos Support** or **About** pages that are linked from the **Help** window

Users are the email recipients served by the groups, which are either imported from a directory services server or are manually created. Mail-filtering actions are applied to specified groups. System administrators can grant users access to web pages that give them the ability to manage certain aspects of their own mail filtering via a web-based GUI. Administrators can set any of the following user preferences:

- Whether users can access web pages from which they can manage (release or delete) their own quarantined messages.
- What authentication method is used when users log in.
- Whether users can create their own allow/block lists.
- Whether users can opt out of spam checking.
- What default language is displayed in the user web access pages.
- Whether users receive emailed summaries of the messages that they have in the quarantine.

Email Appliance Updates

New threats are constantly evolving on the internet: new viruses, new strategies devised by spam senders, and other novel security attacks. To ensure that your Email Appliance is able to deal with these changes, a built-in update mechanism downloads and installs updated information from SophosLabs.

SophosLabs sites around the world provide rapid response to evolving threats like viruses, spam, phishing, spyware and other malware, 24 hours a day, seven days a week.

The Email Appliance constantly updates anti-virus and anti-spam definitions. It also downloads "Critical" and "Maintenance" software updates on a configurable schedule. Critical updates are security-related and protect against anything that can compromise the Email Appliance. Maintenance updates contain the latest non-critical software updates and bug-fixes.

Clustering

Use the **Configuration ➤ System ➤ Clustering** page to manage a cluster.

Note: Using clustering requires that you have two or more Email Appliances with identical software versions that are connected to the same network and able to communicate using the ports specified on the *Configuration of Ports* (page 188) page. All appliances used in a cluster must be configured with static IP addresses, which are configured on the **Network: Network Interface** page. Clustering will not work if any of these appliances are configured for DHCP.

If your appliance is not yet part of a cluster, you can enable 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 **Join**.

Important: If an appliance joins an existing cluster, its configuration is overwritten by the configuration options it receives from the cluster.

If your appliance successfully joins or forms a cluster, a list of cluster members is displayed.

If your appliance is a member of a cluster already, you will see a list of all appliances in the cluster. You can:

- Click on the name of a cluster member to view its system status.

- Click **Remove** to remove an appliance from the cluster.

Email Appliance Hardware

The ES1000, ES1100, ES4000, ES5000, and ES8000 are high-performance appliances that are designed to handle a large volume of email traffic. The ES4000/5000/8000 provide redundant, hot-swappable hard drives and power supplies, and the dual processors help ensure uninterrupted filtering of viruses and spam. See the hard drive and power supply sections for instructions on installing replacement components. All of the Sophos Email Appliances raise alerts via the software and email if any of the hardware is not functioning optimally. The Troubleshooting section describes hardware-related alerts.

Hardware Troubleshooting

The Email Appliance has a number of ways to alert you if there is a problem with one of its hardware components. In addition to text alerts in the graphical user interface (GUI) and alerts sent via email, the Email Appliance also issues warnings using LED indicators and audible alarms.

Audible Alarms [ES4000/5000/8000 Only]

There are two conditions that cause an alarm to sound on the ES4000, ES5000 and ES8000.

- **Disk Drive Failure:** If one of the drives in the RAID 1 mirror fails, an alarm begins to sound. The alarm continues to sound until the failed disk is replaced.
- **Power Supply Failure:** If one of the two power supplies fails completely, an alarm begins to sound. The alarm continues to sound until the failed power supply is replaced. If a power supply fails partially, the alarm does not sound.

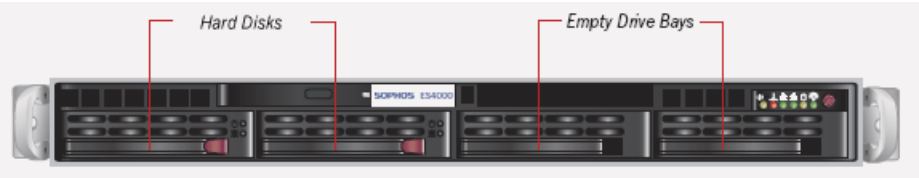
Hardware Alerts

Depending on the severity of the issue, the Email Appliance will raise an alert in the GUI or via email, or both. Alerts advise that devices are working normally or draw attention to potential problems. In most cases, the alert will instruct you to contact *Sophos Technical Support* .

Replacing an ES5000/8000 Hard Drive

A single failed drive can be replaced without exiting the ES5000/8000 application or shutting down the operating system. These are hot-swappable SCSI hard disk drives that can be removed and reinstalled while the power is on. The appliance automatically detects the removal of a failed or defective drive and the installation of its replacement.

This is an appliance with RAID 1 storage. Single hard drive failures do not result in an appliance failure. In the event of a single disk failure, the other disk in the RAID mirror takes over, and the appliance continues to function normally. When a replacement for the failed drive is installed, the RAID controller automatically begins rebuilding the new drive.



Hardware Configuration

On the ES5000/8000, the RAID 1 mirror consists of the leftmost two hard disks (viewed from the front of the unit). The two bays on the right do not contain drives.

Caution: Removal of the other drive during this procedure or during the rebuild will result in system failure.

Static-Sensitive Devices

Caution:

Electrostatic discharge (ESD) can damage electronic components. To prevent damage to any printed circuit boards, it is important to handle them very carefully. The following measures are generally sufficient to protect your equipment from ESD damage.

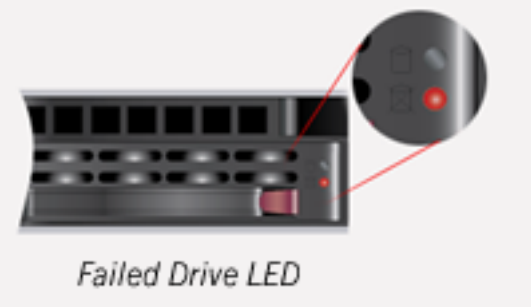
- Be sure that the appliance is properly grounded to the chassis ground through the AC power cord or enclosure frame.
- Touch a grounded metal object before removing the drive from the antistatic bag.
- Handle drive by its edges only; do not touch components on the bottom.

Caution: Removal of the other drive during this procedure or during the rebuild will result in system failure.

Caution: Disk drives are static-sensitive devices. Please make proper use of the wrist strap included in the disk field-replaceable unit (FRU) kit.

To replace a hard drive:

1. First remove the front bezel to expose the disk drives. On a failed disk drive, the red LED on the front of the drive is illuminated (the bottom LED of the two drive-specific LEDs) and the ES5000/8000's audible alarm is sounding.



2. Press the colored release button beside the drive's LEDs on the failed drive to unlatch the handle.

3. Swing the handle fully out to disengage the drive.

4. Slide the drive halfway out of the drive bay and wait for it to spin down. Allow 10-20 seconds before removing the drive from the drive bay.

5. While the system is running, insert the replacement disk in the empty slot. Insert the replacement drive into the disk bay and slide the disk straight to the back of the bay.

6. Swing the handle in toward the appliance. Continue pushing the handle in until you feel it lock in place.

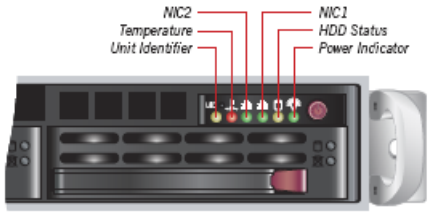
7. Press firmly on the both the left and right edges of the drive with both thumbs. Applying this pressure ensures that the drive is fully engaged, even if no movement of the drive is felt.

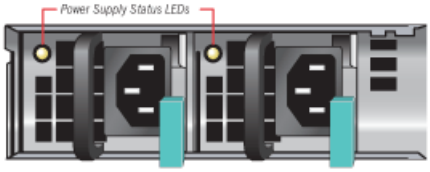
8. After the failed disk is replaced, the green and red LEDs on the new disk start to blink and the audible alarm is silenced, indicating that the mirror is rebuilding. Once the rebuild is complete, the red LED goes off. The front bezel can then be replaced.

Replacing an ES5000/8000 Power Supply

The ES5000 and ES8000 have two hot-swap redundant power supplies. If either power supply fails, the redundant feature allows the other module to take over the full load, and the system runs without interruption.

The power supplies can be replaced without powering the system down or sliding the ES5000/8000 out from the rack. In normal operation, the "Power Indicator" LED on the front panel is green, and the "Power Supply Status" LEDs on the back of the ES5000/8000 are also green for each power supply.





Failure Identification

Case 1

If either of the two power supplies completely fails, the "Power Indicator" LED on the front panel turns yellow, and an alarm sounds until the power supply is replaced.

On the back of the unit, the "Power Supply Status" LED for the unit that has failed is either off or yellow. This is the power supply to replace.

Case 2

If either of the two power supplies partially fails, the "Power Indicator" LED on the front panel is green and no alarm sounds.

On the back of the unit, the "Power Supply Status" LED for the unit that has partially failed is yellow. This is the power supply to replace.

Caution:

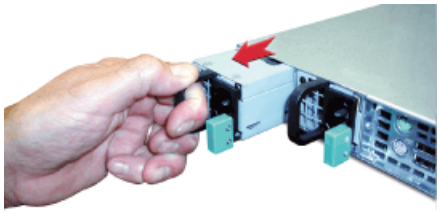
- Be sure that the appliance is properly grounded to the chassis ground through the AC power cord or enclosure frame.
- Touch a grounded metal object before removing the power supply module from the antistatic bag.
- Make sure to replace with the same type of power supply.

Single Power Supply Replacement

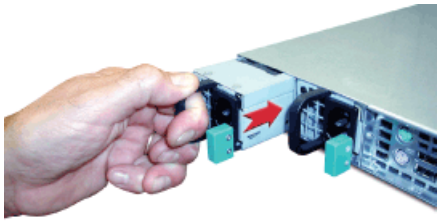
To replace a failed power supply:

1. Ensure that the power cord is unplugged from the failed power supply module. Then, while holding onto the handle, press the green locking tab on the bottom right of the power supply in toward the handle. This will disengage the power supply.

2. Pull the power supply module straight out. Check to make sure that the replacement power supply module is the same type as the one previously removed.



3. Carefully push the power supply module straight into the appliance until you hear the release tab click into place.

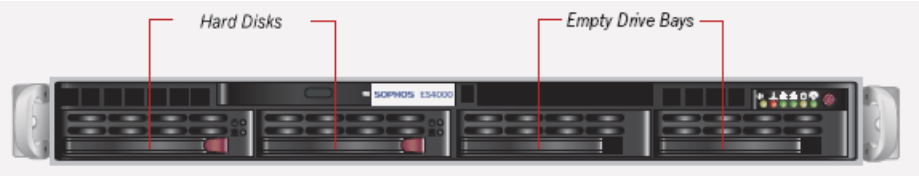


4. Plug the AC power cord back into the new power supply module. The "Power Supply Status" LED on the new module should now be green.

Replacing an ES4000 Hard Drive

A single failed drive can be replaced without exiting the ES4000 application or shutting down the operating system. These are hot-swappable SCSI hard disk drives that can be removed and reinstalled while the power is on. The appliance automatically detects the removal of a failed or defective drive and the installation of its replacement.

This is an appliance with RAID 1 storage. Single hard drive failures do not result in an appliance failure. In the event of a single disk failure, the other disk in the RAID mirror takes over, and the appliance continues to function normally. When a replacement for the failed drive is installed, the RAID controller automatically begins rebuilding the new drive.



Hardware Configuration

On the ES4000, the RAID 1 mirror consists of the leftmost two hard disks (viewed from the front of the unit). The two bays on the right do not contain drives.

Caution: Removal of the other drive during this procedure or during the rebuild will result in system failure.

Static-Sensitive Devices

Caution:

Electrostatic discharge (ESD) can damage electronic components. To prevent damage to any printed circuit boards, it is important to handle them very carefully. The following measures are generally sufficient to protect your equipment from ESD damage.

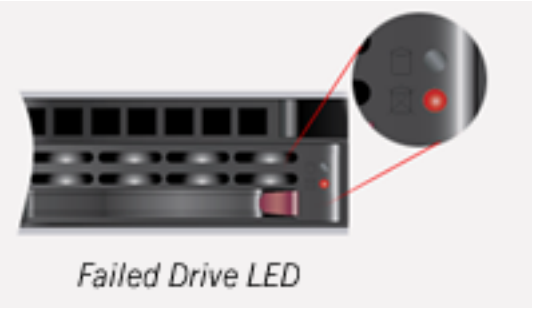
- Be sure that the appliance is properly grounded to the chassis ground through the AC power cord or enclosure frame.
- Touch a grounded metal object before removing the drive from the antistatic bag.
- Put on the grounding wrist strap; handle the drive by its edges only; do not touch components on the bottom.

Caution: Removal of the other drive during this procedure or during the rebuild will result in system failure.

Caution: Disk drives are static-sensitive devices. Please make proper use of the wrist strap included in the disk field-replaceable unit (FRU) ship kit.

To replace a hard drive:

1. First remove the front bezel to expose the disk drives. On a failed disk drive, the red LED on the front of the drive is illuminated (the bottom LED of the two drive-specific LEDs) and the ES4000's audible alarm is sounding.



2. Press the colored release button beside the drive's LEDs on the failed drive to unlatch the handle.

3. Swing the handle fully out to disengage the drive.

4. Slide the drive halfway out of the drive bay and wait for it to spin down. Allow 10-20 seconds before removing the drive from the drive bay.

5. While the system is running, insert the replacement disk in the empty slot. Insert the replacement drive into the disk bay and slide the disk straight to the back of the bay.

6. Swing the handle in toward the appliance. Continue pushing the handle in until you feel it lock in place.

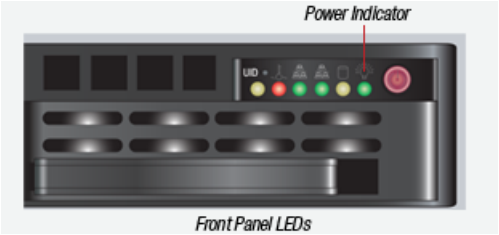
7. Press firmly on the both the left and right edges of the drive with both thumbs. Applying this pressure ensures that the drive is fully engaged, even if no movement of the drive is felt.

8. After the failed disk is replaced, the green and red LEDs on the new disk start to blink and the audible alarm is silenced, indicating that the mirror is rebuilding. Once the rebuild is complete, the red LED goes off. The front bezel can then be replaced.

Replacing an ES4000 Power Supply

The ES4000 has two hot-swap redundant power supplies. If either power supply fails, the redundant feature allows the other module to take over the full load, and the system runs without interruption.

The power supplies can be replaced without powering the system down or sliding the ES4000 out from the rack. In normal operation, the "Power Indicator" LED on the front panel is green, and the "Power Supply Status" LEDs on the back of the ES4000 are also green for each power supply.



Failure Identification

Case 1

If either of the two power supplies completely fails, the "Power Indicator" LED on the front panel turns yellow, and an alarm sounds until the power supply is replaced.

On the back of the unit, the "Power Supply Status" LED for the unit that has failed is either off or yellow. This is the power supply to replace.

Case 2

If either of the two power supplies partially fails, the "Power Indicator" LED on the front panel is green and no alarm sounds.

On the back of the unit, the "Power Supply Status" LED for the unit that has partially failed is yellow. This is the power supply to replace.

Caution:

- Be sure that the appliance is properly grounded to the chassis ground through the AC power cord or enclosure frame.
- Touch a grounded metal object before removing the power supply module from the antistatic bag.
- Make sure to replace with the same type of power supply.

Single Power Supply Replacement

To replace a failed power supply:

1. Unplug the power cord from the failed power supply module.

2. Depress the red locking tab on the top left of the power supply while holding down the rounded handle.

3. Pull the power supply module straight out. Check to make sure that the replacement power supply module is the same type as the one previously removed.

4. Carefully push the power supply module straight into the appliance until you hear the release tab click into place.

5. Plug the AC power cord back into the new power supply module. The "Power Supply Status" LED on the new module should now be green.

The Dashboard

The **Dashboard** tab provides a quick overview of Email Appliance activity and status in six panels:

Summary Statistics

The **Summary Statistics** has four subpanels.

Note: The **View data for** panel is only visible when the appliance is part of a cluster. You can select whether the information shown on the dashboard displays data from the entire cluster, or from a specific appliance in the cluster.

The **Message Volume Today** panel displays information about the messages processed in the last 24 hours. Messages are broken in to five categories:

- **Blocked**: Number of messages blocked by the appliance as a percentage of the total number of messages and number of messages blocked by the appliance.
- **Invalid Recipient**: Number of messages with invalid recipients as a percentage of the total number of messages and number of messages with invalid recipients .
- **Spam**: Number of messages identified as having high or medium spam scores as a percentage of the total number of messages and number of messages identified as having high or medium spam scores.
- **Virus** : Number of messages containing viruses today since midnight as a percentage of the total number of messages and number of messages containing viruses today since midnight.
- **DKIM**: Number of messages which failed DKIM verification as a percentage of the total number of messages and Number of messages which failed DKIM verification.
- **SPF**: Number of messages having an invalid mail sender as a percentage of the total number of messages and number of messages having an invalid mail sender.
- **Other**: Number of all other messages.

The **Average Daily Message Volume** panel displays the daily mean number of messages processed since system startup, both per-user and for all users.

- **Blocked**: Average number of messages blocked by the appliance.
- **Invalid Recipient**: Average number of messages with invalid recipients.
- **Spam**: Average number of messages identified as having high or medium spam scores.
- **Virus** : Average number of messages containing viruses today since midnight.
- **DKIM**: Average number of messages which failed DKIM verification.
- **SPF**: Average number of messages having invalid mail sender.
- **Other**: Average number of all other messages.

The **Quarantine and Mail Queue** panel displays information about the number of queued messages.

- **Quarantine Capacity**: Total capacity of the quarantine expressed as a percentage.

- **Quarantine Age**: The length of time, in days, of the difference between the oldest message in the quarantine and the current date and time.
- **Queued Messages**: The total number of messages currently in the queue.

Note: If you are running multiple appliances in a cluster, and you have elected to view summary statistics for the entire cluster, **Quarantine Capacity** and **Quarantine Age** amounts are prefixed with a ~ to indicate the data has been collected from the entire cluster. This prefix does not appear if you are viewing information from a single machine in the cluster.

The **Delay Queue** panel displays information about the processing of delayed messages.

- **Today**: Total number of messages delayed today.
- **Capacity**: Total capacity used of the maximum allowed delay queue storage, expressed as a percentage.
- **Messages**: The total number of messages currently in the delay queue.

Sender Genotype Test

The **Sender Genotype Test** provides an easy way perform an IP address reputation lookup.

System Console

The **System Console** panel displays indicators (both text and icons) for virus updates, Delay Queue, Sandstorm and the post-configuration status of the appliance.

- **Post-Configuration Checklist**: (temporary): Indicates that the items on the **Quick Tasks** sidebar have not been cleared. Click **Post-Configuration Checklist** to view the **Configuration Homepage**. Once every item in the checklist is cleared by clicking the “x” beside each one, the initial page of the **Configuration** tab changes, and this link disappears.
- **Delay Queue**: Displays status of the Delay Queue feature: On or Off. Click **Delay Queue** to go to the Delay Queue page at **Configuration ➤ Policy ➤ SMTP Options ➤ Delay Queue** .
- **Sandstorm**: Displays status of the Sandstorm feature: On or Off. Click **Sandstorm** to go to the Sandstorm page at **Configuration ➤ Policy ➤ Sandstorm** .

Virus and Spam Counts

The **Virus and Spam Counts** panel displays the following information:

- **Blocked**: Total number of messages blocked by the appliance.
- **Spam**: Total number of messages identified as having high or medium spam scores.
- **Viruses**: Total number of messages identified as containing viruses since the initial system configuration.
- **Total**: Total number of messages identified as containing undesirable content.

Note: The **Total** counter includes all types of messages received, and is not a total of the other counters shown in this panel.

Mail Velocity

The **Mail Velocity** section displays three gauges:

- **Messages/hour**: Number of messages currently being processed by the Email Appliance system. As the message volume varies, the scale of the gauge will adapt to maintain easy readability. Holding your mouse pointer over the gauge will display a tooltip with detailed message volume information.
- **Message Latency**: Average latency or delay that Email Appliance message processing is adding to the delivery of the messages, expressed as the average number of seconds that messages are delayed. Holding your mouse pointer over the gauge will display a tooltip with detailed message latency information.
- **Delayed Messages/hour**: The number of delayed messages processed by Email Appliance system. As the delayed message volume varies, the scale of the gauge will adapt to maintain easy readability. Holding your mouse pointer over the gauge will display a tooltip with detailed delayed message information.

Mail Volume Today

On the bottom right of the Dashboard are five line graphs measuring blocked messages, spam, viruses, mail flow, and delayed messages. The white fill area indicates recent daily traffic flow, while the red line represents a running 7-day average. If the white area graphs higher than the red area, the Email Appliance could be dealing with a mail spike or a virus outbreak. If the red line is above the white area, this could indicate a connection or relay problem.

The **Mail Volume Today** panel displays two types of information on each of the five graphs.

The two types of information are:

- **White area**: The current day's mail volume since midnight.
- **Red line**: The average mail volume over the last week.

These two types of information are displayed for each of the following five graphs:

- **Blocked**: The total number of messages blocked.
- **Spam**: The percentage of the total number of processed messages that are classified as spam.
- **Viruses**: The percentage of the total number of processed messages that are classified as infected with one or more viruses.
- **Mail Volume**: The total number of messages processed.
- **Delayed Volume**: The number of delayed messages processed.

Sophos Sandstorm

The **Sandstorm Analysis for Today** panel displays information about the messages analyzed by Sandstorm in the last 24 hours. Messages are broken in to four categories:

- **Malicious Files**: Number of messages that Sandstorm marked as malicious.
- **Clean Files**: Number of messages that Sandstorm marked as clean.
- **Files Awaiting Analysis**: Number of messages in the Sandstorm queue, waiting for analysis.
- **Total Files Analyzed** : Number of messages analyzed by Sandstorm in the last 24 hours (the sum of malicious and clean files).

Configuration

The **Configuration** tab provides access to pages for setting system options and performing administrative tasks.

There are five groups of Email Appliance configuration pages:

- Use the **Accounts** pages to create and manage Email Appliance administrator and user accounts and groups and to set their preferences.
- Use the **Policy** pages to change how the Email Appliance processes email messages.
- Use the **System** pages to change the configuration of the Email Appliance's system software.
- Use the **Routing** pages to change the configuration of mail routing in your organization's network.
- Use the **Network** pages to change the configuration of the Email Appliance's connection to, and identity in, your organization's network.

After initial configuration, the **Quick Tasks** sidebar on the **Configuration Homepage** shows a number of post-installation tasks, with links to settings that may still require adjustment. 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.

The Content pane of the **Configuration Homepage** contains help links to all the major configuration topics, while the **Configuration** sidebar opens configuration pages in the administrative interface. For example, clicking **Directory Services** under **System** opens the **Directory Services** configuration page.

Accounts

Use the **Accounts** pages to create and manage Email Appliance administrator accounts, user accounts and groups, and to set user preferences.

- Use the **Administrators** page to create, modify, and delete Email Appliance administrator and help desk administrator accounts.
- Use the **User Groups** page to create, modify, and delete user groups, or to create, modify and use alias maps. Also, use this page to select groups created in directory services or remove them from use with the Email Appliance, as well as to enable or disable directory services alias support.
- Use the **User Preferences** page to set whether users have web access to manage their quarantined messages, as well as set any options that you make available to users. You can also set whether users are emailed summaries of their quarantined messages, as well as set options for those quarantine summaries.

Administrators

On the **Administrators** page, you can create, modify, and delete Email Appliance administrator accounts. There are two types of Email Appliance administrators:

- **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. Help desk administrators do not have access to the **Sophos Support** and **About** features, accessed from the Email Appliance's online Help window.

Creating an Administrator Account

1. In either the **System administrators** or **Help desk administrators** table, click **Add**.
   The **Add User** dialog box is displayed.
2. In the *Add User or Modify User* (page 193) dialog box, enter the full name and credentials of the user, and click **OK**.

Modifying an Administrator Account

1. In either the **Administrators** or **Help desk administrators** table, click the **Username** that you want to modify.
   The **Modify User** dialog box is displayed.
2. In the *Modify User* (page 203) dialog box, edit the name and credentials of the user as desired, and click **OK**.

Deleting an Administrator Account

1. In either the **Administrators** or **Help desk administrators** table, select the check box(es) beside the account(s) that you want to remove.
2. Click **Delete**.

User Groups

Groups are used in the Email Appliance to apply different message-filtering options to different sets of users. The user groups created here can be specified on the various pages of the **Policy** tab to determine which policy rules are applied for which users.

User groups can be selected from existing directory services groups or manually specified. Alternatively, you can manually create, modify, and delete user groups. You can enable alias support from directory services.

Note: To use directory services features with your Email Appliance, you must be using Microsoft Exchange and directory services together. A stand-alone directory services server will not provide the necessary features for Email Appliance directory services synchronization.

Note: The Email Appliance must be configured to access your directory services server before you can manage directory services groups and turn on directory services alias support. If this access is not already configured, click **Configure Directory Services** to display the **Directory Services** page and set up your directory services server.

You can also enable alias support from directory services, view directory services alias maps, and enable and configure custom alias maps that allow messages to be redirected from one email address to another.

Adding Directory Services Groups

1. In the **Select groups from directory services** table, click **Add**.
   The *Directory Services Groups* (page 192) dialog box is displayed.
2. From the **Directory Server** drop-down list, choose the server for which you want to select groups.
3. In the **Available Groups** list, select the group(s) that you want to add, and click the right arrow button.
   The groups are added to the **Selected Groups** list. To remove groups from the **Selected Groups** list, select the group(s), and click the left arrow button.

Deleting Directory Services Groups

1. In the **Select groups from directory services** table, select the check box(es) beside the account(s) that you want to remove.
2. Click **Delete**.

Adding a Group Manually

1. In the **Create groups manually** table, click **Add**.
   The *Group Editor* (page 200) dialog box is displayed.
2. In the **Group name** text box, enter a name for the group.
3. In the **Email address** text box, either add email addresses individually, clicking **Add** after each entry, or click **Upload** to upload a list of email addresses.
4. When you have finished adding entries, in the *Group Editor* (page 200) dialog box, click **OK**.

Modifying a Group Manually

1. In the **Create groups manually** table, click the name of the group that you want to modify.
   The *Group Editor* (page 200) dialog box is displayed, with the email addresses belonging to that group displayed in the **Email addresses** table.
2. You can make any of the following modifications:
   - Change the **Group name**.
   - Add users by entering the email addresses of individual users in the **Add entries** text box and clicking **Add** after each entry, or by clicking **Upload** to add a list (with one email address per line).
   - Delete users by selecting the check box beside that user's email address and clicking **Delete**.

     Note: To find email addresses in large groups, enter a search string in the **Find** text box, and click **Find Next**. Continue clicking **Find Next** to search for additional matches of the same string.

3. When you have finished making changes in the **Group Editor** dialog box, click **OK**.

Deleting a Group Manually

1. In the **Create groups manually** table, select the check box beside the group that you want to remove.
2. Click **Delete**

Enabling/Disabling Alias Maps

An alias map is a mechanism that substitues one email address for another. Directory services alias maps can be retrieved by the Email Appliance from your directory services server, and you can also create custom alias maps.

- To turn directory services alias maps support on or off, click **Directory services alias maps On** or **Off** button below the **Select groups from directory services** table.

  Note: Directory services alias maps are retrieved from the directory server, and can only be viewed, not edited by the Email Appliance.

- To turn custom alias maps support on or off, click **Custom alias maps On** or **Off** button below the **Create groups manually** table.

Creating Alias Maps for Custom Groups

To create alias maps for custom groups:

1. Click the **Custom Alias Maps** link below the **Create groups manually** table.
   The *Alias Map Editor* (page 195) dialog box is displayed.
2. Enter an email address to be substituted in the **Map from address** text box, then enter the substitute email address in the **Map to address** text box.
3. Click **Add** to add this to the list. Alternatively, click **Upload** to upload a list of addresses. The list should contain one pair of colon-separated email addresses per line, where the first address is the address you want to substitute, and the second is the substitute address itself.

   Note: You can map one domain to another by entering @<*from_domain*> as the **Map from address**, and @<*to_domain*> as the **Map to address**. For example, you could enter *@subdomain.example.com* for the **Map from address**, and *@example.com* for the **Map to address**. This would cause any mail addressed to users at *subdomain.example.com* to be mapped instead to *example.com* for policy purposes.

4. After you have finished adding entries, click **OK**.

> Example: if email aliases have been configured using directory services or the **Custom alias maps** feature, and alias support is turned on, the Email Appliance applies these same aliases for policy filtering and user preferences. For example, if you have an alias that redirects mail destined for *userA@example.com* and *userB@example.com* to *userC@example.com*, the effects are as follows:
>
> - **Policy Filtering**: Instances of *userA@example.com* and *userB@example.com* are interpreted as *userC@example.com* when messages are processed by the policy. Any explicit references to *userA@example.com* and *userB@example* in the policy are ignored.
> - **Quarantine Summaries**: If the Email Appliance is configured to email quarantine summaries, the summaries for *userA@example.com* and *userB@example.com* are mailed to *userC@example.com* only.
> - **User Block Lists**: Messages addressed to *userA@example.com* and *userB@example.com*, which are subsequently blocked, are stored in the Blocked Messages list for *userC@example.com*.

User Preferences

On the **User Preferences** page, you can set whether users have web access to manage their quarantined messages, and you can configure the other options available to users.

You can also set whether users are sent quarantine email summaries, and set options for their summaries. When the **Enable quarantine email summary** option is turned on, users receive email messages at regular intervals. These messages list all email quarantined by the Email Appliance. Users can respond to the summary message to release or delete their quarantined messages. Users can opt out of receiving quarantined email summaries by disabling this feature in the End User Web Quarantine.

Note: Options on the **User Preferences** page can be configured individually, but you must click **Apply** after configuring preferences to make the settings take effect.

Configuring User Privileges for Spam Management

You can set whether users have web access to manage their quarantined messages and set the form of authentication required for this access.

For complete descriptions of the features that can be made available to users, see the End User Web Quarantine documentation.

1. Select the **Enable end user 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.
2. Select one of the **Authentication** option buttons:

   - **Active Directory**: You must have Active Directory server access configured to use this option. When using this method, users log in by entering their assigned Active Directory username and password.
   - **Custom list**: Create the list by clicking the associated **Define users** button, which opens the *Email Password List* (page 199) dialog box. When using this method, you must supply users with the email/login and password they will need to access the web quarantine.

   With both of these options, users log in by pointing their browsers to the Web Quarantine address:
   `http://<EUWQ_host>.<domain>`
3. Set any **Options** that you want to grant your users:

   - Select **Enable allow/block lists** to allow users to create and use personalized allow and block lists for hosts and senders.
   - Select **Allow wildcard usage in allow/block lists** to let users use wildcards when defining their personalized allow and block lists for hosts and senders.
   - Select **Allow users to opt-out of spam checking** to allow users to bypass spam checking of their messages.
4. On the **Default user interface language** drop-down list, select the users' preferred language. Users also have the option of personalizing the language via a feature in the End User Web Quarantine.

   Note: The End User Web Quarantine and its associated help file are displayed to users in the default language set by an administrator or in the language they have selected for themselves. In addition to English, help pages are available in the following languages: Chinese (Simplified or Traditional), French, German, Italian, Japanese, Spanish and Swedish.
5. Click **Configure** in the **Configure end user service** panel to set the port used by the End User Web Quarantine.

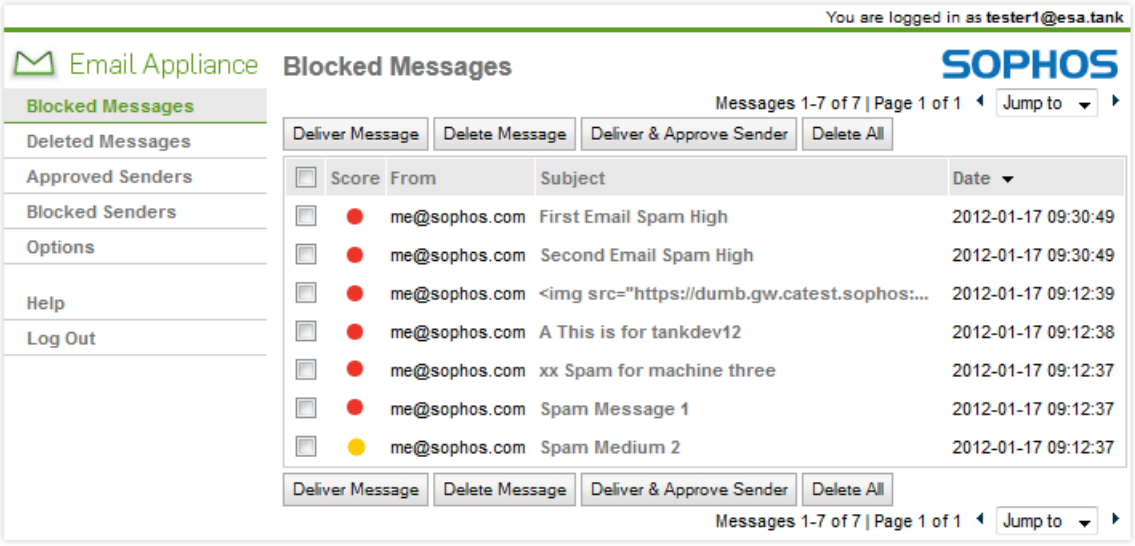


Figure 1: The end user's view of the Web Quarantine

Configuring Quarantine Summary Mailouts

You can set whether users are automatically emailed summaries of their quarantined messages, and the frequency with which they're delivered.

To configure automated emailing of quarantine summaries:

1. Select the **Enable email quarantine summary** check box to email users summaries of their quarantined emails.
2. Click the **Configure** button to configure the quarantine summary schedule in the **Advanced Email Quarantine Summary Schedule** dialog box.

Setting Banner Options for Quarantine Summaries

Optionally, you can append banners to quarantine summary messages in the form of headers and footers.

By default, the following message 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.
```

To set banner options for email quarantine summaries:

1. Select the **Add header** or **Add footer** check box and type the content for the banner (the note inserted at the top or bottom of the message body) in the associated text box.
2. From the **Banner Format** drop-down list, select whether the banner is **Plain Text** or **HTML**.

Policy

Use the **Policy** pages to change how the Email Appliance processes email messages.

- Use the **Policy: Anti-Virus** page to configure whose messages are scanned for viruses and how messages containing viruses are handled.

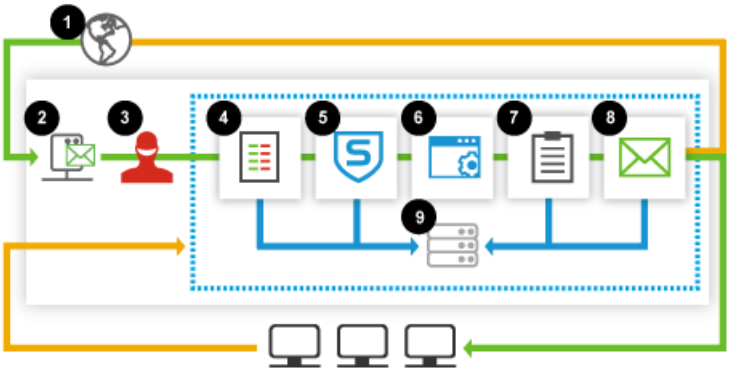
- Use the **Policy: Anti-Spam** page to configure whose messages are scanned for spam and how messages identified as spam are handled.
- Use the **Policy: Additional Policy** page to configure whose messages are scanned for offensive language or specified keywords and how the messages that match these content scans are handled.
- Use the **Policy: Allow/Block Lists** page to create and modify lists of hosts and senders whose messages are delivered or blocked with anti-virus scanning but without anti-spam scanning.
- Use the **Policy: Sandstorm** page to enable/disable communication between appliance and Sandstorm, view the files sent to Sandstorm for threat analysis and release messages that are pending analysis.
- Use the **Policy: Filtering Options** page to set the message-processing stage at which the IP reputation filtering is used, whether protection against denial of service and directory harvest attacks are enabled, and whether aggregate traffic data is shared with SophosLabs to help improve spam detection.
- Use the **Policy: Encryption** page to manage the Email Appliance's email encryption and encryption policies.
- Use the **Policy: SMTP Authentication** page to enable SMTP authentication, enable and configure TLS encryption, and select one or more ports for SMTP authentication.
- Use the **Policy: SMTP Options** page to configure SMTP options and perimeter protection.

Using the Policy and Template Wizards

The rules associated with each category of the policy are easily configured by using a wizard, which can be launched by clicking the **Add** button. The Policy Wizard is available from the following pages: **Anti-Virus**, **Anti-Spam**, **Data Control**, and **Additional Policy**. You can also launch the SPX Template Wizard by clicking **Add** on the **SPX Encryption** tab of the **Encryption** page. For more information, see the documentation for these Policy configuration pages.

Policy Message Flow

Sophos Email Appliance Policy Message Workflow



Each email that the appliance receives from external mail relays ❶ is processed to determine how it will be handled. Messages are processed in the following order:

❷**Perimeter Protection:** Denial of Service and Directory Harvest Attack protection, and rate control occurs at the Mail Transfer Agent (MTA) layer. You can configure this in Filtering options.

Recipient verification is also performed at the MTA level. This is done either by synchronizing a list of valid recipients from a Directory Server, or verifying recipient addresses at the relevant downstream mail server. A message sent to an invalid recipient will be rejected during the SMTP connection, so that the message is never accepted or stored on the Sophos Email Appliance.

❸**Sender Genotype:** Sender Genotype filtering uses data from SophosLabs to block email from known bad senders. When enabled, this improves overall performance by reducing the number of spam messages processed. Sophos Sender Genotype filtering is responsible for blocking and rejecting anywhere from 70-85% of unwanted email before it even reaches the Sophos Spam Engine.

❹ **Allow/Block Lists:** Allow/Block lists can significantly improve the performance of the appliance. Messages from Allowed Hosts/Senders will bypass anti-spam filtering, while messages from Blocked Hosts/Senders are blocked without being scanned for spam or content.

Note: Allow List entries override conflicting Block List entries. The Allow List will not exempt message from Threat Protection checks.

Messages are processed in the following order:

1. Allowed hosts/senders (Global)
2. Blocked hosts/senders (Global)
3. Allowed senders (per-user)
4. Blocked senders (per-user)

This ensures that Global settings always take precedence over end-user settings.

❺ **Threat Protection:** The *Threat Protection* (page 35) feature tests both content and reputation of a message. If a virus, encrypted attachment, unscannable attachment, or SophosLabs suspected attachments is found, the message will be discarded or quarantined by default. Threat protection also does SPF and DKIM checks to validate the authenticity of a message.

❻ **Data Control:** Next, messages are checked against your *Data Control* (page 49) policies to prevent data leakage.

❼ **Additional Policy:** A message is next checked against content policy. The content policy identifies and takes appropriate action on messages based on administrator-configured rules around corporate governance or compliance. Additional Policy can be configured to check messages for:

- Mail sent or received from specific users or groups.
- Offensive language.
- Specific keywords.
- Specific attachments or file types.
- Specific hostnames or IP addresses.

Additional Policy rules can also be used to:

- Add banners to messages.
- Enforce appropriate use policies.

❽ **Anti-Spam Policy:** Finally, a cumulative spam score is assigned to each scanned message based on results of anti-spam tests. This score determines the relative likelihood that a message is spam and classifies messages in one of three ways: not spam, medium probability of being spam, or high probability of being spam.

Within each **Policy** section, individual rules are processed in the order in which they are listed. Depending on how each policy rule is configured, a message may be placed in the quarantine ❾, delivered to the appropriate recipient(s), or it may be discarded.

Threat Protection

On the **Configuration** sidebar, select **Policy ➤ Threat protection** to configure various policy options for inbound and outbound messages.

By adding a policy rule you can control how the appliance will handle messages containing known viruses, unscannable attachments, encrypted attachments, or suspect attachment types. For each of these message categories, actions can be configured for a specific set of users.

Additionally, you can configure DKIM (DomainKeys Identified Mail) and SPF (Sender Policy Framework) functionality by adding a policy rule.

If the default policy settings do not suit your organization's needs, you can modify them (see the encrypted attachments example later in this section). The threat categories and their default settings are as follows:

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. This rule cannot be deleted.
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.
SophosLabs 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.
DKIM (DomainKeys Identified Mail) test verification	DKIM provides a way of verifying the reputation of senders using cryptographic authentication. Creating DKIM policy rules can attach an identifier to outbound messages, and can verify the identifier of incoming messages.
SPF (Sender Policy Framework)	SPF provides a way to verify that a message does not have a forged sender address. For senders that provide an SPF record, creating an inbound policy rule will ensure that the envelope sender address has not been forged.
Sandstorm	Sandstorm provides a higher level of security by performing real-time, in-depth threat analysis of potentially malicious messages. Suspicious messages are sent for analysis. If found to be infected, messages are dropped, else delivered to the respective recipient.
Time-of-Click (ToC) Protection	ToC Protection provides protection against any malicious hyperlinks (URLs) in a message at the time a user clicks. All hyperlinks (URLs) present in a message are encoded by the appliance at the time of delivery. When a user clicks any of the links, appliance dynamically determines the reputation of that link and performs actions as per configured policy(s) for that reputation. **Note:** Action performed on URL click is that specified in the policy at the time that email is processed by the Email Appliance.

Rules for these threat categories can be configured by clicking on the description. Rules are processed in order of their priority. A rule's priority can be changed by clicking the up or down arrow to the left of the rule description.

Threat Protection Policy Configuration

Use the **Configuration ➤ Policy ➤ Threat Protection** page to configure general anti-virus rule settings.

- Select the **Outbound** or **Inbound** tab.
- To add a rule, click **Add** in the rules table.

  The Policy Wizard is displayed.
- To configure a rule, click the **Description** of the rule in the rules table.

  The **Configure Rule** dialog box is displayed.
- To change the priority of a rule:

  Click the up or down arrow buttons in the rules table, next to the **Description** of the rule or rules whose priority you want to change.

  After you have finished setting rule priorities:

  - Click the **Save order** button when you are satisfied with the order of the priorities.
  - Click the **Reset order** button to cancel and restore the rule priorities.
- You can also enable or disable existing rules.
  - An active rule is displayed in the rules table with a green **Active** icon, next to which is a **Turn Off** button. There is also a priority for an active rule.

- An inactive rule is displayed in the rules table with a gray **Active** icon, next to which is a **Turn On** button. There is also no priority for an inactive rule, and it will not be processed.
- To disable an active rule, click **Turn Off** in the rules table, next to the rule.
- To enable an inactive rule, click **Turn On** in the rules table, next to the rule.

- To delete a rule, select the check box next to the rule in the table of rules, then click **Delete**.

Policy Wizard: Threat Protection

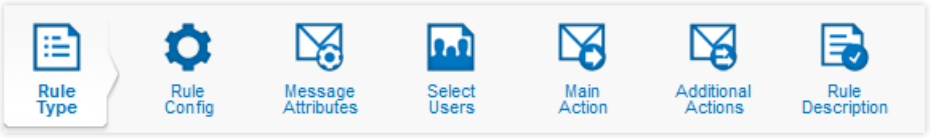
Each page of the Policy Wizard allows you to configure specific aspects of a rule's behavior, and can be thought of as answering a series of questions:

1. **What type of rule do you want to configure?** This is the first page presented by the Policy Wizard. Its contents are contextually based, and depend on whether you're in the Anti-Virus, Anti-Spam, or Additional Policy section when you enter the Policy Wizard. The choice made on this page defines the policy rule and any subsequent steps. It is the only rule attribute that cannot be changed after it has been created.
2. **How do you want a rule to trigger?** You can answer this question on the **Rule Config** and **Message Attributes** pages of the Policy Wizard by specifying what elements of a message will cause a policy rule to trigger.
3. **Who do you want the rule to apply to?** You can answer this question on the **Select Users** page of the Policy Wizard, where you can specify which groups, specific senders, or recipient email addresses can be included or excluded.
4. **What should happen when the rule is triggered?** You can answer this question on the **Main Action** page, and also on the **Additional Actions** page of the Policy Wizard. You can specify what actions will be performed on a message, or what action will be performed after the appliance receives a message that triggers this rule.
5. **How is this policy rule identified?** You can answer this question on the **Rule Description** page of the Policy Wizard, where you can provide a description of the rule.

Depending on the rule type, and whether you have selected **Enable advanced policy options**, some sections may not be enabled for configuration.

Note: If you are adding a rule for the first time, you must proceed through the configuration items in sequence. If you are configuring a rule that already exists, you can select a specific action to configure by clicking on its icon.

Rule Type



1. Select one of the following rule types:

   - **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.
   - **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.
   - **SophosLabs 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.
   - **Sender Policy Framework (SPF)**: SPF provides a way to verify that a message does not have a forged sender address. For senders that provide an SPF record, creating an inbound policy rule will ensure that the envelope sender address has not been forged.
   - **DKIM (DomainKeys Identified Mail) verification**: DKIM provides a way of verifying the reputation of senders using cryptographic authentication. Creating DKIM policy rules can attach an identifier to outbound messages, and can verify the identifier of incoming messages.

- **Sophos Sandstorm**: Sandstorm provides a higher level of security by performing real-time, in-depth threat analysis of potentially malicious messages. Suspicious messages are sent for detailed threat analysis. If found to be malicious, messages are dropped, else delivered to the respective recipient.
- **Time-of-Click Protection**: Time-of-Click Protection scans URLs contained in an email message at the time a user clicks. It dynamically blocks malicious links while genuine links can be accessed.

Reputation-based threat protection:

- For an outbound policy rule you can select **Add DKIM signature**.
- For an inbound policy rule you can select **Sender Policy Framework (SPF)** or **DKIM verification.**

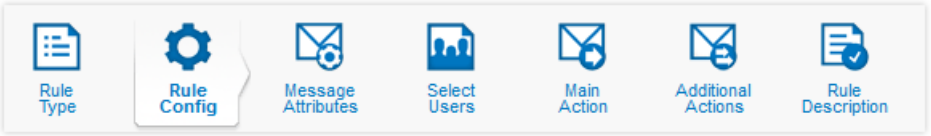
2. Configure reputation-based threat protection.

   - For an outbound policy rule you can select **Add DKIM signature**. By adding a DKIM signature, you permit the verification of the signer of the mail, as well as the integrity of its contents.
   - For an inbound policy rule you can select **Sender Policy Framework (SPF)** or **DKIM verification.**

   Note: An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of your domain. DKIM provides a domain-level digital signature authentication framework for email. Both provide a way to determine if a message has been forged.

3. [Optional] Select **Enable advanced policy options** to make all additional wizard options available. Certain steps in the wizard are grayed out, according to the selected rule type.
4. Click **Next**.

Rule Config: Attachment type



Add, edit or view the attachments or file types that will be tested by a rule.

- To add attachment filenames or file extensions:
  - Enter a filename or file type extension in the text box in the **Add Entries** section, then click **Add**, or:
  - Click **Upload** to upload a list of file names or file type extensions from a text file.

  Entries will appear in the **Entries** table.

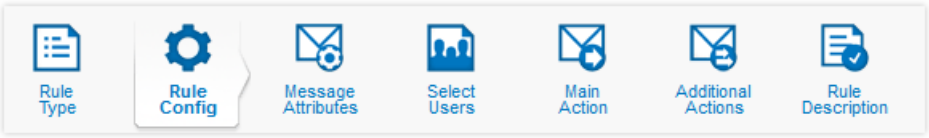
  Note: To match all files with a given file type extension, use an entry with a form similar to **.exe*.

- To edit a filename or file type extension, click on its description in the **Entries** table.
- To delete a filename or file type extension, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of filenames or file type extensions. The number of pages, as well as the page number that you are viewing, will be indicated above the **Entries** table.
  - To move to a specific page, enter the page number in the page number text box, then press **Enter** .
  - Click the > button to move forward one page.
  - Click the < button to move backward one page.
  - Click the << button to move to the first page of entries.
  - Click the >> button to move to the last page of entries.
- To search for a filename or file type extension, enter your query in the **Find** text box, then click **Find Next**.
- If you want to configure the "Entries" list as an exclusions list, select **Exclude listed attachment types**. When this check box is enabled, all files except those listed will trigger this policy rule.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Rule Config: SPF



Sender Policy Framework (SPF) is a technique based on a special DNS record to identify valid mail senders. Here, you can select the options that affect an SPF policy rule.

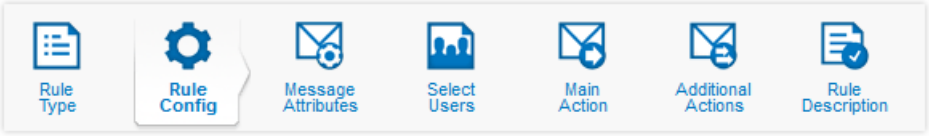
1. Select which SPF results you want as a condition of your rule.

   Select one or more of the following check boxes:

   - **None:** The domain does not have an SPF record.
   - **Pass:** The SPF record designates the host to be allowed to send.
   - **Fail:** The SPF record has designated the host as NOT being allowed to send.
   - **SoftFail:** The SPF record has designated the host as NOT being allowed to send, but is in transition.
   - **Error:** A syntax or evaluation error has occurred.

2. Select **Next**.

Rule Config: DKIM



DomainKeys Identified Mail (DKIM) is an authentication framework used to sign and validate a message based on the domain of the sender. Here, you can select the options that affect a DKIM policy rule.

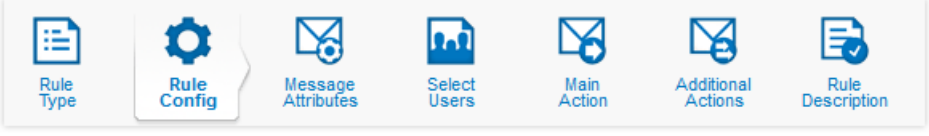
1. Select which DKIM results you want as a condition of your rule.

   Select one or more of the following check boxes:

   - **None:** There is no DKIM signature.
   - **Pass:** A DKIM signature is detected and verified.
   - **Fail:** A DKIM signature is present but failed verification.
   - **Invalid:** The message cannot be verified for some reason..

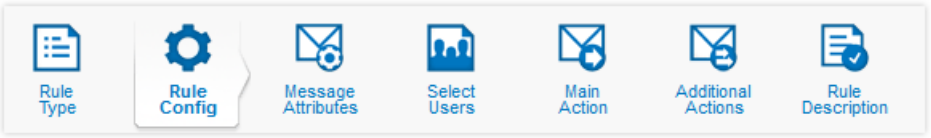
2. Select **Next**.

Rule Config: Sandstorm



1. Specify the **File Size**. Files/attachments exceeding the specified size will not be analyzed . Sophos Sandstorm can analyse a file of maximum size 10 MB.

Rule Config: Time-of-Click Protection



1. Specify the action to be performed for hyperlinks of the risk levels High, Medium, Low and Unverified.
   The available **Actions** are:
   - Block URL: Access to any URL marked with corresponding risk level will be blocked.
   - Allow URL: Access to any URL marked with corresponding risk level will be allowed.
   - Warn and Allow URL: A warning page will be displayed to the user with a link to access the URL.

   Note: By default, the actions are set to:

   High Risk: Block URL

   Medium Risk: Warn and Allow URL

   Low Risk: Warn and Allow URL

   Unverified: Allow URL

2. Select any of the following options, if required.

   Do not rewrite Whitelisted URLs

   Appliance will not rewrite or encode Whitelisted URLs present in a message. You can whitelist URLs from **Configuration ➤ Policy ➤ Allow/Block Lists** .

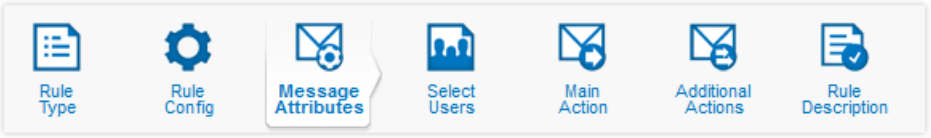
   Rewrite non-hyperlinked URLs

   Appliance will rewrite or encode even the URLs mentioned as plain text, and not hyperlinked.

   Rewrite URLs mentioned in message Subject

   Appliance will rewrite or encode even those URLs that are present in the subject of a message.

Message Attributes



Add, edit or delete additional message attributes that will trigger a rule.

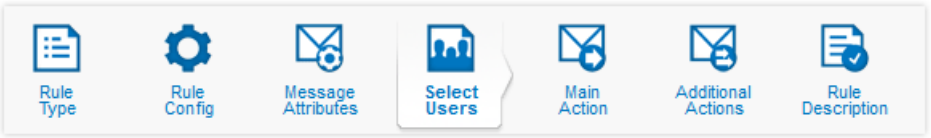
- *To add a new message attribute*, click **Add**.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- *To edit a message attribute*, click the attribute description in the **Identify message attributes** table.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- *To delete a message attribute*, select the check box next to the attribute description in the **Identify message attributes** table, then click **Delete**.
  The message attribute will be removed from the **Identify Message Attributes** table.
- [Optional] *To set the matching condition for attributes*, under **Matching logic**, select either **All message attributes must be present**, or **One of the message attributes must be present**. This option is unavailable unless at least two message attributes are specified.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.

- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Select Users



In the **Select Users** section, you can configure users and groups to be included or excluded with a policy rule.

- To configure which users or groups are affected by a policy rule:
  - Select the **Include Recipient** tab to specify which message recipients a rule will apply to.
  - Select the **Exclude Recipient** tab to specify which message recipients a rule will *not* apply to.
  - Select the **Include Sender** tab to specify which message senders a rule will apply to.
  - Select the **Exclude Sender** tab to specify which message senders a rule will *not* apply to.
- Within a tab:
  - Select **All users** if you want to configure the current tab so that it affects all users.
  - Select the **Selected groups** option if you want to configure the current tab so that it affects one or more existing groups. Groups listed in the **Available** table are available, but will not be used with this policy rule. Groups in the **Selected groups** table are configured for use with this policy rule.
    - Use the >> button to move available groups from the **Available** table to the **Selected groups** table.
    - Use the << button to remove groups from the **Selected groups** table, and back to the **Available** table.
  - Select **Custom groups** if you want to create custom groups. To add entries to a custom group:

    1. In the **Custom groups** text box, enter an email address.

       Note: You can enter wild-card characters in this text box to match on multiple addresses. For instance, `test?@*example.com` would match on both `test1@example.com` and `test3@mail.example.com`.

    2. Click **Add**. Optionally, click **Paste**, paste in a list of entries (one per line), and click **OK**.

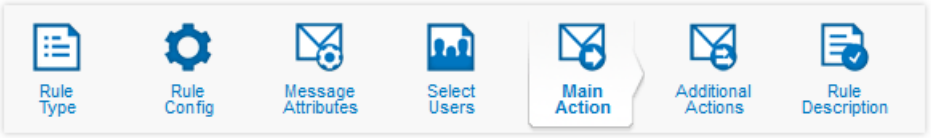
  - To delete an address from the **Custom groups** table, select the check box next to its name, then click **Delete**.

    For more information about creating and managing groups, see “User Groups” in the Accounts section of the documentation.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Main Action



Configure the main action.

- From the drop-down list in the **Message actions** section, select the action to be taken if this rule is triggered:

- **Continue Processing** to continue processing the message.
- **Deliver Immediately** to deliver the message immediately to the intended recipient(s) without triggering any subsequent policy rules.
- **Discard** to immediately discard the message.
- **Quarantine** to quarantine the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.

  Note: Only messages quarantined for the reason "spam" are accessible through the web quarantine and will be included in email quarantine summaries.

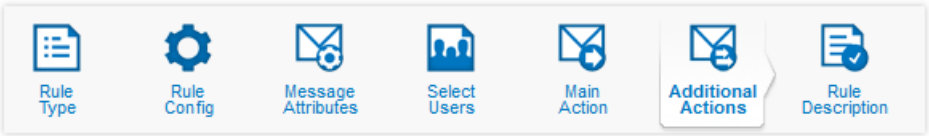
- **Quarantine and continue** to quarantine a copy of the message, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
- **Quarantine, drop file(s) and continue** to quarantine a copy of the message, drop any offending attachments, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
- **Redirect** to redirect the message to a specified email address. The original recipients will not receive the message. Specify the email address to which you want to redirect the mail to in the **Redirect email address** text box in the **Configuration** section.
- **Re-route message to another server** to send the message to another mail server. The message body, and the original sender and recipient information will be preserved, but the original recipients will not receive the message. To specify the mail server to which you want to redirect the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
- **Send a copy of the message to another server** to send the message to the original destination, and a copy of the message to another mail server. The message body and the original sender and recipient information will be preserved. To specify the mail server to which you want to send a copy of the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
- **Tag subject and continue** to tag the subject line of the message with the specified text, after which the email appliance will continue to process the message.

  Note: You can include the original subject of the message by using the %%SUBJECT%% template variable.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Additional Actions



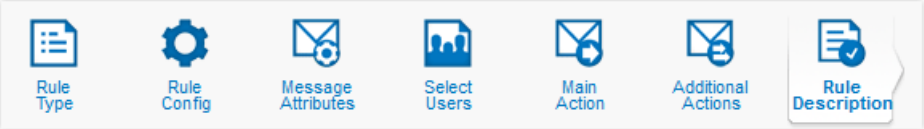
In the **Additional Actions** section, you can configure extra actions.

- To add a new action, click **Add**.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the new action, which is then displayed in the **Additional actions** table.
- To configure an existing action, click an action's description in the **Additional actions** table.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the action.
- To delete an action, select the check box next to the action description in the **Additional actions** table. Click **Delete**.
  The action will be removed from the **Additional actions** table.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Rule Description



To configure a rule description:

1. In the **Policy rule name** text box, enter or edit the description for the policy rule. This is the description that will appear in the rule table.
2. Select the **Activate this rule** check box.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Threat Protection Example

If you wanted to quarantine encrypted attachments for all but a select group of users, and notify an administrator when they are received, you could set up the threat protection policy like this:

1. In the **Inbound** threat protection rule table on the **Configuration ➤ Policy ➤ Threat Protection** page, click **Add**. The Policy Wizard is displayed.
2. Select the **Encrypted attachments** rule type. Select the **Enable advanced policy options** check box. Click **Next**.
3. In the **Message attributes** section, click **Next**.
4. On the **Include Recipient** tab of the **Users & Groups** section, select **All Users.**
5. Select the **Exclude Recipient** tab of the **Users & Groups** section, and select **Selected groups**.
6. Select the group(s) you want to exclude, then click the >> button. When you have finished, click **Next**.
7. In the **Main Action** section, select **Quarantine**. Then select **Encrypted attach** in the **Configuration ➤ Quarantine for reason** section. Click **Next**.
8. In the **Additional Actions** section, click **Add**.
   The **Additional Message Actions** dialog box is displayed.
9. From the first drop-down list, select **Notify**. In the **Configuration** section, select **Custom email address**. Enter the administrator's email address in the **Notify users** text box. In the **Notify options** section, add the custom notification subject and message. Select the **Attach original message** check box if you want the administrator to receive a copy of the original message.
10. Click **Apply**
11. Click **Next**.
12. In the **Rule Description** section, enter a description for the rule. Select the **Activate this rule** check box.
13. Click **Apply**.

Encrypted attachments will now be quarantined, and a notification will be sent to the administrator.

Anti-Spam

Use the **Configuration ➤ Policy ➤ Anti-Spam** page to configure how to handle messages with spam characteristics. A cumulative spam score is assigned to each scanned message based on results of anti-spam tests. This score determines the

relative likelihood that a message is spam and classifies messages in one of three ways: not spam, medium probability of being spam, or high probability of being 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** (probably spam), and **bounce messages**.

Each row of the Anti-Spam policy configuration table is a policy rule with options for defining the relevant users and the actions to be taken. By default, there is one rule defined for each of the two spam categories. Mail with high spam scores is discarded for all inbound messages, and quarantined for all outbound messages. Mail with medium spam scores is quarantined for all users.

Important: While completing the initial configuration of your appliance with the Setup Wizard, you were prompted to select one of three anti-spam modes: Passthrough mode, Pilot mode, or Full mode. Passthrough and Pilot modes are intended solely for testing. You should review the anti-spam settings, and configure a policy that is appropriate for your organization. For more information, see “Anti-Spam Policy Configuration” and “Policy Wizard: Anti-Spam”.

Anti-Spam Policy Configuration

Use the **Configuration ➤ Policy ➤ Anti-Spam** page to configure general anti-spam rule settings.

- Select the **Outbound** or **Inbound** tab.
- To add a rule, click **Add** in the rules table.

  The Policy Wizard is displayed.
- To configure a rule, click the **Description** of the rule in the rules table.

  The **Configure Rule** dialog box is displayed.
- To change the priority of a rule:

  Click the up or down arrow buttons in the rules table, next to the **Description** of the rule or rules whose priority you want to change.

  After you have finished setting rule priorities:

  - Click the **Save Order** button when you are satisfied with the order of the priorities.
  - Click the **Reset Order** button to cancel and restore the rule priorities.
- You can also enable or disable existing rules.
  - An active rule is displayed in the rules table with a green **Active** icon, next to which is a **Turn Off** button. There is also a priority for an active rule.
  - An inactive rule is displayed in the rules table with a gray **Active** icon, next to which is a **Turn On** button. There is also no priority for an inactive rule, and it will not be processed.
  - To disable an active rule, click **Turn off** in the rules table, next to the rule.
  - To enable an inactive rule, click **Turn on** in the rules table, next to the rule.
- To delete a rule, select the check box next to the rule in the table of rules, then click **Delete**.

Policy Wizard: Anti-Spam

Each page of the Policy Wizard allows you to configure specific aspects of a rule's behavior, and can be thought of as answering a series of questions:

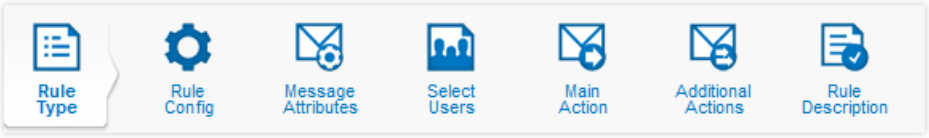
1. **What type of rule do you want to configure?** This is the first page presented by the Policy Wizard. Its contents are contextually based, and depend on whether you're in the Anti-Virus, Anti-Spam, or Additional Policy section when you enter the Policy Wizard. The choice made on this page defines the policy rule and any subsequent steps. It is the only rule attribute that cannot be changed after it has been created.
2. **How do you want a rule to trigger?** You can answer this question on the **Rule Config** and **Message Attributes** pages of the Policy Wizard by specifying what elements of a message will cause a policy rule to trigger.
3. **Who do you want the rule to apply to?** You can answer this question on the **Select Users** page of the Policy Wizard, where you can specify which groups, specific senders, or recipient email addresses can be included or excluded.

4. **What should happen when the rule is triggered?** You can answer this question on the **Main Action** page, and also on the **Additional Actions** page of the Policy Wizard. You can specify what actions will be performed on a message, or what action will be performed after the appliance receives a message that triggers this rule.
5. **How is this policy rule identified?** You can answer this question on the **Rule Description** page of the Policy Wizard, where you can provide a description of the rule.

Depending on the rule type, and whether you have selected **Enable advanced policy options**, some sections may not be enabled for configuration.

Note: If you are adding a rule for the first time, you must proceed through the configuration items in sequence. If you are configuring a rule that already exists, you can select a specific action to configure by clicking on its icon.

Rule Type

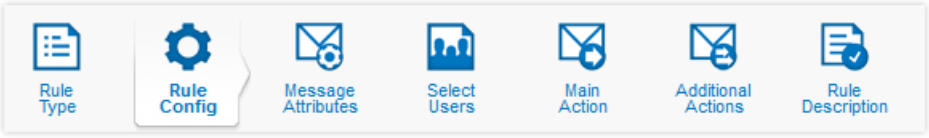


1. Select one of the following rule types:
   - **High spam**: Mail that is almost certainly spam. It is recommended that you discard all messages in this category.
   - **Medium spam**: Mail that is probably spam. It is recommended that you quarantine all messages in this category.
   - **Bounce messages**: Messages that have been bounced (also know as non-delivery report (NDR) messages. It is also recommended that you enable Bounce Address Tag Verification (BATV), which is done in the next step of the wizard. Using BATV distinguishes between legitimate and illegitimate bounce messages. This allows you to quarantine or discard bounced spam messages to spoofed senders (backscatter). If you use BATV, all outbound messages must be sent through the Email Appliance.
2. [Optional] Select **Enable advanced policy options** to make all additional wizard options available. Certain steps in the wizard are grayed out, according to the selected rule type.
3. Click **Next**.

Rule Config

Depending on the option you selected in the previous Rule Type step, this step may offer additional options for configuring the rule. If you selected Bounce Messages, you will be prompted to activate Bounce Address Tag Verifictation (BATV) options. If you selected Potentially unwanted messages, you will be prompted to specify the kinds unwanted messages for which the appliance will perform actions.

Rule Config: Bounce Address Tag Verification (BATV)



Bounce Address Tag Verification (BATV) allows the appliance to distinguish between legitimate and illegitimate bounce (NDR) messages by tagging each message with a unique signature. Upon creation of this rule, all outbound messages will be tagged for the users and groups to which this rule applies, even if the rule is not active.

Note: All outbound mail must be sent through the appliance to ensure that BATV can function correctly.

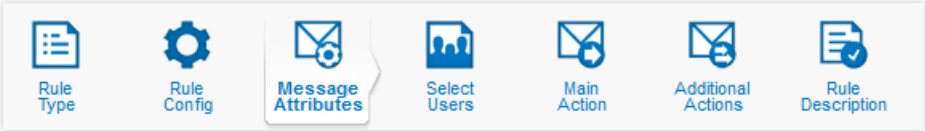
Enabling BATV will not block emails that have been identified by SophosLabs as automatically generated responses. The **Treat all auto-responders identified by SophosLabs as bounces** option will cause any email messages identified by SophosLabs as automatically generated responses to be treated as bounces.

Note: Enabling this option will quarantine all auto-responses that have been identified by SophosLabs, such as vacation responders, and not just invalid auto-responses.

To activate BATV options:

1. [Recommended] Select the **Enable Bounce Address Tag Verification (BATV)** check box to enable BATV.
2. [Optional] Select the **Treat all auto-responders identified by SophosLabs as bounces** check box to treat all automatically generated responses as bounces.
3. Click **Next**.

Message Attributes



In the **Message Attributes** section, add, edit or delete additional message attributes that will trigger a rule.

- To add a new message attribute, click **Add**.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- To edit a message attribute, click the attribute description in the **Identify Message Attributes** table.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- To delete a message attribute, select the check box next to the attribute description in the **Identify Message Attributes** table, then click **Delete**.
  The message attribute is removed from the **Identify Message Attributes** table.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Including/Excluding Hostnames for BATV

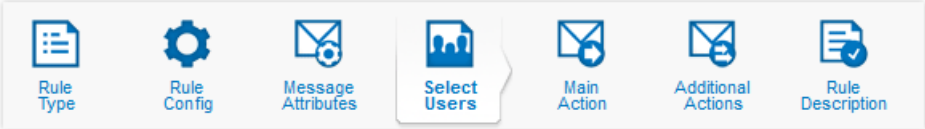
If you selected **Bounce messages** as the Rule Type, It is also possible to use the **Source Hostname** message attribute to include hosts in BATV, or exclude hosts from BATV. To do this:

1. In the **Rule Type** section, ensure that the **Enable advanced policy options** check box is selected.
2. In the **Message Attributes** section, click **Add** to add a new message attribute.
3. In the **Add message attribute** dialog box, select **Source Hostname** from the drop-down list, and add the hostname or domain that you want to include or exclude.
4. Click **Apply**.

Examples of source hostname entries and some of the hostnames that they match are shown in the table below. The hostname is determined through a reverse DNS lookup of the first untrusted relay (FUR) IP and the Trusted Relays list.

Source Hostname entry	Matches for Source Hostname entry
example.com or ***example.com**	example.com, mx1.example.com
.example	mx1.example.com, mx2.sub.example.net, mx3.example.org
mx*.example.com	mx1.example.com, mx15.example.com

Select Users



In the **Select Users** section, you can configure users and groups to be included or excluded with a policy rule.

- To configure which users or groups are affected by a policy rule:
  - Select the **Include Recipient** tab to specify which message recipients a rule will apply to.
  - Select the **Exclude Recipient** tab to specify which message recipients a rule will *not* apply to.
  - Select the **Include Sender** tab to specify which message senders a rule will apply to.
  - Select the **Exclude Sender** tab to specify which message senders a rule will *not* apply to.
- Within a tab:
  - Select **All users** if you want to configure the current tab so that it affects all users.
  - Select the **Selected groups** option if you want to configure the current tab so that it affects one or more existing groups. Groups listed in the **Available** table are available, but will not be used with this policy rule. Groups in the **Selected groups** table are configured for use with this policy rule.
    - Use the >> button to move available groups from the **Available** table to the **Selected groups** table.
    - Use the << button to remove groups from the **Selected groups** table, and back to the **Available** table.
  - Select **Custom groups** if you want to create custom groups. To add entries to a custom group:
    1. In the **Custom groups** text box, enter an email address.

       Note: You can enter wild-card characters in this text box to match on multiple addresses. For instance, `test?@*example.com` would match on both `test1@example.com` and `test3@mail.example.com`.

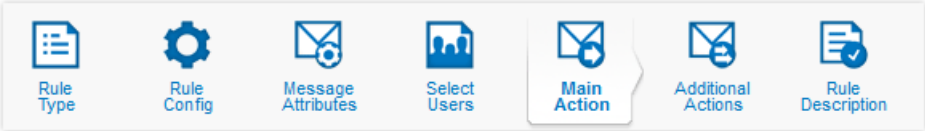
    2. Click **Add**. Optionally, click **Paste**, paste in a list of entries (one per line), and click **OK**.
  - To delete an address from the **Custom groups** table, select the check box next to its name, then click **Delete**.

    For more information about creating and managing groups, see “User Groups” in the Accounts section of the documentation.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Main Action



Configure the main action.

- From the drop-down list in the **Message actions** section, select the action to be taken if this rule is triggered:
  - **Continue Processing** to continue processing the message.

- **Deliver Immediately** to deliver the message immediately to the intended recipient(s) without triggering any subsequent policy rules.
- **Discard** to immediately discard the message.
- **Quarantine** to quarantine the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.

  Note: Only messages quarantined for the reason "spam" are accessible through the web quarantine and will be included in email quarantine summaries.

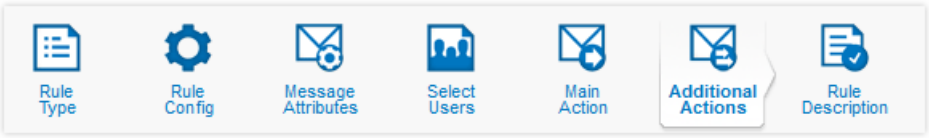
- **Quarantine and continue** to quarantine a copy of the message, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
- **Quarantine, drop file(s) and continue** to quarantine a copy of the message, drop any offending attachments, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
- **Redirect** to redirect the message to a specified email address. The original recipients will not receive the message. Specify the email address to which you want to redirect the mail to in the **Redirect email address** text box in the **Configuration** section.
- **Re-route message to another server** to send the message to another mail server. The message body, and the original sender and recipient information will be preserved, but the original recipients will not receive the message. To specify the mail server to which you want to redirect the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
- **Send a copy of the message to another server** to send the message to the original destination, and a copy of the message to another mail server. The message body and the original sender and recipient information will be preserved. To specify the mail server to which you want to send a copy of the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
- **Tag subject and continue** to tag the subject line of the message with the specified text, after which the email appliance will continue to process the message.

  Note: You can include the original subject of the message by using the %%SUBJECT%% template variable.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Additional Actions



In the **Additional Actions** section, you can configure extra actions.

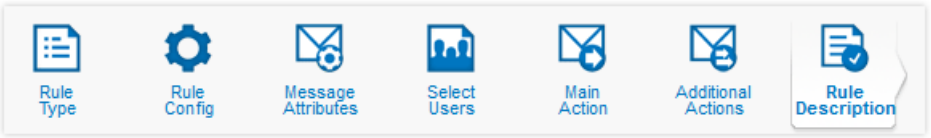
- To add a new action, click **Add**.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the new action, which is then displayed in the **Additional actions** table.
- To configure an existing action, click an action's description in the **Additional actions** table.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the action.
- To delete an action, select the check box next to the action description in the **Additional actions** table. Click **Delete**.
  The action will be removed from the **Additional actions** table.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.

- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Rule Description



To configure a rule description:

1. In the **Policy rule name** text box, enter or edit the description for the policy rule. This is the description that will appear in the rule table.
2. Select the **Activate this rule** check box.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Anti-Spam Example

If you wanted to quarantine messages with high spam scores for most users, but deliver messages addressed to a specific group:

1. In the **Inbound** anti-virus table, click **Add**.
   The Policy Wizard is displayed.
2. Select the **High spam** rule type. Click **Next**.
3. In the **Message attributes** section, click **Next**.
4. On the **Include Recipient** tab of the **Users & Groups** section, select **All Users.**
5. Select the **Exclude Recipient** tab of the **Users & Groups** section, and click **Selected groups**.
6. Select the group(s) you want to exclude, then click the >> button. Click **Next**.
7. In the **Message Actions** section, select **Quarantine**. Then select **Spam** in the **Configuration ➤ Quarantine for reason** section. Click **Next**.
8. In the **Additional Actions** section, click **Next**.
9. In the **Rule Description** section, enter a description for the rule. Select the **Activate this rule** check box.
10. Click **Apply**.

Important: It is possible to select the same user or group for more than one rule in a given spam category (high spam or medium spam). In cases where a particular user or group is defined in more than one rule in a category, the action for the first matching rule in the list takes precedence.

Data Control

The Data control policy allows you to create rules for monitoring or restricting messages and attachments based on content, filename, or file type.

Data control allows you to reduce accidental data loss from workstations by monitoring and restricting the transfer of files containing sensitive data.

Accidental data loss is commonly caused by employees mishandling sensitive data. For example, a user sends a file containing sensitive data home via web-based email.

The **Data Control** page allows you to configure both inbound and outbound rules. By default, there are default rules on the **Outbound** tab that are based on SophosLabs Content Control Lists (CCLs). The terms "inbound" and "outbound" refer to messages received by the Sophos Email Appliance, and messages delivered through the appliance.

Use the **Configuration ➤ Policy ➤ Data Control** page to configure CCLs and other data control options.

Data Control Policy Configuration

Use the **Configuration ➤ Policy ➤ Data Control** page to configure CCLs and other data control options.

- Select the **Outbound** or **Inbound** tab.
- To add a rule, click **Add** in the rules table.

  The Policy Wizard is displayed.
- To configure a rule, click the **Description** of the rule in the rules table.

  The **Configure Rule** dialog box is displayed.
- To change the priority of a rule:

  Click the up or down arrow buttons in the rules table, next to the **Description** of the rule or rules whose priority you want to change.

  After you have finished setting rule priorities:

  - Click the **Save order** button when you are satisfied with the order of the priorities.
  - Click the **Reset order** button to cancel and restore the rule priorities.

- You can also enable or disable existing rules.

  - An active rule is displayed in the rules table with a green **Active** icon, next to which is a **Turn Off** button. There is also a priority for an active rule.
  - An inactive rule is displayed in the rules table with a gray **Active** icon, next to which is a **Turn On** button. There is also no priority for an inactive rule, and it will not be processed.
  - To disable an active rule, click **Turn Off** in the rules table, next to the rule.
  - To enable an inactive rule, click **Turn On** in the rules table, next to the rule.

- To delete a rule, select the check box next to the rule in the table of rules, then click **Delete**.

Policy Wizard: Data Control

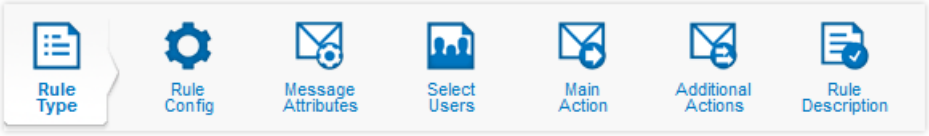
Each page of the Policy Wizard allows you to configure specific aspects of a rule's behavior, and can be thought of as answering a series of questions:

1. **What type of rule do you want to configure?** This is the first page presented by the Policy Wizard. Its contents are contextually based, and depend on whether you're in the Anti-Virus, Anti-Spam, or Additional Policy section when you enter the Policy Wizard. The choice made on this page defines the policy rule and any subsequent steps. It is the only rule attribute that cannot be changed after it has been created.
2. **How do you want a rule to trigger?** You can answer this question on the **Rule Config** and **Message Attributes** pages of the Policy Wizard by specifying what elements of a message will cause a policy rule to trigger.
3. **Who do you want the rule to apply to?** You can answer this question on the **Select Users** page of the Policy Wizard, where you can specify which groups, specific senders, or recipient email addresses can be included or excluded.
4. **What should happen when the rule is triggered?** You can answer this question on the **Main Action** page, and also on the **Additional Actions** page of the Policy Wizard. You can specify what actions will be performed on a message, or what action will be performed after the appliance receives a message that triggers this rule.
5. **How is this policy rule identified?** You can answer this question on the **Rule Description** page of the Policy Wizard, where you can provide a description of the rule.

Depending on the rule type, and whether you have selected **Enable advanced policy options**, some sections may not be enabled for configuration.

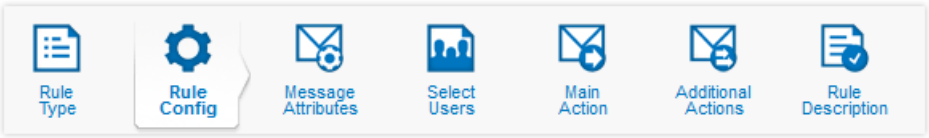
Note: If you are adding a rule for the first time, you must proceed through the configuration items in sequence. If you are configuring a rule that already exists, you can select a specific action to configure by clicking on its icon.

Rule Type



1. Select one of the following rule types:
   - **Messages containing financial information**: Detect and take action on messages containing credit or debit card information. This protects sensitive data and helps to meet compliance requirements such as those defined in Payment Card Industry (PCI) and Sarbanes-Oxley (SoX) regulations. This rule uses Sophos Content Control Lists (CCLs), which you can configure further in the "Rule Type" section of the wizard, if **Enable advanced policy options** is selected.
   - **Messages containing personally-identifiable information**: Detect and take action on messages containing personal information like addresses, phone numbers, or email addresses. This protects sensitive data and helps to meet compliance requirements, such as those defined in the Health Insurance Portability and Accountability Act (HIPAA) regulations. This rule uses Sophos Content Control Lists (CCLs), which you can configure further in the "Rule Type" section of the wizard, if **Enable advanced policy options** is selected.
   - **Messages containing attachments with confidential document markers**: Detect and take action on messages containing attachments that have been marked as 'confidential'. This CCL contains several specific keywords, including "Confidential" and "Secret." Attachments that contain these keywords are detected when this list is applied. This rule uses Sophos Content Control Lists (CCLs), which you can configure further in the "Rule Type" section of the wizard, if **Enable advanced policy options** is selected.
   - **Messages matching specific Sophos Content Control Lists (CCLs)**: Detect sensitive data such as credit card numbers, social security numbers (SSNs), personally identifiable information (PII), etc, using Sophos Content Control Lists (CCLs). Sophos CCLs are XML-based descriptions of structured data. They are managed and updated by SophosLabs to provide an easy and effective way to address data leakage prevention (DLP) and other data protection concerns. Use standard SophosLabs-managed CCLs or import custom CCLs created in Sophos Enterprise Console.
   - **Messages matching specific words or phrases**: Search for keywords in messages using keywords or regular expressions. Keyword lists are often used for data leakage prevention, detection of inappropriate behavior, etc.
   - **Messages containing certain types of attachments**: Detect certain types of files attached to messages. This type of list is typically used for restricted or allowed attachment lists. Both the file extension and the actual file type as reported by the Sophos Anti-Virus Engine are used to detect the attachment file type.
2. [Optional] Select **Enable advanced policy options** to make all additional wizard options available. Certain steps in the wizard are grayed out, according to the selected rule type.
3. Click **Next**.

Rule Config: Content Control Lists



Depending on which options you selected during the **Rule Type** stage of the wizard, you may be presented with a "Rule Config" wizard page for configuring Content Control Lists (CCLs).

One or more CCLs are automatically selected, based on your rule type selection. You can add other CCLs to the rule by selecting the check box next to a rule. When you click on a CCL name, a summary of that CCL is displayed in the **Description** box.

Optionally, you can import a custom CCL that was created in Sophos Enterprise Console. See “Importing Content Control Lists” for more information.

Custom lists are displayed in **Content control lists** scroll box, along with the SophosLabs CCLs. Unlike SophosLabs rules, the quantity settings for custom CCLs must be configured in Sophos Enterprise Console.

Custom lists are shown with the name and description assigned to them in Sophos Enterprise Console. Any details that were specified are displayed in the **Description** box when you click the name of the custom CCL

To configure a CCL-based rule:

- On the **Content Control Lists** tab:
  a) From the **Filter by region** drop-down list, select the country for which you want the rule to apply. To filter for all countries, select **All**.
  The name of the selected region will be displayed in brackets after the CCL name. If this drop-down list is set to **All**, the CCL will be tagged as **[Global]**.
  b) From the **type** drop-down list, select the type of data you want to display, or select **All** to show all data types.
  c) By default, the **All CCLs** option button is selected, which means the complete list of available CCLs is displayed. If you only want to see the CCLs that have been applied to this rule, select **Only active (selected) CCLs**.
  d) Click on an individual rule to set the quantity for each CCL, or use the default that is set by SophosLabs. See *CCL Configuration* (page 205) for details.
  e) If you selected **Messages matching specific Sophos Content Control Lists (CCLs)** on the **Rule Type** page, or if you want to select additional rules, select the check box next to each rule.
  f) Enter the number of CCL matches that are required to trigger this rule in the text box of **[n] of the CCLs must match**. By default **n** is set to **1**. Optionally, if you want all of the CCLs to match before the rule is triggered, select **All of the CCLs must match**.

  Important: On the following tabs, you must select one or both of **Match Content Control Lists (CCLs) within message parts** or **Match Content Control Lists (CCLs) within attachments**, or you will not be able to proceed to the next step of the wizard.

- On the **Inspect message parts** tab, configure whether the rule searches for CCL matches within the message body and message subject. By default, the rule will match CCLs within the message body, but not the message subject. When this option is enabled, you must select one or both of **Include message body** or **Include subject**.
  - Use the **Match Content Control Lists (CCLs) within message parts** check box to enable or disable matching within message parts.
  - Use the **Include message body** check box to select whether the rule will match CCLs within the message body.
  - Use the **Include subject** check box to select whether the rule will match CCLs within the message subject.
- On the **Inspect attachments** tab, the **Match Content Control Lists (CCLs) within attachments** option searches for matches inside of attachments. This check box is selected by default. Clear this box only if you do not want to search within attachments.
- Select the **Logging** tab if you want to enable and configure logging of CCL-based rules.

  Although logging is off by default, you can configure the manner in which CCL-based rules are logged. The logging level varies, depending on what is selected in the **CCL Logging** dialog box.

  If logging is off, an entry is still added indicating simply that a CCL policy rule was triggered. If you choose to include more CCL information in the logs, you can view this by clicking **View log details** in the search results.

  Note: Logging for each CCL-based rule is configured separately. You must complete the steps shown below for each rule that you want to log.

  a) Click **Configure**.
  The **CCL Logging** dialog box is displayed.
  b) Select one or more of the following **Log Level** options:
    - **Log CCL violations**: When enabled, an entry is added to the logs indicating which CCL list was triggered.
    - **Include matched text**:

      When enabled, the logs will also include the exact test that triggered the violation.

Caution: Logging matched text results in sensitive data being stored on the appliance, and, potentially, backed up to your FTP server. The data is stored in a format that is not encrypted.

- **Include partial matches**: When enabled, an entry is added to the logs whenever there is message that contains many of the characteristics identified in a CCL, but not enough to trigger a rule.

Importing a Custom Content Control List (CCL)

Although the appliance includes many Content Control Lists (CCLs) that are prepared and maintained by SophosLabs, you can create your own CCL, if necessary. These custom lists are created in Sophos Enterprise Console and exported as XML to a file location that is accessible to the Email Appliance. For more about exporting custom CCLs, see the Sophos Enterprise Console documentation.

To import a custom CCL:

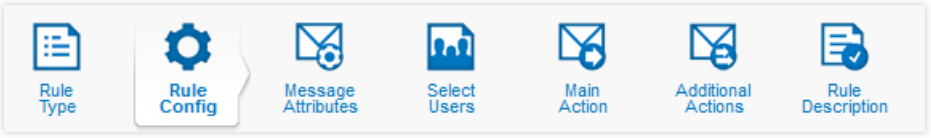
1. Under **Content control lists**, click **Import**.
   The **CCL Import** dialog box is displayed.
2. Click **Browse** to navigate to the location where the CCL was exported, and select the file.
3. [Optional] Select **Force overwrite of existing CCL of the same name** if you want to replace any existing CCLs that have the same filename.
4. Click **OK**.
   The custom CCL is displayed in the **Content control lists** scroll box. The file is displayed with name that was specified during creation in Sophos Enterprise Console.

To remove an imported custom CCL from the list of CCLs:

1. Click the garbage can icon next to the CCL that you want to remove.

   The **Delete CCL** dialog box is displayed.
2. Click **OK**.

Rule Config: Keyword list



Add, delete or view the keyword entries for a rule.

- Select the **String** or **Regular Expression** tab.
- To add keywords:
  - Enter a keyword or regular expression in the **Add Entries** section text box, then click **Add**, or:
  - Click **Upload** to upload a list of keywords or regular expressions from a text file.

  Entries will appear in the **Entries** table.
- Select the **Match keyword entries within attachments** check box to enable the appliance to also search for keywords inside of supported attachment types.

  Note: Certain keyword entries that make extensive use of wildcards, such as "*example*", may cause large attachments to be processed slowly. It is important to ensure that you are familiar with wildcards and regular expressions before using them in keyword lists.

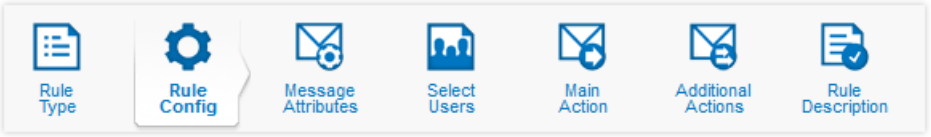
- To delete a keyword or regular expression, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of keywords or regular expressions. The number of pages, as well as the page number that you are viewing, will be indicated above the **Entries** table.

  - To move to a specific page, enter the page number in the page number text box, then press **Enter** .
  - Click the > button to move forward one page.
  - Click the < button to move backward one page.
  - Click the << button to move to the first page of entries.
  - Click the >> button to move to the last page of entries.
- To search for a keyword or regular expression, enter your query in the **Find** text box, then click **Find Next**.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move to the previous or next configuration section.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Rule Config: Attachment type



Add, edit or view the attachments or file types that will be tested by a rule.

- To add attachment filenames or file extensions:
  - Enter a filename or file type extension in the text box in the **Add Entries** section, then click **Add**, or:
  - Click **Upload** to upload a list of file names or file type extensions from a text file.

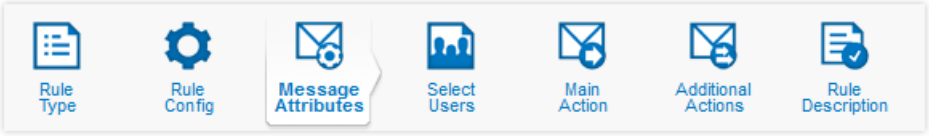
  Entries will appear in the **Entries** table.

  Note: To match all files with a given file type extension, use an entry with a form similar to **.exe*.
- To edit a filename or file type extension, click on its description in the **Entries** table.
- To delete a filename or file type extension, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of filenames or file type extensions. The number of pages, as well as the page number that you are viewing, will be indicated above the **Entries** table.
  - To move to a specific page, enter the page number in the page number text box, then press **Enter** .
  - Click the > button to move forward one page.
  - Click the < button to move backward one page.
  - Click the << button to move to the first page of entries.
  - Click the >> button to move to the last page of entries.
- To search for a filename or file type extension, enter your query in the **Find** text box, then click **Find Next**.
- If you want to configure the "Entries" list as an exclusions list, select **Exclude listed attachment types**. When this check box is enabled, all files except those listed will trigger this policy rule.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Message Attributes



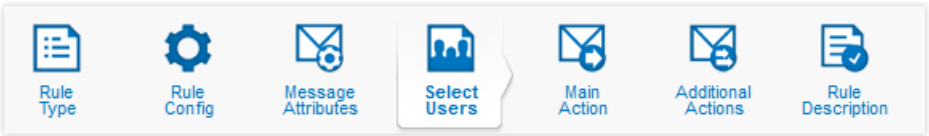
Add, edit or delete additional message attributes that will trigger a rule.

- *To add a new message attribute*, click **Add**.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- *To edit a message attribute*, click the attribute description in the **Identify message attributes** table.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- *To delete a message attribute*, select the check box next to the attribute description in the **Identify message attributes** table, then click **Delete**.
  The message attribute will be removed from the **Identify Message Attributes** table.
- [Optional] *To set the matching condition for attributes*, under **Matching logic**, select either **All message attributes must be present**, or **One of the message attributes must be present**. This option is unavailable unless at least two message attributes are specified.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Select Users



In the **Select Users** section, you can configure users and groups to be included or excluded with a policy rule.

- To configure which users or groups are affected by a policy rule:
  - Select the **Include Recipient** tab to specify which message recipients a rule will apply to.
  - Select the **Exclude Recipient** tab to specify which message recipients a rule will *not* apply to.
  - Select the **Include Sender** tab to specify which message senders a rule will apply to.
  - Select the **Exclude Sender** tab to specify which message senders a rule will *not* apply to.
- Within a tab:
  - Select **All users** if you want to configure the current tab so that it affects all users.
  - Select the **Selected groups** option if you want to configure the current tab so that it affects one or more existing groups. Groups listed in the **Available** table are available, but will not be used with this policy rule. Groups in the **Selected groups** table are configured for use with this policy rule.
    - Use the >> button to move available groups from the **Available** table to the **Selected groups** table.
    - Use the << button to remove groups from the **Selected groups** table, and back to the **Available** table.
  - Select **Custom groups** if you want to create custom groups. To add entries to a custom group:

    1. In the **Custom groups** text box, enter an email address.

       Note: You can enter wild-card characters in this text box to match on multiple addresses. For instance, `test?@*example.com` would match on both `test1@example.com` and `test3@mail.example.com`.

2. Click **Add**. Optionally, click **Paste**, paste in a list of entries (one per line), and click **OK**.

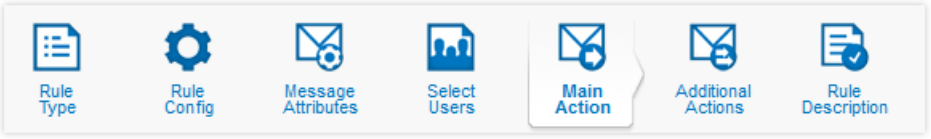
- To delete an address from the **Custom groups** table, select the check box next to its name, then click **Delete**.

  For more information about creating and managing groups, see “User Groups” in the Accounts section of the documentation.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Main Action



Configure the main action.

- From the drop-down list in the **Message actions** section, select the action to be taken if this rule is triggered:
  - **Continue Processing** to continue processing the message.
  - **Deliver Immediately** to deliver the message immediately to the intended recipient(s) without triggering any subsequent policy rules.
  - **Discard** to immediately discard the message.
  - **Encrypt the message using SPX** to encrypt the message using the SPX options configured in the template selected in the **Template** drop-down list. This action is only available for outbound messages.

    You can also:

    - Select **Attach original email to PDF** if you want recipients to have the option of receiving an additional, unencrypted version of the email message. Doing so ensures that recipients can save an unencrypted copy of the email message once they have received and successfully opened an SPX email. Although they can save the PDF itself, it must be decrypted each time it is opened.
    - Opt to have the sender receive a registration confirmation.
    - Opt to *always* have the sender receive an encryption notification.
    - Select how a message will be handled if it cannot be delivered; on failure, you can choose to bounce the message to the **Sender**, the **Administrator**, or both the **Sender and Administrator**.
  - **Quarantine** to quarantine the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.

    Note: Only messages quarantined for the reason "spam" are accessible through the web quarantine and will be included in email quarantine summaries.

  - **Quarantine and continue** to quarantine a copy of the message, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
  - **Quarantine, drop file(s) and continue** to quarantine a copy of the message, drop any offending attachments, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
  - **Redirect** to redirect the message to a specified email address. The original recipients will not receive the message. Specify the email address to which you want to redirect the mail to in the **Redirect email address** text box in the **Configuration** section.
  - **Re-route message to another server** to send the message to another mail server. The message body, and the original sender and recipient information will be preserved, but the original recipients will not receive the message. To specify

the mail server to which you want to redirect the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.

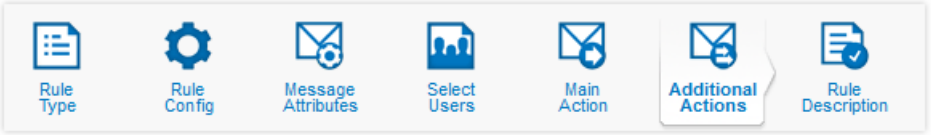
- **Send a copy of the message to another server** to send the message to the original destination, and a copy of the message to another mail server. The message body and the original sender and recipient information will be preserved. To specify the mail server to which you want to send a copy of the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
- **Tag subject and continue** to tag the subject line of the message with the specified text, after which the email appliance will continue to process the message.

Note: You can include the original subject of the message by using the %%SUBJECT%% template variable.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Additional Actions



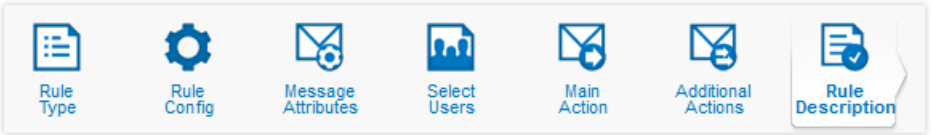
In the **Additional Actions** section, you can configure extra actions.

- To add a new action, click **Add**.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the new action, which is then displayed in the **Additional actions** table.
- To configure an existing action, click an action's description in the **Additional actions** table.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the action.
- To delete an action, select the check box next to the action description in the **Additional actions** table. Click **Delete**.
  The action will be removed from the **Additional actions** table.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Rule Description



To configure a rule description:

1. In the **Policy rule name** text box, enter or edit the description for the policy rule. This is the description that will appear in the rule table.
2. Select the **Activate this rule** check box.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.

- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Data Control Deployment Guide

Creating Data Control policy rules requires both planning and testing. It is also important to choose rules that best suit your organization, and then configure them in a way that prevents data loss. Review the guidelines shown below before testing and implementing rules that are based on SophosLabs Content Control Lists (CCLs).

Note: This document describes the configuration, testing, and implementation of SophosLabs rules only. If you are using custom CCLs, they must be created and edited in Sophos Enterprise Console. For more information, see the Enterprise Console documentation.

Best Practices

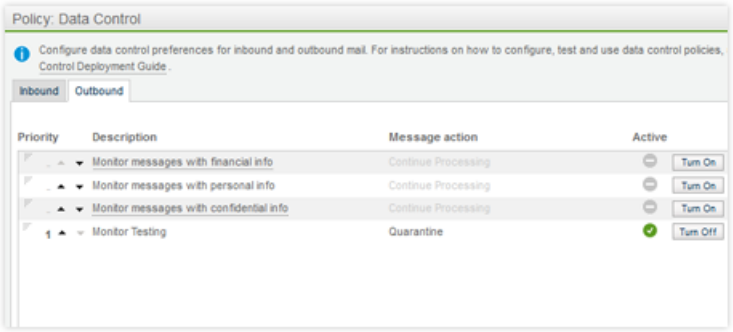
There are various considerations when creating a data control policy for your organization. Review the following guidelines before creating data control rules on the Sophos Email Appliance:

- Content scanning can be a resource-intensive process, and it may affect system performance. This should be considered when creating content rules, and implementing a large number of CCLs. It is important to test the impact of a content rule prior to applying it across a large number of users. Deploy your data control policy to a smaller group of pilot users to make it easier to analyze data control events triggered by the policy.
- Create different policies for different groups. For example, you may want to allow users within the finance department to transfer financial information outside of your organization, but prevent all other groups from doing so.
- Consider what types of information you want to identify and create rules for. Sophos provides a set of sample policy rules on the **Outbound** tab of the **Data Control** page that you can use to help build your data control policy.
- Although logging of rules based on Content Control Lists (CCLs) is off by default, you can enable various levels of logging in the rule configuration section of the Policy Configuration Wizard. It is important to keep in mind that, in a production environment, selecting **Include matched text** results in sensitive data being stored on the appliance, and, potentially, backed up to your FTP server. This data is not encrypted.

Deploying CCL-Based Rules

1. **Inspect the initial configuration**

   Several disabled default rules are provided on the **Outbound** tab of the **Configuration ➤ Policy ➤ Data Control** page. You can use these default rules to see which messages cause particular rules to trigger. By default, logging and copying to the quarantine is disabled.



   See the **Description** box on the **Rule Type** page of the Policy Wizard for details of the selected rule.

   a. **Select a rule:** Click on a default rule that matches the type of sensitive data you want to secure. This will open the Policy Wizard for the data control policy rules, where you can review the settings of the rule, and adjust them to match your requirements.
   b. **Configure the CCL(s):** On the **Rule Config** page of the Policy Wizard, you can check that suitable CCLs are enabled, and you can configure the **quantity** for each CCL.

Note: The quantity is a measure of a weighted number of matches a rule needs to find in a message before the rule will trigger. Increasing the quantity will make the rule less likely to trigger, and decreasing the quantity will have the opposite effect.

c. **Select the users:** When configuring the rule, you want to ensure that its impact is limited. With this in mind, select a small test group of pilot users for whom the rule will be used.
d. **Select a Main Action:** Selecting the **Quarantine and continue** option for a CCL makes it simpler to check the effectiveness of the rule.
e. **Check notifications:** Ensure that notifications are sent to the correct people for testing purposes.
f. **Save and activate the rule:** Save the rule, then make it active by clicking the **Turn On** button next to the rule name.

2. **Calibrate and test data control rules**

You should audit and calibrate a rule's effectiveness before deploying it for all of your users.

a. **Enable logging:** On the **Rule Config** page of the Policy Wizard, you can set the logging level for each rule. The progressive log levels each provide more information as to why a rule was triggered and allow you to monitor the effectiveness of the rules for your particular application. While testing, it is recommended that you select all of the following:

- **Log CCL violations** will add log entries showing which CCL list was triggered.
- **Include matched text** will also include the exact text that triggered the rule.

  Note: Logging matched text causes sensitive data to be stored on the appliance, and, potentially, backed up to your FTP server. The data is stored in a format that is not encrypted.

- **Include partial matches** will add entries to the logs whenever there is message that contains many of the characteristics identified in a CCL, but not enough to trigger a rule.

b. **Adjust the quantity setting for each rule:** Each CCL has a quantity setting that can be adjusted on the **Rule Config** page of the **Configuration ➤ Policy ➤ Data Control** Policy Wizard. If, after examining your logs, you find that a CCL is triggering too frequently, you can adjust the quantity setting upwards to decrease sensitivity.

Important: CCL default quantity settings are designed to provide a balance between false positives and reducing accidental data loss. To test a given CCL, it is recommended that you ensure that its quantity setting is '1'. If necessary, you can adjust the CCL quantity settings upward.

c. **Test the rule:** After you have selected and configured a rule, you will want to ensure that you can check whether the rule is working as you expect. To allow a more thorough analysis of the rule's operation, additional actions can be configured to provide more extensive information:

- If logging is enabled, you can choose to notify the administrator by using the %%CCL_HITS%% template variable. This will send the administrator the data that is triggering the rule.

  Note: Only the data that has caused the rule to trigger is provided by this template variable, after which the rule will stop processing and register a violation. However, there may be additional sensitive data contained in the triggering email that can be seen by viewing the email itself.

- Copy the message to the quarantine. The administrator can then view the entire message that triggered the rule.

d. **Search the mail logs:** You can use the **Search** tab to check the logs and quarantine to see what effect the adjustment has had. Now you can see whether the CCLs are triggering, and what is causing them to trigger. To do this:

- Perform a log search on the **Search** tab.
- Click **View log details**.
- A popup is displayed where you can view a list of which CCLs triggered on the **Content inspection** tab.
- To view the data that caused a specific CCL violation or warning, click the expand (+) icon next to each CCL. The red icons indicate violations, while yellow icons indicate warnings. Click **Expand All** to view details of all CCLs.

e. **Search the quarantine:** Since log searches only provide the data that caused the rule to trigger, you may want to also view the entire message in the quarantine. To do this:

- Perform a quarantine search by way of the **Search** tab.
- Click on the email you want to view.
- Click **View message details** to display the **Message Details** popup.

You can view the complete message on the **Body** tab, and information about the data control policy rule that triggered on the **Info** tab.

f. **Adjust rule settings:** If the rule is not working as expected, you can:

- Change the selection of CCLs that the rule uses.
- Change the **Quantity** setting for a CCL.

After changing the settings, check the effectiveness of the rule again, using the steps described above. Continue to refine the settings until the rule works the way you want it to. If you still experience unexpected behaviour with data control policies or CCLs, contact Sophos Technical Support, or consider consulting Sophos Professional Services.

3. **Production Deployment**

After you are satisfied that the rule is working as expected, you can activate the rule for all intended users. For email that triggers the rule, it is suggested that you choose one of the following common actions:

- Encrypt the message using SPX encryption.
- Block the message and notify the sender.
- Quarantine the message for further review.

These options can be selected on the **Main Action** page of the Policy Wizard.

After activating the rule, you should consider whether you want to disable logging and quarantining of messages.

Rule Examples

You can use the sample rules on the **Outbound** tab as-is, build rules that are based on these rules, or use the Policy Wizard to create new rules. Launch the Policy Wizard by clicking **Add** on the **Inbound** or **Outbound** tab of the **Data Control** page.

For sample rules that are designed to cover common data control scenarios, see the *Data Control Examples* in the Sophos Knowledgebase. These examples are only intended to provide guidelines. Configure rules as necessary to address the needs of your organization.

Content Control Lists

The matching of file content is defined using a Content Control List (CCL). This is an XML-based description of structured data. SophosLabs provides an extensive set of CCLs. If necessary, however, you can create custom lists using Sophos Enterprise Console, a single, automated console that centrally deploys and manages Sophos security software.

A CCL is made up of conditions that describe structured file content. It may describe a single type of data (for example, a postal address or social security number), or a combination of data types (for example, a project name near to the term "confidential").

Tip:

With the Sophos Enterprise Console, you can:

- Protect your network against viruses, Trojans, worms, spyware, and unknown threats, as well as adware and other potentially unwanted applications.
- Control which applications can run on the network.
- Manage client firewall protection on endpoint computers.
- Assess computers' compliance with the conditions you set before they are allowed to log on to the network and enforce compliance.

- Reduce accidental data loss, such as unintentional transfer of sensitive data, from endpoint computers.

SophosLabs CCLs provide expert definitions for common financial and personally identifiable data types, for example, credit card numbers, social security numbers, postal addresses, or email addresses. Advanced techniques, such as checksums, are used in SophosLabs CCLs to increase the accuracy of sensitive data detection.

You cannot edit SophosLabs CCLs, but you can submit a request to Sophos to create a new SophosLabs CCL. For details, see *How to get additional items added to Content Control Lists* in the Sophos Knowledgebase.

Additional Policy

Use the **Configuration ➤ Policy ➤ Additional Policy** page to configure how to handle messages based on various rule types. You can add, edit or turn off existing rules. Rules can be added for the following types:

- Add banner
- Keyword list
- Attachment type list
- Offensive language
- Watch list
- Hostname/IP address list
- Use only message attributes
- Bulk email messages.

The **Policy: Additional Policy** page defines rules for inbound and outbound messages separately.

Each of these rules has a number of configuration options available. See “Configuring Policy Rules with the Policy Wizard” for more information.

Additional Policy Configuration

Use the **Configuration ➤ Policy ➤ Additional Policy** page to configure policy rules for offensive language, specified keywords, watch lists, and banners.

- Select the **Outbound** or **Inbound** tab.
- To add a rule, click **Add** in the rules table.

  The Policy Wizard is displayed.
- To configure a rule, click the **Description** of the rule in the rules table.

  The **Configure Rule** dialog box is displayed.
- To change the priority of a rule:

  Click the up or down arrow buttons in the rules table, next to the **Description** of the rule or rules whose priority you want to change.

  After you have finished setting rule priorities:

  - Click the **Save order** button when you are satisfied with the order of the priorities.
  - Click the **Reset order** button to cancel and restore the rule priorities.

- You can also enable or disable existing rules.

  - An active rule is displayed in the rules table with a green **Active** icon, next to which is a **Turn Off** button. There is also a priority for an active rule.
  - An inactive rule is displayed in the rules table with a gray **Active** icon, next to which is a **Turn On** button. There is also no priority for an inactive rule, and it will not be processed.
  - To disable an active rule, click **Turn Off** in the rules table, next to the rule.
  - To enable an inactive rule, click **Turn On** in the rules table, next to the rule.

- To delete a rule, select the check box next to the rule in the table of rules, then click **Delete**.

Policy Wizard: Additional Policy

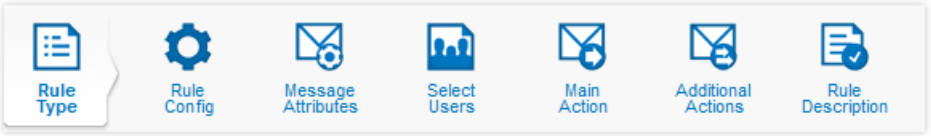
Each page of the Policy Wizard allows you to configure specific aspects of a rule's behavior, and can be thought of as answering a series of questions:

1. **What type of rule do you want to configure?** This is the first page presented by the Policy Wizard. Its contents are contextually based, and depend on whether you're in the Anti-Virus, Anti-Spam, or Additional Policy section when you enter the Policy Wizard. The choice made on this page defines the policy rule and any subsequent steps. It is the only rule attribute that cannot be changed after it has been created.
2. **How do you want a rule to trigger?** You can answer this question on the **Rule Config** and **Message Attributes** pages of the Policy Wizard by specifying what elements of a message will cause a policy rule to trigger.
3. **Who do you want the rule to apply to?** You can answer this question on the **Select Users** page of the Policy Wizard, where you can specify which groups, specific senders, or recipient email addresses can be included or excluded.
4. **What should happen when the rule is triggered?** You can answer this question on the **Main Action** page, and also in the **Additional Actions** page of the Policy Wizard. You can specify what actions will be performed on a message, or what action will be performed after the appliance receives a message that triggers this rule.
5. **How is this policy rule identified?** You can answer this question in the **Rule Description** page of the Policy Wizard, where you can provide a description of the rule.

Depending on the rule type, and whether you have selected **Enable advanced policy options**, some sections may not be enabled for configuration.

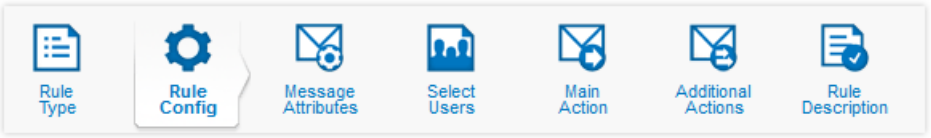
Note: If you are adding a rule for the first time, you must proceed through the configuration items in sequence. If you are configuring a rule that already exists, you can select a specific action to configure by clicking on its icon.

Rule Type



1. Select one of the following rule types:
   - **Add Banner**: Add a banner to the top or bottom of the message. This type of rule is typically used to add legal banners to outgoing messages, acceptable use reminders for incoming messages, etc.
   - **Keyword list**: Search for keywords in messages using keywords or regular expressions. Keyword lists are often used for data leakage prevention, detection of inappropriate behavior, etc.
   - **Attachment type list**: Detect certain types of files attached to messages. This type of list is typically used for restricted or allowed attachment lists. Both the file extension and the file type as reported by Sophos Anti-Virus Engine are used to detect the attachment file type.
   - **Offensive language**: Detect the use of offensive language in messages. Sophos provides an initial list of offensive words that can be used as a starting point for creating a list of offensive language that is customized to your environment.
   - **Watch list**: Detect messages being sent or received by specific users, groups, or email addresses. This type of list is typically used for monitoring possible misuse of email by specific users or groups.
   - **Hostname/IP address list**: Detect messages originating from specific hosts or IP addresses. This type of list is typically used to implement policies specific to servers operated by trusted or untrusted entities.
   - **Use only message attributes**: Use message attributes to trigger this policy rule. Valid message attributes to detect include message size, attachment size, headers, and the source IP address of the message.
   - **Bulk email messages**: You can use a **Bulk email messages** policy rule to detect opt-in bulk email messages, such as those from mailing lists, advertisers, political parties, and others that users have opted to receive mail from.
2. [Optional] Select **Enable advanced policy options** to make all additional wizard options available. Certain steps in the wizard are grayed out, according to the selected rule type.
3. Click **Next**.

Rule Config: Keyword list



Add, delete or view the keyword entries for a rule.

- Select the **String** or **Regular Expression** tab.
- To add keywords:
  - Enter a keyword or regular expression in the **Add Entries** section text box, then click **Add**, or:
  - Click **Upload** to upload a list of keywords or regular expressions from a text file.

  Entries will appear in the **Entries** table.
- Select the **Match keyword entries within attachments** check box to enable the appliance to also search for keywords inside of supported attachment types.

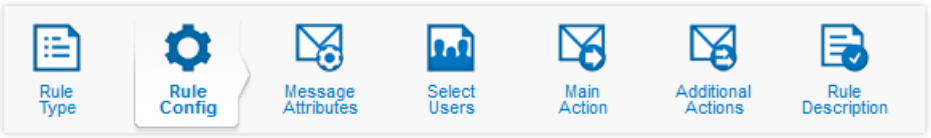
  Note: Certain keyword entries that make extensive use of wildcards, such as "*example*", may cause large attachments to be processed slowly. It is important to ensure that you are familiar with wildcards and regular expressions before using them in keyword lists.

- To delete a keyword or regular expression, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of keywords or regular expressions. The number of pages, as well as the page number that you are viewing, will be indicated above the **Entries** table.
  - To move to a specific page, enter the page number in the page number text box, then press **Enter** .
  - Click the > button to move forward one page.
  - Click the < button to move backward one page.
  - Click the << button to move to the first page of entries.
  - Click the >> button to move to the last page of entries.
- To search for a keyword or regular expression, enter your query in the **Find** text box, then click **Find Next**.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move to the previous or next configuration section.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Rule Config: Attachment type



Add, edit or view the attachments or file types that will be tested by a rule.

- To add attachment filenames or file extensions:
  - Enter a filename or file type extension in the text box in the **Add Entries** section, then click **Add**, or:
  - Click **Upload** to upload a list of file names or file type extensions from a text file.

  Entries will appear in the **Entries** table.

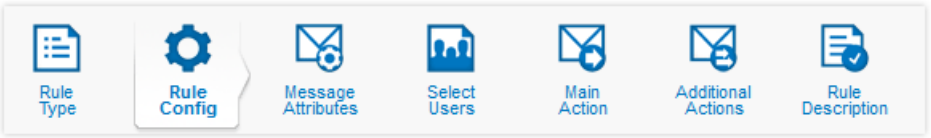
  Note: To match all files with a given file type extension, use an entry with a form similar to *.*exe*.

- To edit a filename or file type extension, click on its description in the **Entries** table.
- To delete a filename or file type extension, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of filenames or file type extensions. The number of pages, as well as the page number that you are viewing, will be indicated above the **Entries** table.
    - To move to a specific page, enter the page number in the page number text box, then press **Enter** .
    - Click the > button to move forward one page.
    - Click the < button to move backward one page.
    - Click the << button to move to the first page of entries.
    - Click the >> button to move to the last page of entries.
- To search for a filename or file type extension, enter your query in the **Find** text box, then click **Find Next**.
- If you want to configure the "Entries" list as an exclusions list, select **Exclude listed attachment types**. When this check box is enabled, all files except those listed will trigger this policy rule.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Rule Config: Offensive language



Add, edit or view the offensive language entries for this rule.

- Select the **String** or **Regular Expression** tab.
- To add offensive language entries:
    - Enter a string or a regular expression in the text box in the **Add Entries** section, then click the **Add**, or:
    - Click **Upload** to upload a list of offensive language or regular expressions from a text file.

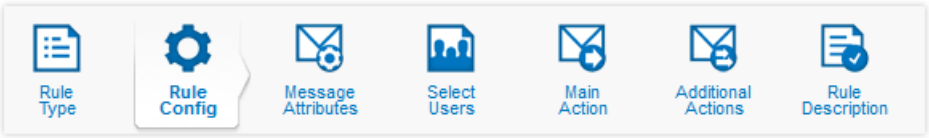
  Entries will appear in the **Entries** table.
- Select the **Match keyword entries within attachments** check box to enable the appliance to also search for keywords inside of supported attachment types.
- To edit offensive language or a regular expresson, click on its description in the **Entries** table.
- To delete offensive language or a regular expression, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of offensive language or regular expressions. The number of pages, as well as the page number that you are viewing, will be indicated above the **Entries** table.
    - To move to a specific page, enter the page number in the page number text box, then press **Enter** .
    - Click the > button to move forward one page.
    - Click the < button to move backward one page.
    - Click the << button to move to the first page of entries.
    - Click the >> button to move to the last page of entries.
- To search for an offensive language entry, enter your query in the **Find** text box, then click **Find Next**.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.

- Click **Previous** or **Next** to move to the previous or next configuration section.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Rule Config: Hostname/IP address list



Add, edit or view the hostnames or IP addresses that will be tested by this rule

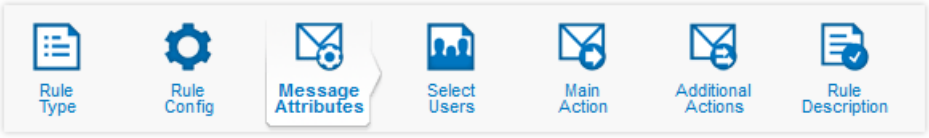
- To add hostnames or IP addresses:
  - Enter a hostname or IP address in the text box in the **Add Entries** section, then click **Add**, or:
  - Click **Upload** to upload a list of hostnames or IP addresses from a text file.

  Entries will appear in the **Entries** table.
- To edit a hostname or IP address, click on its description in the **Entries** table.
- To delete a hostname or IP address, select the check box next to its description in the **Entries** table, then click **Delete**.
- There may be more than one page of hostnames/IP addresses. The number of pages, and the page number that you are viewing, will be indicated above the **Entries** table.
  - To move to a specific page of entries, enter the page number in the page number text box, then press **Enter** .
  - Click the > button to move forward one page.
  - Click the < button to move backward one page.
  - Click the << button to move to the first page of entries.
  - Click the >> button to move to the last page of entries.
- To search for a hostname or IP address, enter your query in the **Find** text box, then click **Find Next**.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move to the previous or next configuration section.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Message Attributes



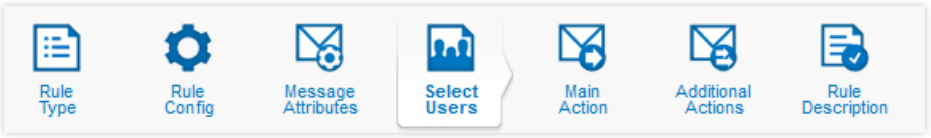
Add, edit or delete additional message attributes that will trigger a rule.

- *To add a new message attribute,* click **Add**.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- *To edit a message attribute*, click the attribute description in the **Identify message attributes** table.
  The *Add Message Attribute* (page 194) dialog box is displayed.
- *To delete a message attribute*, select the check box next to the attribute description in the **Identify message attributes** table, then click **Delete**.
  The message attribute will be removed from the **Identify Message Attributes** table.
- [Optional] *To set the matching condition for attributes,* under **Matching logic**, select either **All message attributes must be present**, or **One of the message attributes must be present**. This option is unavailable unless at least two message attributes are specified.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Select Users



In the **Select Users** section, you can configure users and groups to be included or excluded with a policy rule.

- To configure which users or groups are affected by a policy rule:
  - Select the **Include Recipient** tab to specify which message recipients a rule will apply to.
  - Select the **Exclude Recipient** tab to specify which message recipients a rule will *not* apply to.
  - Select the **Include Sender** tab to specify which message senders a rule will apply to.
  - Select the **Exclude Sender** tab to specify which message senders a rule will *not* apply to.
- Within a tab:
  - Select **All users** if you want to configure the current tab so that it affects all users.
  - Select the **Selected groups** option if you want to configure the current tab so that it affects one or more existing groups. Groups listed in the **Available** table are available, but will not be used with this policy rule. Groups in the **Selected groups** table are configured for use with this policy rule.
    - Use the >> button to move available groups from the **Available** table to the **Selected groups** table.
    - Use the << button to remove groups from the **Selected groups** table, and back to the **Available** table.
  - Select **Custom groups** if you want to create custom groups. To add entries to a custom group:

    1. In the **Custom groups** text box, enter an email address.

       Note: You can enter wild-card characters in this text box to match on multiple addresses. For instance, `test?@*example.com` would match on both `test1@example.com` and `test3@mail.example.com`.

    2. Click **Add**. Optionally, click **Paste**, paste in a list of entries (one per line), and click **OK**.

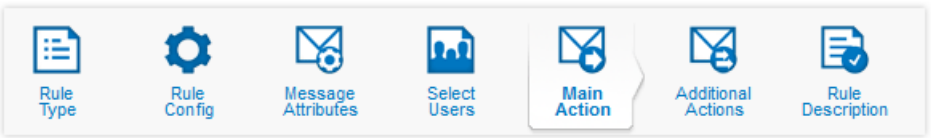
  - To delete an address from the **Custom groups** table, select the check box next to its name, then click **Delete**.

    For more information about creating and managing groups, see “User Groups” in the Accounts section of the documentation.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Main Action



Configure the main action.

- From the drop-down list in the **Message actions** section, select the action to be taken if this rule is triggered:
  - **Continue Processing** to continue processing the message.
  - **Deliver Immediately** to deliver the message immediately to the intended recipient(s) without triggering any subsequent policy rules.
  - **Discard** to immediately discard the message.
  - **Encrypt the message using SPX** to encrypt the message using the SPX options configured in the template selected in the **Template** drop-down list. This action is only available for outbound messages.

    You can also:

    - Select **Attach original email to PDF** if you want recipients to have the option of receiving an additional, unencrypted version of the email message. Doing so ensures that recipients can save an unencrypted copy of the email message once they have received and successfully opened an SPX email. Although they can save the PDF itself, it must be decrypted each time it is opened.
    - Opt to have the sender receive a registration confirmation.
    - Opt to *always* have the sender receive an encryption notification.
    - Select how a message will be handled if it cannot be delivered; on failure, you can choose to bounce the message to the **Sender**, the **Administrator**, or both the **Sender and Administrator**.
  - **Quarantine** to quarantine the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.

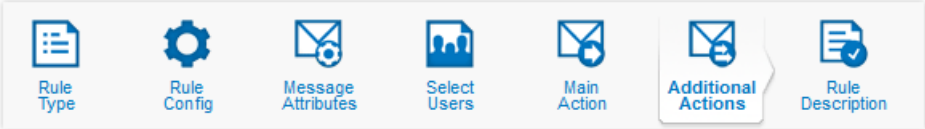
    Note: Only messages quarantined for the reason "spam" are accessible through the web quarantine and will be included in email quarantine summaries.
  - **Quarantine and continue** to quarantine a copy of the message, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
  - **Quarantine, drop file(s) and continue** to quarantine a copy of the message, drop any offending attachments, then continue processing the message. Select a reason for quarantining the message from the **Quarantine for reason** drop-down list in the **Configuration** section.
  - **Redirect** to redirect the message to a specified email address. The original recipients will not receive the message. Specify the email address to which you want to redirect the mail to in the **Redirect email address** text box in the **Configuration** section.
  - **Re-route message to another server** to send the message to another mail server. The message body, and the original sender and recipient information will be preserved, but the original recipients will not receive the message. To specify the mail server to which you want to redirect the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
  - **Send a copy of the message to another server** to send the message to the original destination, and a copy of the message to another mail server. The message body and the original sender and recipient information will be preserved. To specify the mail server to which you want to send a copy of the message, enter its hostname or IP address in the **Server** text box, and the port number in the **Port** text box in the **Configuration** section.
  - **Tag subject and continue** to tag the subject line of the message with the specified text, after which the email appliance will continue to process the message.

    Note: You can include the original subject of the message by using the %%SUBJECT%% template variable.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Additional Actions



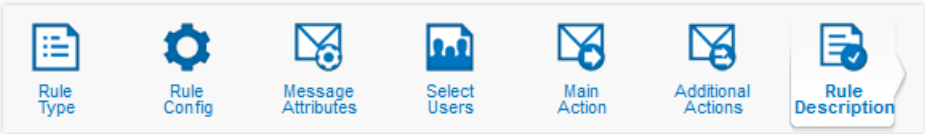
In the **Additional Actions** section, you can configure extra actions.

- To add a new action, click **Add**.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the new action, which is then displayed in the **Additional actions** table.
- To configure an existing action, click an action's description in the **Additional actions** table.
  The *Additional Message Actions* (page 196) dialog box is displayed. Use this to configure the action.
- To delete an action, select the check box next to the action description in the **Additional actions** table. Click **Delete**.
  The action will be removed from the **Additional actions** table.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward or forward in the wizard.
- Click **Cancel** to exit the **Add Policy Rule** dialog box without saving your changes.

Rule Description



To configure a rule description:

1. In the **Policy rule name** text box, enter or edit the description for the policy rule. This is the description that will appear in the rule table.
2. Select the **Activate this rule** check box.

After you have added or deleted message attributes:

- Click **Save** to save your changes, and exit the Policy Wizard.
- Click **Previous** or **Next** to move backward and forward in the wizard.
- Click **Cancel** to exit the Policy Wizard without saving your changes.

Allow/Block Lists

Use the **Configuration ➤ Policy ➤ Allow/Block Lists** page to configure lists that define trusted and known bad hosts and senders, and list of Whitelisted URLs.

- Messages from **Allowed Hosts/Senders** bypass anti-spam filtering.
- Messages from **Blocked Hosts/Senders** are blocked without being scanned for spam or content.
- URLs in **Whitelisted URLs** will not be rewritten if ToC Policy is configured to skip those URLs.

Reducing the volume of messages scanned by the Email Appliance can significantly improve system performance.

Note: Message relays known to be spam senders are included in lists used by the **IP Reputation Filtering** feature, which can be configured on the **Policy: Filtering Options** page. This page provides the ability to allow or block senders based on sender reputation data compiled by SophosLabs. It is important to ensure that a host never appears simultaneously in the **Trusted relay list** and the **Allowed Hosts** list.

- To add entries to the **Allowed hosts/senders**, **Blocked hosts/senders** or **Whitelisted URLs** list:

  1. Click on the appropriate list on the **Configuration ➤ Policy ➤ Allow/Block Lists** page. The **List Editor** dialog box is displayed.
  2. Select the **Domains** or **Senders** tab.
  3. In the **Add entries** text box, enter an IP address, domain, email address or URL, then click **Add**. Alternatively, use the **Upload** button.

     Note:

     - List entries should be in the form of an IP address, host, domain, or CIDR range, for trusted and known bad hosts, or else an email address for trusted or known bad senders. Entries such as 123.123.123.123, 123.123.0.0/10, host.example.com, @example.com, or user@example.com would all be examples of valid entries.
     - Cannot enter IP Address for Whitelisted URLs.

  4. Click **OK**.

- To delete entries from the **Allowed hosts/senders**, **Blocked hosts/senders** or **Whitelisted URLs** list:

  1. Click on the appropriate list on the **Configuration ➤ Policy ➤ Allow/Block Lists** page. The **List Editor** dialog box is displayed.
  2. Select the **Domains** or **Senders** tab.
  3. Select the check boxes beside the entries that you want to remove.
  4. Click **Delete**.
  5. Click **OK**.

Filtering Options

Use the **Configuration ➤ Policy ➤ Filtering Options** page to set advanced mail security settings and configure the Blocked and Warning page .

Sender Genotype Service

Messages from known bad senders can be blocked using SophosLabs Sender Genotype connection management technology. Choose one of three options for this setting:

- **Enable connection-level blocking of mail from known bad senders** rejects messages from known bad senders as soon as the sender information from the TCP/IP connection is received. This option is recommended because it improves performance by blocking spam before it reaches more complex tests in the policy. With this option enabled, policy blocking is also active, and messages that were last relayed from hosts in the **Trusted Relays** list may be blocked if the message was passed by a known bad sender earlier in the relay chain. Configure whether blocked messages are discarded or quarantined with the **Action for policy-level blocked messages** drop-down list.
- **Enable policy-level blocking of mail from known bad senders** blocks messages from known bad senders using a policy rule. This option is not as efficient as connection-level blocking, since the entire message must be accepted by the appliance. When messages are blocked at the policy level, the action is logged for reporting. Configure whether blocked messages are discarded or quarantined with the **Action for policy-level blocked messages** drop-down list.
- **Disable blocking of mail from known bad senders** disables reputation filtering. When blocking of bad senders is disabled, messages identified as spam are quarantined rather than discarded.

Use the **Action for policy-level blocked messages** drop-down list to select how messages blocked by policy are managed. This action is only available for the **Enable connection-level blocking of mail from known bad senders** and **Enable policy-level blocking of mail from known bad senders** options. You can choose to:

- **Discard** all blocked messages. This is the default.

- **Quarantine** for reason "spam" any messages that did not match the anti-virus policy rules. These messages will usually be reported as blocked messages; however, if the message and/or its attachments include a virus, or an unscannable, encrypted, or suspect attachment, the message is processed at the policy level, and the reason is reported.

Note: If your network has trusted local SMTP relays that pass inbound messages to the Email Appliance, use policy-level blocking instead of connection-level blocking, and add the local inbound SMTP relays to the Trusted Relays list. Connection-level blocking will only work correctly if the Email Appliance receives messages directly from the internet.

The **Enable proactive IP connection control for blocking suspicious hosts** option rejects messages originating from dynamic hosts, spambots, and suspicious hosts. Enabling this option allows the appliance to block spam from hosts that have not yet established a reputation, but which are very likely to be sending spam.

Blocked/Warning Page for Time-of-Click Protection

Using this section, you can customize the warning or blocked page displayed to the user when a Time-of-Click policy is applied. You can:

- View the current appearance of the blocked or warning page by clicking **Preview**.
- Use the default blocked or warning page provided by Sophos, by clicking **Use Default** button.
- You can upload a customized HTML file and images by clicking **Configure**. You can customize the appearance and messages displayed in the blocked or warning page.

  Note:

  - Customizing the blocked or warning page is an advanced topic. Only those with sufficient knowledge of HTML and JavaScript should attempt these tasks.
  - HTML file with .html or .htm extension only is allowed with maximum file size 10 KB.
  - Image file with .gif, .jpg, .jpeg or .png extension only is allowed with maximum file size 1 MB.
  - While customizing the Warning Page, make sure you include the **Proceed** button, clicking which user can access the desired URL.
  - Make sure you **Apply** your changes within 15 minutes of uploading your files.

Sample Templates

For guidance, Sophos provides sample templates. These templates show you how to use variables that can dynamically insert information that is relevant for individual user messages. For example, if a URL is blocked because it is malicious, you can include a variable that inserts the actual URL that was blocked.

To download the sample templates and images, click the link below, and save the .zip file:

SampleTemplates.zip

Variables

Each of the web templates provided by Sophos supports the use of variables to help customize the pages that are displayed to users. If you are uploading your own HTML files, you must use the template-specific variables in the same context that they are used in the sample templates supplied by Sophos.

The variables used in the templates are:

- <?url?>: The domain of the URL clicked by the user.
- <?date?>: Date when URL is submitted to Email Appliance.
- <?admin_email?>: Email address of the administrator as mentioned in **Configuration ➤ System ➤ Alerts & Monitoring ➤ Email** .
- <?image_path?>: Path of the image uploaded to Email Appliance.
- <?full_url?> : This variable is used in Warning Page, in the onclick event of the 'Proceed' button. It will contain the complete URL to which will get redirected on clicking the Proceed button.

Sandstorm

Sophos Sandstorm is a Cloud service that provides in-depth analysis of potentially malicious email messages.

Sandstorm provides a higher level of security by performing real-time, in-depth threat analysis of potentially malicious messages. Suspicious messages are sent for analysis. If found to be infected, messages are dropped, else delivered to the respective recipient.

For more details, see *Sophos Sandstorm*.

Sandstorm

Use this page to enable/disable communication between the appliance and Sandstorm.

You can activate a 30-day free evaluation to try it out or purchase the full Sandstorm license. Contact your Sophos Representative for more details.

Sandstorm Monitoring

This section displays all the suspicious messages that are currently held by the appliance for further analysis by SophosLabs. Messages that are found to have malicious content are processed according to the configured action in Sandstorm policies. The clean messages are delivered to their respective recipients, if no other policies are applied on them.

The administrator can manually release messages held by Sandstorm by selecting the message(s) and clicking the **Release** button. The released messages are delivered to their respective recipients without being analysed.

Note: Malicious messages may enter your network if you release messages before analysis is done.

Encryption

Manage email encryption for the Email Appliance.

Use the **Configuration ➤ Policy ➤ Encryption** page to configure the Email Appliance's encryption settings for Transport Layer Security and Secure PDF Exchange.

TLS

Transport Layer Security (TLS) enables the encrypted communication of messages between hosts that support TLS, and can also allow one host to verify the identity of another. On the Email Appliance, TLS is set to "off" by default. In this state, the Email Appliance will never attempt to encrypt email or verify the identity of a host to which it sends email.

SPX Encryption

Secure PDF Exchange (SPX) encryption is a next generation version of email encryption. It is clientless, and is extremely easy to set up and customize to any environment. More information about SPX is available in the SPX Encryption documentation.

Note: SPX Encryption requires a license. You can activate a trial version that will expire in 30 days. Contact your Sophos representative for more information.

Encryption: TLS

Use the **TLS** tab on the **Configuration ➤ Policy ➤ Encryption** page to activate and configure the Email Appliance's email encryption. You can also manage specific encryption policies for domains that the Email Appliance communicates with. The Email Appliance uses Transport Layer Security (TLS), allowing it to send and receive encrypted email with other servers that support TLS.

Note: Email encryption is set to **Off** by default.

Advanced email encryption policies

When email encryption is turned off (the default), the Email Appliance will not attempt to send encrypted email. When email encryption is turned on, the Email Appliance will attempt to encrypt email. However, if the receiving server does not support TLS encryption, the Email Appliance will instead send unencrypted email.

You can select the **Support Legacy SSL Connections** checkbox to enable CBC and RC4 ciphers, and also to enable the SSLv3 protocol instead of TLSv3 to support legacy servers like Microft Exchange 2003. As these protocols are not secure, this is not recommended unless necessary.

It is possible to configure the Email Appliance email encryption level on a per-domain basis in the **Advanced outbound encryption policy** section.

Three levels of encryption are available:

- **Prevent Encryption:** The Email Appliance will not encrypt outbound email, even if the receiving server is TLS-capable.
- **Require Encryption:** The Email Appliance will not send email unless the receiving server is TLS-capable. The Email Appliance will not require the receiving server to have a valid certificate.
- **Require Encryption and Validate Certificate:** The Email Appliance will not send email unless the receiving server is TLS-capable, and has a valid certificate.

Note: It is never possible to require other organizations' servers to encrypt email; it is only possible to require the Email Appliance to encrypt outbound email.

Activating Email Encryption

To turn email encryption on and off:

1. Click **On** to activate TLS.

   The certificate configured for encrypting outbound email will be indicated as the **Active certificate for TLS**. By default, this is the Email Appliance's self-signed certificate.

2. Click the name of the **Active certificate** to display more information about it, or to configure it.
3. Click **Off** to deactivate TLS.

   Note: Turning email encryption off will disable, but not delete, domain-specific encryption policies. Existing policies will be reactivated when email encryption is re-enabled.

Advanced Encryption Policy

You can configure domain-specific policies for email encryption. The "Incoming" and "Outgoing" options described below refer to mail that is received and sent by the Email Appliance, not mail that is received and sent by the network.

To configure a policy for a domain:

1. In the **Domain name** text box, enter the domain name to which you wish to send and\or receive encrypted email.

   Note: Email encryption must be turned on, and a valid domain name must be entered. If encryption if turned on, but nothing is configured in the **Advanced Encryption Policy** section, the appliance with attempt encryption for all incoming and outgoing domains.

2. Select **Yes** to apply the policy to any sub-domains, or **No** to apply the policy to only one specific domain.
3. Select the level of encryption:

   The following encryption levels are available:

   Note: Prevent Encryption is not an option for **Incoming** domains.

   - **Attempt Encryption:** The Email Appliance will attempt, but not require, encryption for incoming or outgoing mail.
   - **Prevent Encryption:** The Email Appliance will not encrypt incoming or outgoing email, even if the receiving server is TLS-capable.

- **Require Encryption:** The Email Appliance will not receive or send email unless the connecting server is TLS-capable. The Email Appliance will not require the connecting server to have a valid certificate.
- **Require Encryption and Validate Certificate:** The Email Appliance will not send or receive email unless the connecting server is TLS-capable, and has a valid certificate.

4. Click **Add**.

   The policy is added to the list of outbound encryption policies.

Deleting a Domain

To delete a domain from the **Advanced outbound encryption policy** list:

1. In the **Advanced outbound encryption policy** table, select the check box(es) beside the domain(s) that you want to remove.
2. Click **Delete**.

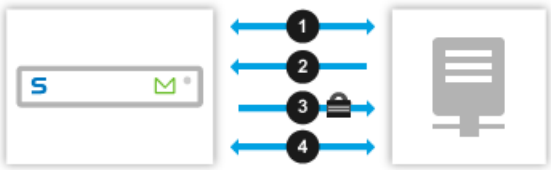
Transport Layer Security (TLS) Email Encryption

Transport Layer Security (TLS) in the Email Appliance

Transport Layer Security (TLS) enables the encrypted communication of messages between hosts that support TLS and can also allow one host to verify the identity of another. On the Email Appliance, TLS is set to **Off** by default. In this state, the Email Appliance will never attempt to encrypt email or verify the identity of a host to which it sends email.

Establishing a TLS connection

Once **Email Encryption (TLS)** is set to **On**, the Email Appliance will offer to encrypt incoming email by default. Other TLS-capable mail relays can then encrypt email sent to the Email Appliance. The appliance will also attempt to use TLS encryption for outbound email. To encrypt email, a TLS session must be established as follows:



1. A connection is established between the Email Appliance and the other mail relay.
2. The receiving host offers TLS encryption.
3. The sending host starts a TLS session.
4. The Email Appliance and the other relay attempt to exchange encryption ciphers.

Note: The host sending the mail is responsible for whether encryption is used. The receiving host can not require the sending host to encrypt email that it sends.

Encryption and Identity Verification

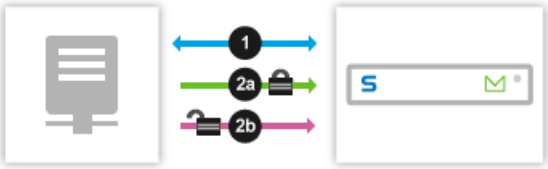
When email is encrypted, it cannot be read by anyone who does not have the appropriate key to decrypt it. However, encryption by itself does not allow you to verify the identity of the person or organization to whom you are sending the encrypted email. It is conceivable that the encrypted email could be redirected and read if the identity of the receiving mail relay has not been verified. To prevent this, the Email Appliance can be configured to use *Certificates and Certificate Authorities* (page 132) to verify the identity of the TLS-capable host receiving that is receiving email.

Setting Policies for Specific Domains

The Email Appliance can be configured to use specific policies for email that is sent to and from particular domains, including requiring the verification of the identity of a mail relay. Available policies include:

Incoming Domains

- **Attempt Encryption:** When this option is selected and TLS is set to **On**, the Email Appliance will attempt, but not require, the use of TLS encryption for all incoming email. When an email relay attempts to send mail to the Email Appliance:

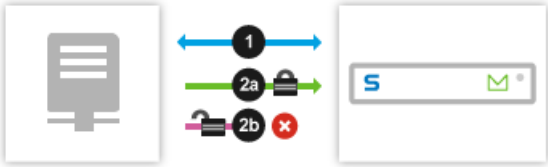


1. A TLS connection sequence and cipher exchange will be attempted (as shown above in **Establishing a TLS connection**).

2a. If the sequence is successful, email sent by the mail relay to the Email Appliance will be encrypted.

2b. If the TLS session or cipher exchange fails, the Email Appliance will still receive mail from the other mail relay, but the mail will not be encrypted.

- **Require Encryption:** Selecting this policy ensures that the mail relay will send email from the specified domain only if the Email Appliance supports TLS encryption. The mail relay will also check if the Email Appliance has a valid certificate. If the certificate check fails, the mail relay will still send encrypted email.

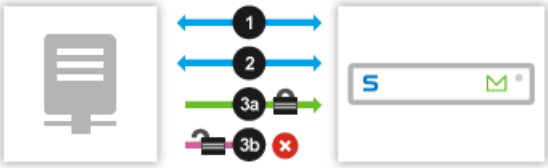


1. A TLS connection sequence and cipher exchange will be attempted (as shown above in **Establishing a TLS connection**).

2a. If the sequence is successful, email sent by the mail relay to the Email Appliance will be encrypted.

2b. If the sequence fails, the mail relay will not send mail to the Email Appliance.

- **Require Encryption and Validate Certificate:** Selecting this policy ensures that the mail relay will only send email if the Email Appliance supports TLS encryption, and also has a valid certificate that has been signed by a trusted certificate authority. This ensures that the email is encrypted and that the identity of the Email Appliance can be confirmed.



1. A TLS connection sequence and cipher exchange will be attempted (as shown above in **Establishing a TLS connection**).

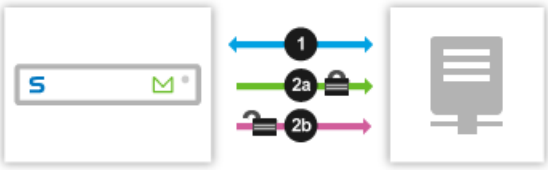
2. The mail relay will retrieve the Email Appliance mail certificate and authenticate it.

3a. If the connection sequence is successful and the identity of the mail relay can be verified, email sent by the relay to the Email Appliance will be encrypted.

3b. If the connection sequence fails, or if the identity verification fails, the mail relay will not send mail to the Email Appliance.

Outgoing Domains

- **Attempt Encryption:** When this option is selected and TLS is set to **On**, the Email Appliance will attempt, but not require, the use of TLS encryption for all outgoing email. When the Email Appliance attempts to send mail to a mail relay:

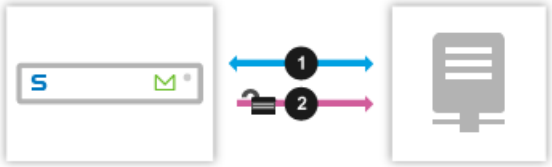


1. A TLS connection sequence and cipher exchange will be attempted (as shown above in **Establishing a TLS connection**).

2a. If the sequence is successful, email sent by the Email Appliance to the other host will be encrypted.

2b. If the TLS session or cipher exchange fails, or the other host does not support TLS, the Email Appliance will still send email to the other host, but the email will not be encrypted.

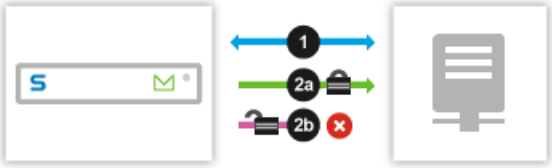
- **Prevent Encryption:** No attempt is made to encrypt email, even if encryption is supported by the receiving host. This may be useful in cases where encryption is not necessary, and attempts to use TLS encryption are having a performance impact.



1. The Email Appliance will connect to the other mail relay.

2. Email sent by the Email Appliance to the other mail relay will not be encrypted.

- **Require Encryption:** Selecting this policy ensures that the Email Appliance will send email to the specified domain only if the receiving host supports TLS encryption. The Email Appliance will also check if the host has a valid certificate. If the certificate check fails, the Email Appliance will still send encrypted email. However, it will not be possible to confirm the identity of the receiving host.

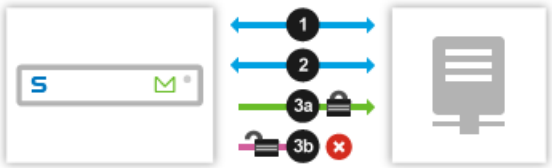


1. A TLS connection sequence and cipher exchange will be attempted (as shown above in **Establishing a TLS connection**).

2a. If the sequence is successful, email sent by the Email Appliance to the other mail relay will be encrypted.

2b. If the sequence fails, the Email Appliance will not send email to the other mail relay.

- **Require Encryption and Validate Certificate:** Selecting this policy ensures that the Email Appliance will only send email if the receiving host supports TLS encryption, and also has a valid certificate that has been signed by a trusted certificate authority. This ensures that the email has both been encrypted and that the identity of the receiving host has been confirmed.



1. A TLS connection sequence and cipher exchange will be attempted (as shown above in **Establishing a TLS connection**).

2. The Email Appliance will retrieve the mail relay's certificate and authenticate it.

3a. If the connection sequence is successful and the identity of the mail relay can be verified, email sent by the Email Appliance to the other mail relay will be encrypted.

3b. If the connection sequence fails, or if the identity verification fails, the Email Appliance will not send email to the other mail relay.

Note: After the Email Appliance has passed encrypted email to another mail relay, there is no way to guarantee it will remain encrypted or confidential, even if the identity of the other relay has been verified. You may need to communicate with the organization that manages the other relay if this is a concern.

Encryption: SPX

Secure PDF Exchange (SPX) encryption is a next-generation version of email encryption. It is clientless and is extremely easy to set up and customize to any environment. For detailed information about how SPX works, see “What is SPX Encryption?”

SPX email messages can be sent in any of the supported languages, and can be viewed by anyone with one of the *Supported PDF Readers* (page 105). Supported languages include English, French, Spanish, Portuguese, Italian, German, Dutch, Swedish, Norwegian, Finnish, Korean, Japanese, Simplified Chinese and Traditional Chinese.

Use the **SPX Encryption** tab on the **Configuration ➤ Policy ➤ Encryption** page to activate and manage the Email Appliance's SPX email encryption.

Note: SPX email encryption requires a separate license. If you do not already have an SPX license, contact your Sophos representative. SPX will operate on a trial basis for 30 days. If you do not have a license, a dialog box is displayed when you view this page, prompting you to begin the trial period. For more information, see “Viewing the Trial Status”.

What is SPX Encryption?

Secure PDF Exchange (SPX) has many advantages compared to other encryption models, including:

- Simplicity of setup: it takes less than 10 minutes to get up and running.
- A familiar process means protection of sensitive email data without changing your user's experience.
- There are no client requirements, since the PDF file format is ubiquitous and is supported on multiple platforms.
- When offline, there is no requirement to connect to the internet to view or open encrypted messages.
- Fully customizable template management provides a consistent end user experience tailored to your department/group or policy.
- Flexible password management allows passwords to be communicated out-of-band, or created by end users through a scalable registration system.
- Secure reply functionality through an HTTPS web portal allows end users to reply securely to encrypted messages.

SPX enables immediate compliance with internal or external data protection regulations and privacy guidelines. A point-and-click policy engine integrates with Microsoft Active Directory services to make policy administration simple and effective.

How SPX Works

1. Unencrypted email messages are sent to the Email Appliance, which converts each message and any attachments to a PDF document, which is then encrypted with a password. You can configure the appliance to allow recipients to select their own passwords via the SPX Secure Email Portal, or the appliance can generate passwords for recipients.
2. The encrypted message is then sent to the recipient's mail server.

3. The recipient can then decrypt the message using Adobe Reader, and the password that was used to encrypt the PDF.
4. [Optional] If secure reply is enabled, the recipient can respond securely by clicking the **Reply** button that is embedded in the encrypted PDF. If the optional **Reply All** feature is enabled, each recipient can choose to respond securely to both the original sender and to all other recipients.

Encryption Standards

Sophos uses industry-standard 128-bit AES encryption to encrypt the secure PDF messages. This is a FIPS-compliant standard adopted by the U.S. government, and used in many applications to provide a high degree of security for confidential data.

SPX On Mobile Platforms

SPX-encrypted email messages are accessible on all popular smartphone platforms that have native or third-party PDF file support, including Blackberry and Windows Mobile devices.

PCI Compliance

PCI compliance is not directly related to SPX encryption, but an increasing number of organizations are bound to these requirements as part of their overall data protection strategy.

While Sophos is unable to provide a blanket guarantee of PCI compliance of our appliance products due to constantly changing regulations, we are constantly testing our appliances and updating them as necessary to best keep up with the compliance requirements. As such, Sophos is able to confirm that our appliances are fully PCI compliant when deployed according to our best practices as of testing that took place in December 2009.

Configuring Secure PDF Exchange (SPX)

Configuring the Email Appliance to use SPX encryption involves a number of steps. Most of these are completed on the **SPX Encryption** tab of the appliance's **Encryption** page, including creating a template, setting the SPX Secure Email Portal, and configuring a password method.

Once a template has been created, you can create outbound policy rules with an action that encrypts messages if certain conditions are met. For examples, see the "SPX Deployment Guide".

- *To create a new SPX template*, click **Add**. This launches the *SPX Template Wizard* (page 79).
- *To edit an existing template*, click the name in the list of templates. This launches the *SPX Template Wizard* (page 79). Click any wizard toolbar button for direct access to that configuration page.
- *To delete one or more templates*, select the check box next to the template(s), then click **Delete**.

  Note: If a template is currently referenced by a policy, the words "in use" are displayed in brackets to right of the template name. In addition, the associated check box is unavailable (grayed out). If you want to delete a template, you must first ensure that it is not used by any policies. The Sophos Default Template cannot be edited.

- *To configure the SPX portal*, click *Configuring the SPX Portal* (page 206).
- *To set expiry and notification times for various SPX features*, click *Setting Expiry Times and Passwords* (page 205).
- *To reset the password for an email account*, enter the email address in the *Resetting an Account* (page 85) text box, and click **Reset**.
- If you are using a trial license, the number of days remaining are displayed under *Viewing the trial Status* (page 85).

Configuring Your Network For SPX

Sending SPX messages does not require any special network configuration. However, to allow SPX recipients to access the SPX Secure Email Portal, you must ensure that the portal can be reached through your firewall. When secure reply is enabled (using the SPX Template wizard), users can send encrypted responses to the encrypted messages that they receive. The SPX web portal can be configured to use either port 443, or port 10443.

It is also important to note that for the purposes of SPX secure reply, the appliance determines whether a message is inbound or outbound by comparing whether the recipient's domain appears in the list of incoming mail domains. A message to an external recipient may be considered inbound if you have configured your appliance to use an incoming mail domain that

is the same as the recipient's domain name. This in turn may affect any policy rules that are configured to use SPX encryption only for outbound messages.

Note: If you have configured the End User Web Quarantine to use one of those ports, only the remaining port will be available for the SPX portal.

Receiving SPX Messages

Recipients of SPX messages require a *Supported PDF Readers* (page 105) PDF reader.

Choosing an SPX Password Method

There are three methods of password management that you can use with SPX-encrypted email messages. These are selected on the **Password Settings** page of the SPX Template wizard.

Two or three of the password methods can be used at the same time: you just have to create different templates and policy rules to support the different models. Regardless of the password model, after the password is established, each of the password models provides a similar experience for senders and recipients.

Note: Password data is not preserved as part of system backups on an Email Appliance. Backing up confidential data of this type would pose a substantial security risk. Running two or more appliances in a clustered deployment creates data redundancy as protection against hardware failure. For more information, contact your Sophos representative.

- **User registration password management**

  The first method is user registration. When this option is selected, and a message is sent to a recipient for the first time, it triggers a policy rule that requires it to be encrypted, then:

  1. The message will be held by the Email Appliance.
  2. The appliance will send the recipient a registration email containing a link, and a request to set a password.
  3. After the recipient clicks on the link and enters the password, the original email is encrypted using the new password and relayed to the recipient, who can use the password to decrypt and read the email. All subsequent email messages to that recipient will then be encrypted using the password created during registration.

- **Sender-communicated password management**

  The second method is sender-communicated passwords. There are two variants of this method. The first variant uses a generated password, while the second variant uses a sender-specified password. With the first variant (generated password), when a message is sent to a recipient for the first time, it triggers a policy rule that requires it to be encrypted, then:

  1. The message will be encrypted using a password generated by the Email Appliance and relayed to the recipient.
  2. An email message containing the generated password will be delivered to the sender.
  3. The sender must then communicate the password to recipient in a secure fashion (for example, by telephone). The recipient uses the password to decrypt and read the email. The generated password is used to encrypt all subsequent email messages to that recipient.

  With the second variant (sender-specified password), when a message is sent to a recipient, the sender first chooses a password and adds it to the subject line enclosed in brackets, and using a specified tag. Both the tag and brackets are selected by the admin when configuring this password method. The brackets and tag trigger a policy rule that requires the email to be encrypted, then:

  1. The sender-specified password, the tag, and the brackets are removed from the subject line.
  2. The message will be encrypted using the sender-specified password and relayed to the recipient.
  3. Optionally, a copy of the email message will be delivered to the sender.
  4. The sender must communicate the chosen passwrold to the recipient in a secure fashion (for example, by telephone). The recipient uses the password to decrypt and read the email.

  Note: If a message is sent to a recipient who is not in a group that triggers the policy for sender-specified passwords, the message will not be encrypted, and the password will not be removed from the subject line before the email is delivered to the recipient.

- **Custom web service password management**

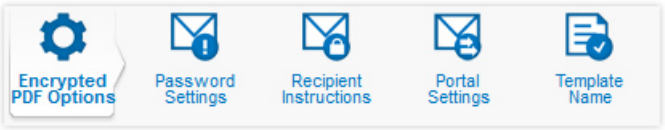
  The third method is to use a custom remote authentication service to assign passwords. This enables the appliance to retrieve passwords from your own existing authentication infrastructure. This password is then used to encrypt messages sent to the recipient. To use this method, a web service must have been created within your environment, and it must integrate with your existing authentication infrastructure. Visit the *Sophos Support Knowledgebase* for an example of how to configure the web service, or contact Sophos Professional Services for assistance.

SPX Template Wizard

Use the **Template Wizard** on the **SPX** tab of the **Configuration ➤ Policy ➤ Encryption** page to create and manage templates for SPX encryption. The Sophos Default Template cannot be edited.

To launch the SPX Template wizard, click **Add**, or click on a name in the list of existing templates.

Encrypted PDF Options



Configure various attributes of the PDF that is sent to recipients.

1. In the **Cover page** panel, select your desired cover page style. You can choose:
   - **None**: No cover page will be used.
   - **Sophos**: The default cover page supplied with the Email Appliance.
   - **Custom**: If you select this option, you must click **Upload** and select a PDF cover page that you have created. For more information on creating custom cover pages, see *SPX Best Practices* (page 104).
2. From the **Page size** drop-down list, select the page size to use for the SPX message. You can choose from **Letter**, **A4** and **Legal** sizes.

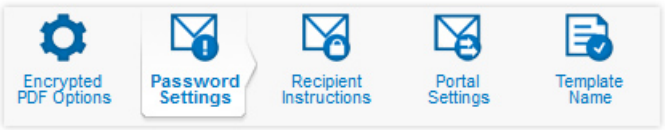
   Note: This selection affects only the pages that follow the cover page.

3. Use the **Template language** drop-down list to select the language used for labels that appear in encrypted messages (From, To, Cc, etc), and language for text displayed in the SPX portal.
4. From the **Encryption settings** drop-down list, select 128-bit or 256-bit encryption.

   Note: Only Adobe Reader 9.0 and later supports 256-bit encryption.

5. Click **Preview** to display a preview of a message that uses your selected settings, or click **Next** to configure the password settings.

Password Settings



Select the SPX password service method, and customize the messages sent for registration and password notification.

Important: Before selecting one of the following options, review the *Password Management Comparison* (page 103) section of the Password Management documentation. Each of these password services has different advantages, so it is best to choose the one that best suits your organization's needs.

1. Select the option button for the type of password service you want to use with this template.

a) Select **Allow the message recipient to choose their own password** if you want to require recipients to register using the SPX Secure Email Portal before they can receive SPX-encrypted email messages. New recipients are sent a registration link. Delivery of any SPX-encrypted mail sent to them is delayed until they have registered. Any mail sent to newly registered recipients is encrypted with the password that was used to register.

Selecting this method automatically enables the password component of the SPX portal. After adding this template, you should review the portal settings by clicking **Settings** on the **SPX** tab of the **Configuration ➤ Policy ➤ Encryption** page.

b) Select **Encrypt the message with a generated password** if you want the appliance to generate a random password. This password will be used to encrypt messages sent to the recipient. A separate, unencrypted message that contains the generated password will be delivered to the message sender. The sender must securely communicate this password to the recipient, so that recipients can decrypt the SPX-encrypted messages that are sent to them.

c) Select **Encrypt the message with a sender-specified password** if you want senders to be able to select a specific password for the recipient. This password will be used to encrypt messages sent to the recipient. A separate, unencrypted message that contains the password can optionally be delivered to the message sender. The sender must securely communicate this password to the recipient, so that recipients can decrypt the SPX-encrypted messages that are sent to them.

Note:

- If a message is sent to a recipient who is not in a group that triggers the policy for sender-specified passwords, the message will not be encrypted, and the password will not be removed from the subject line before the email is delivered to the recipient.
- Messages sent to multiple recipients will be encrypted using the same sender-specified password. The sender must communicate the password to each of the recipients.
- Password recovery options are not available for sender-specified passwords.

d) Select **Use a custom remote authentication service to assign passwords** if you want the appliance to retrieve passwords from your own existing authentication infrastructure. This password will be used to encrypt messages sent to the recipient. To use this method, a web service must have been created within your environment, and it must integrate with your existing authentication infrastructure. Visit the *Sophos Support Knowledgebase* for an example of how to configure the web service, or contact Sophos Professional Services for assistance.

Note: If you select this password method, the **End user password options** section of the **Password Settings** page is unavailable (grayed out).

2. [Sender-specified passwords only] The sender must specify a password in the subject line of the email that they want to encrypt. The password must:

- Be enclosed in the same brackets that you have configured below.
- Follow the tag you have specified, separated by a colon (":").
- Appear at the beginning of the subject line.

Note: Passwords can only contain letters, numbers and the following characters: **!@#$%+=,.**. Messages with invalid passwords will not be sent, and will be returned to the sender, the administrator, or both, depending on your configuration.

In the **Password settings** section:

a) Select the bracket type you want to use from the **Bracket type** drop-down list.

b) In the **Prefix** text box, enter the prefix that senders should use.

Note: The prefix can be a maximum of fifteen characters long.

c) [Optional] Select the **Notify password sender by email** option to send an notification email to the password sender.

3. Click the **Configure** button to *Edit notification email* (page 198) of the notification email.

4. [Optional] If you want a separate password to be issued each time a message is sent, select **Always generate a new password**.
5. In the **End user password options** section, configure the features that you want to make available to message recipients.

   It is best to decide which of these password options you want to make available to end users during the initial configuration and deployment of SPX encryption. Although you can edit the settings later, this could pose problems for senders and recipients.

   If you decide, for example, to enable password reset or recovery after SPX has been deployed, those who were previously issued passwords will not automatically have access to reset or recovery. The same is true for SPX recipients whose passwords were issued before end user password features were added to the Email Appliance. For more information, see “Using SPX Passwords” in the SPX End User Experience section.

   Select one or more of the following:

   - **Password change**: Allows users to replace their existing passwords with new passwords. Users are prompted to enter the current password before submitting a new password.
   - **Password reset**: Allows users to create a new password if the previous password has been forgotten. Users are prompted to enter answers for the configured number of questions (see description in "questions" option below) before a new password is issued. Passwords can also be reset by the administrator using the **Account reset** option on the **SPX Encryption** tab.
   - **Password recovery**: Allows users to retrieve a forgotten password. Users are prompted to enter answers for the configured number of questions (see description in "questions" option below) before the password is recovered.
   - **Require (n) password challenge question(s) for reset/recovery**: This option is unavailable (grayed out) unless you select “Password reset” and/or “Password recovery.” When you do so, recipients are prompted to establish at least one challenge question that must be answered to reset or recover a password. Recipients should be encouraged to select questions with answers that others are unlikely to guess. You can choose to have users answer 1-3 questions. The default is 3.

   Selecting any of the options above automatically inserts text on the next page of the wizard (**Recipient Instructions**) that contains an associated template variable. Each variable creates a URL that recipients can click to access the appropriate password page on the SPX Secure Email Portal.

   If you attempt to apply any of these options to an existing or customized template, the text will remain unchanged.

   You can customize the recipient instructions text as necessary, but for each option selected here, ensure that the associated template variable is preserved on the **Recipient Instructions** page. If the selected features do not match the included template variables, a warning message is displayed. A match is required to create an active link to the appropriate SPX portal page.

   Important: Recipients should understand that a new password only applies to encrypted messages received after the password has been reset or changed. Recipients must use the password that was active during the period that encrypted messages were sent in order to access those messages.

6. Optionally, configure a **Fallback template**.

   You can configure a different SPX Template to be used as a fallback template. If SPX encryption fails, it will use the **Fallback template** if one is selected here.

7. Click **Previous** to configure PDF email attributes or **Next** to configure the recipient instructions.

Edit notification email

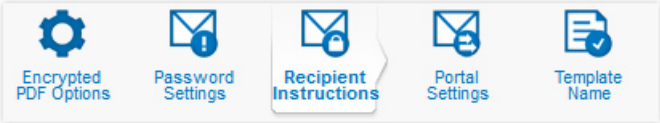
Customize the **Subject** and **Body** of the message that accompanies the password service method that you have chosen.

A number of template variables are available to customize messages. The template variables available depend on which password service you have selected. Template variables specific to the *SPX registration message* (page 191) are available if you have opted to let recipients choose their own passwords, and variables specific to *messages with SPX generated or sender-specified passwords* (page 191) are available if you have opted to either generate passwords or allow sender-specified passwords and have the sender communicate passwords to recipients.

Note: Certain template variables must be present in the subject or text of different kinds of notification emails, or you will not be able to save it:

Password service	Required template variable(s)
Allow the message recipient to choose their own password	%%REGISTRATION_URL%%
Encrypt the message with a generated password	%%ENVELOPE_TO%%, %%GENERATED_PASSWORD%%
Encrypt the message with a sender-specified password	%%ENVELOPE_TO%%, %%SPECIFIED_PASSWORD%%

Recipient Instructions



Use the **Recipient instructions** page to customize the email that is sent with each SPX email message.

You can customize the text of the email, and also specify the header and footer images that are displayed in the recipient instructions that accompany all encrypted messages.

Customize the recipient instructions, and configure the images displayed in the instructional message:

1. Click the **Configure** button to *Edit SPX Recipient Instructions* (page 199) of the recipient instructions.
2. Use the **Header image** option buttons to select whether the recipient instructions that accompany encrypted messages contain a header that uses the Sophos image, no image, or a custom image. If you select the **Custom** option, you must click **Upload**, and select an image.
3. Use the **Footer image** option buttons to select whether the recipient instructions that accompany encrypted messages contain a header that uses the Sophos image, no image, or a custom image. If you select the **Custom** option, you must click **Upload**, and select an image.

   Note: Header and footer images must be JPG, GIF or PNG format. The portal is optimized to use images that are 752 pixels wide by 69 pixels high. Other image sizes may be used, though results may vary.

4. Click **Previous** to configure the password settings or **Next** to configure SPX Secure Email Portal settings.

Edit SPX Recipient Instructions

Use the **SPX recipient instructions** page to customize the text of the email that is sent with each SPX email message. This provides recipients with information about the SPX message that they have received, such as the required Adobe Reader software, and, if necessary, how to obtain the password needed to read the message.

Note: When using sender-specified passwords, the instructional email will have the same subject as the sender-specified password email, except that the associated tag, password, and brackets will be removed.

Add or edit email body:

1. In the **SPX recipient instructions** dialog, edit the text as necessary.

   Note: You can use basic HTML to help format the registration email. If the recipient's email client is configured to accept HTML messages, the formatted version is displayed; otherwise, their email client shows a text version of the registration email, with no special formatting. The registration email has a size limit of 4KB.

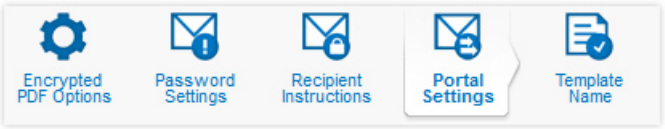
   You can customize messages with any of the template variables *available for the SPX instructional text* (page 190).

   Selecting any of the **End user password options** on the previous wizard page automatically inserts text on this page that contains an associated template variable. Included in the text is a URL that recipients can click to access the appropriate password page on the SPX Secure Email Portal.

Customize the recipient instructions text as necessary, but for each end user password option check box selected on the previous page (**Password Settings**), ensure that the associated template variable is preserved. If the included template variables do not match the selected check boxes, a warning message is displayed. A match is required to create an active link to the appropriate SPX portal page.

2. In the **Text** text box, edit or update the instructions that will be sent to recipients of SPX messages. This should contain useful information, such as how to open SPX messages, how to obtain their password and so forth.

Portal Settings



To activate secure email reply, and configure the images displayed in the portal:

1. Click **On** to activate the secure email reply feature.

   If you want recipients of encrypted messages to be able to send encrypted responses, this option must be turned on. When enabled, a **Reply** button is included in all encrypted PDFs. Optionally, messages with multiple recipients may also include a **Reply All** button. To respond from within the PDF itself, recipients can click the **Reply** button or, when available, the **Reply All** button.

   Note: After you finish adding this template, you should review the portal settings by clicking **Settings** on the **SPX** tab of the **Configuration ➤ Policy ➤ Encryption** page.

2. [Optional] Select **Require users to log in to send a secure message** so that mail recipients must log in using their SPX password to respond to an encrypted message. This provides an additional level of security in cases where recipients are accessing encrypted messages in less secure locations, such as public email kiosks.
3. [Optional] Select **Include text of original message in reply** if you want the original message to be displayed as part of secure responses.

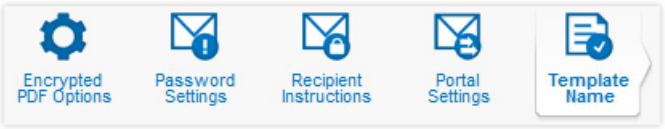
   Note: If the original message text is too long, it may be truncated.

4. [Optional] Select **Include Reply All button in encrypted messages** to allow recipients to reply to all message recipients as well as the sender. The **Reply All** button is only displayed when a message has more than one recipient.
5. Use the **Header image** option buttons to select whether the SPX portal header uses the Sophos image, no image, or a custom image. If you select the **Custom** option, you must click **Upload** , and select an image.
6. Use the **Footer image** option buttons to select whether the SPX portal footer uses the Sophos image, no image, or a custom image. If you select the **Custom** option, you must click **Upload** , and select an image.

   Note: Header and footer images must be JPG, GIF or PNG format. The portal is optimized to use images that are 752 pixels wide by 69 pixels high. Other image sizes may be used, though results may vary.

7. Click **Previous** to configure the recipient instructions or **Next** to edit the template name.

Template Name



On this page of the wizard, you will provide a descriptive name to be displayed in the list of SPX templates on the **SPX Encryption** tab. In addition, provide the organization name that you want to be displayed in text containing the %%ORGANIZATION_NAME%% template variable. Provide the “from” email address that you want displayed to recipients in all SPX messages that are auto-generated by the Sophos Email Appliance.

Add or edit the template name, organization name, and system email address:

1. In the **Template name** text box, add or edit a name for this template. This is the name that will be displayed in the list of SPX templates.
2. In the **Organization name** text box, enter the name that you want displayed to email recipients in SPX communications. The name entered here will be inserted in the message if the %%ORGANIZATION_NAME%% template variable is included in the body text used for registration request and recipient instructions messages.
3. In the **System email address** text box, enter the address that you want displayed as the “from” address in all automated system communications that the appliance delivers to recipients. For example, you may want to provide your organization's help desk as the return address for all system-delivered messages related to SPX. If you prefer not to provide a “from” address, you can indicate that instead (for instance, no-reply@example.com).
4. [Optional] Select the **Sophos SPX Logo** check box if you do *not* want the "Powered by Sophos SPX" logo displayed in SPX messages and on the SPX portal.
5. Click **Save** to save this template, **Previous** to configure to reply settings, or **Cancel** to discard any changes.

Configuring the SPX Portal

Clicking **Settings** in the **Portal** section of the **Policy: Encryption** page opens the **Configure SPX Portal** dialog box. Here, you configure the URL used for the Secure PDF Exchange (SPX) email portal. By default, port 10443 is used for the (SPX) portal, and port 443 is used for the End User Web Quarantine.

Note: By activating the SPX portal you give recipients a means of registering for an SPX password. If you want recipients to have the option of securely responding to encrypted messages, you must enable secure reply using the SPX Template wizard. For more information, see “Portal Settings”.

To configure the portal URL:

1. Select either the **Use hostname from SSL certificate (Recommended)** if you want to use the hostname from the Email Appliance's SSL certificate, or select the **Specify a custom hostname** option and enter the hostname of the Email Appliance on which the SPX portal is located.
2. Under **Ports**, select the port used for the **SPX portal**.
   Whichever port you select for the SPX Portal, the remaining port will automatically be selected for the End User Web Quarantine (the reverse is also true).
3. Click **OK**.

Note: You may need to add or configure a certificate for use with the SPX portal. See the *Certificates* (page 129) documentation for more information.

Setting Expiry Times and Passwords

Clicking **Configure** in the **Expiry and user password settings** section of the **Policy: Encryption** page opens the **SPX Expiry and Password Limits** dialog box. Here you can configure the periods for SPX option expiry, and notification times. All values must be entered as days. You can also specify the minimum number of characters required for passwords.

1. Set one or more of the following:
   - In the **Keep unused passwords** text box, enter the maximum number of days between password uses that passwords will remain valid.
   - In the **Allow secure reply** text box, enter the maximum number of days that the link sent for the secure reply portal remains valid for recipients of SPX email messages.
   - In the **Keep delayed emails** text box, enter the number of days that an appliance will hold email while waiting for an SPX recipient to set a password.
   - In the **Registration reminder** text box, enter the number of days before an SPX recipient will receive an email reminder to set a password.

     Note: The **Registration reminder** period should be shorter than the **Keep delayed emails** period.

- In the **Password strength** text box, enter the minimum number of characters an SPX user must type in order to create a valid password. The default is passwords that are at least 8 alphanumeric characters in length. The maximum length is 32.
- Select **Require special characters** to enforce inclusion of at least one special character in each password. Valid special characters are shown to recipients when they are setting a password.

2. Click **OK**.

Resetting an Account

Use the **Account reset** feature to assign a new password to a specific SPX recipient. Enter the email address of the recipient whose password you want to reset, and click **Reset**.

You should provide contact information on SPX cover pages, or in the messages that are sent to recipients that detail who, in your organization, they should contact in the event that they require a new password. Depending on your organization, this could include:

- Your organization's helpdesk
- The original sender of the SPX message
- An email address at your organization that directs the requests to the appropriate contact in your organization

After you reset a password, the recipient receives a new registration request.

You can also grant SPX recipients the ability to reset their own passwords. For more information, see “Password Settings” in the SPX Template Wizard documentation.

Viewing the trial Status

The Secure PDF Exchange (SPX) evaluation gives you the opportunity to test and evaluate this email encryption technology for 30 days. SPX allows you to send selected outbound email as encrypted PDFs, without the need to exchange complex and cumbersome encryption keys.

Recipients are sent a message in the form of a strongly-encrypted PDF that can also include attachments. Reading encrypted email messages is a matter of simply opening the message using Adobe Reader, and entering a password. Several easy methods of exchanging passwords are provided.

After the 30-day trial has expired, you can arrange a longer evaluation period or purchase a full license by contacting your Sophos representative.

SPX Deployment Guide

A guide to setup requirements, with two example configuration scenarios.

Secure PDF Exchange (SPX) lets you grant your end users the ability to send secure, encrypted email messages through the appliance. As demonstrated in the examples that follow, SPX deployment involves a number of stages, including creating an SPX template, configuring an associated policy rule, and testing the configuration.

Important: Policy rules may be configured to use SPX encryption only for outbound messages. For SPX Secure Reply, the appliance determines whether a message is inbound or outbound by comparing whether the recipient's domain appears in your list of incoming mail domains. A message to an external recipient may be considered inbound if you have configured your appliance to use an incoming mail domain that is the same as the recipient's domain name.

Each of these examples offers a step-by-step guide to everything required to set up and use SPX encryption.

Example Deployment: User Registration

An example of SPX deployment that uses the SPX Secure Email Portal for password self-registration.

This example uses many of the default template settings. If you need to customize any of these to suit your needs, see the SPX Encryption documentation for detailed descriptions of each option.

Deploying SPX to allow user-registered passwords requires the following steps:

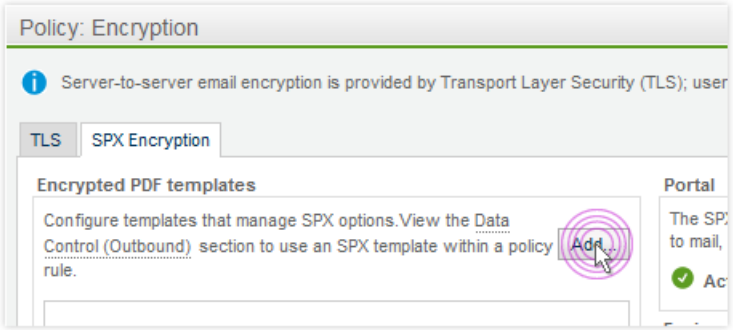
1. Creating a template
2. Configuring the portal that recipients use to register their passwords
3. Configuring expiry times and password strength

4. Configuring a policy rule
5. Testing your configuration

Configuring SPX: Passwords Set by User-Registration

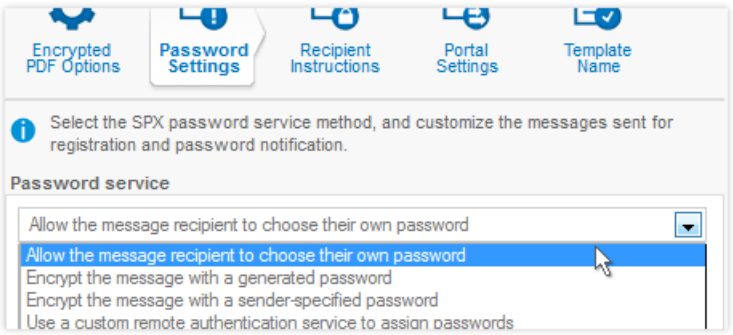
1. **Creating a template**
   a) First, create a template. This includes customizing the appearance of encrypted messages, setting up the SPX portal, defining the content for messages, and specifying the method used to set passwords.

   On the **Configuration ➤ Policy ➤ Encryption** page, select the **SPX Encryption** tab, and click **Add**.



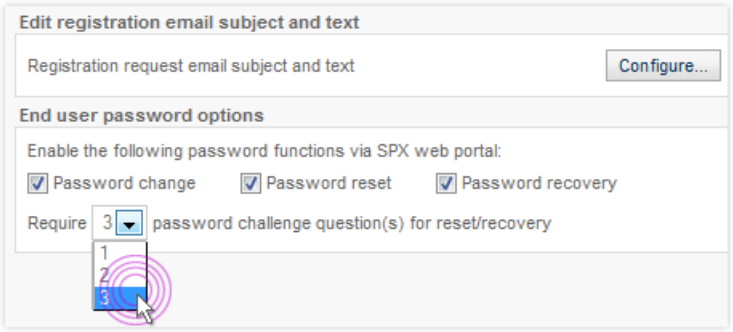
   The template wizard launches.
   b) On the **Encrypted PDF Options** page of the wizard, you can set the properties of encrypted messages, including the cover page and the page size for the page(s) containing the body of the message.

   In this example, you will upload a Sophos cover page, and accept the default settings for **Page size** and **Template language**.
   c) Click **Preview**. A sample PDF loads, allowing you to view the SPX cover page and the email layout.
   d) Click **Next**.
   e) On the **Password Settings** page of the wizard, select **Allow the message recipient to choose their own password**.



   First, accept the default **Subject** line for encrypted messages. Although you can customize both the body and the subject of the email message that notifies SPX recipients of encrypted email messages, make sure that the text does not suggest contacting the sender for password information. If user registration is selected, senders do not manage recipient passwords. Click **Next** to proceed to the **Recipient Instructions** page.
   f) You can edit the text as necessary to convey decryption instructions. For the sake of this example, however, accept the default text.
   g) Under **End user password options**, select **Password change**, **Password reset**, and **Password recovery**.This will create links in the recipient instructions (next wizard page) that allow recipients to access password management

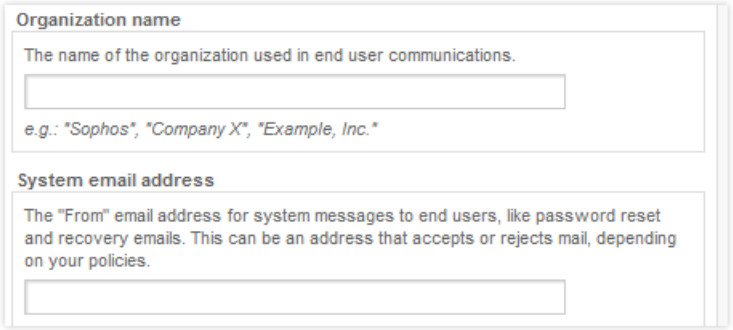
pages on the SPX portal. Accept the default number of password challenge questions (3). Recipients will be prompted to set a series of questions that they must answer if they need to reset or recover their password. Click **Next**.



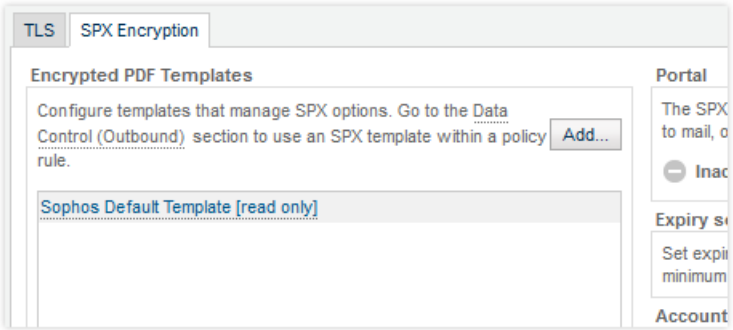
h) On the **Portal Settings** page, configure the settings for the SPX portal. Make sure that **Enable Secure Reply** is set to **On**, then select the **Sophos** option for both the header and footer images.

Note: See the references at the end of this example for information about creating PDF cover pages, and custom header and footer images.

i) On the **Template Name** page, enter a descriptive name for the template you have just created. This is the name that is displayed in the list of templates. In the **Organization name** text box, enter the name that you want to be displayed in instructions to recipients. The text specified here is used by the %%ORGANIZATION_NAME%% template variable. In the **System email address** text box, enter the address that you want to appear in auto-generated communications sent by the appliance. Click **Save**.

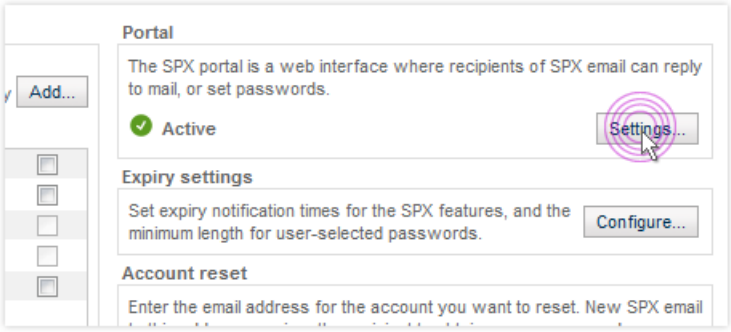


View the **SPX Encryption** tab. You will see the new template that has been created. If you want to change anything, you can click the name of the template to edit it. Note that the SPX portal is now active, indicated by the green icon.



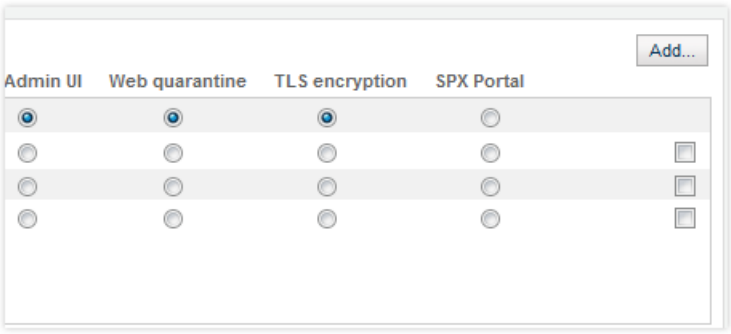
2. Configuring the SPX Secure Email Portal

a) On the **SPX Encryption** tab, click the **Settings** button.



The **Configure SPX Portal** dialog box is displayed. The dialog box shows that the Email Appliance is using its default, self-signed certificate. Sophos recommends never using the default, self-signed certificate for services exposed to the internet. Instead, obtain a valid certificate. This ensures that the appliance references the desired hostname instead of the internal hostname that it uses by default.

b) To obtain a certificate for the appliance, close the **Configure SPX Portal** dialog box. Then, on the **Configuration ➤ System ➤ Certificates** page, click **Add**.

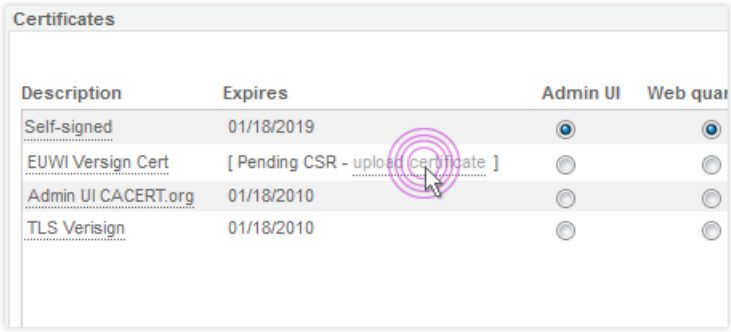


This opens the **Add certificate** dialog box, where you select **Initiate Certificate Signing Request**. Click **Next**.

c) In the **Initiate CSR** dialog box, enter the information required to obtain a certificate. In this example, enter a **Description**, and use `msgportal.example.com` for the **Hostname/Domain**. Click **Next**. A certificate signing request (CSR) will be generated that you can send to the certificate authority (CA) of our choice in order to purchase a valid certificate.

d) In the **CSR text** box, click **Download**. Use your web browser to save the text as a `.pem` file. Click **Close**.

e) In the list of certificates shown on the **Configuration ➤ System ➤ Certificates** page, the new certificate request is shown as a *Pending CSR*. Next to its description will be an **upload certificate** link. After you've obtained your new certificate from the authority, click this link to upload it.



The **Upload Certificate** dialog box is displayed, and you can either paste or upload your new certificate. This completes the certificate creation process.

Note: Although this example shows how to use the appliance's built-in capabilities to obtain a new certificate, you can also use an existing certificate for your appliance.

f) Configure your SPX portal to use the new certificate. On the **Configuration ➤ Policy ➤ Encryption** page, select the **SPX Encryption** tab. Under **Portal**, click **Settings**. In the **Configure SPX Portal** dialog box, select the **Use hostname from SSL certificate** option, and port **10443**. Click **OK**.

Important: You should ensure that your firewall allows access to port 10443.

3. **Configuring expiry settings and password strength**

a) Under **Expiry and user password settings**, click **Configure**. Confirm that the expiry settings are correct, accept the default password length, and click **OK**.

4. **Configuring a policy rule**

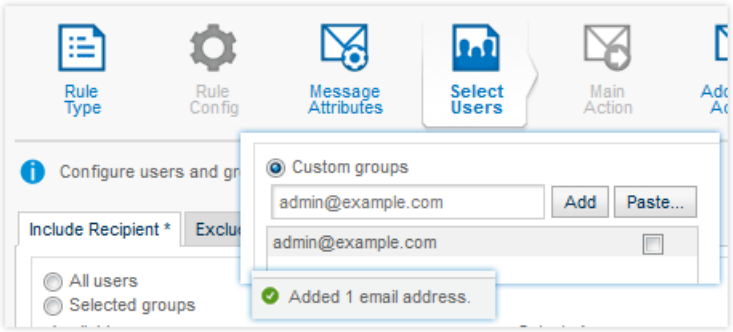
a) Create a policy rule that uses the SPX template and the portal settings. You can configure multiple rules associated with SPX encryption, but an extremely useful rule is one that allows internal users to specify that a message be encrypted by setting a "confidential" option in the sender's mail client (for example, Microsoft Outlook). To do this, on the **Configuration ➤ Policy ➤ Additional Policy** page, select the **Outbound** tab, then click **Add**. This opens the Policy wizard. Select the **Use only message attributes** option, then click **Next**.

Important: For SPX secure reply, the appliance determines whether a message is inbound or outbound by comparing whether the recipient's domain appears in your list of incoming mail domains. A message to an external recipient may be considered inbound if you have an incoming mail domain that is the same as their domain name. In this case, the policy rule will not trigger, and emails to a recipient in this domain will not be encrypted.

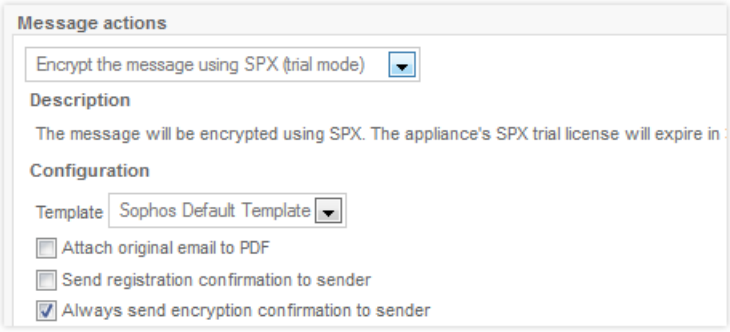
b) In the **Identify message attributes** section, click **Add**. This opens the **Add Message Attribute** dialog box. Since setting the "Confidential" option in Outlook creates a mail header called "Sensitivity", with a value of "company-confidential", the rule must use these keywords too. Select the **Header** option from the drop-down list. Then, in the **Name** text box, add a header `Sensitivity`, and select **is (exact match)**.

c) In the **Value** text box, enter `company-confidential`. Click **Apply**. In the list of message attributes, you will now see a single new attribute that is based on your selections. After you confirm this, click **Next** to set user and group options.

d) Before applying this new rule to active users, you should ensure that it works. To do this, on the **Select Users** page of the wizard, add a custom group. This should consist of a single internal email address from which you can send test messages. Make sure it is included in this policy rule (ensure that the address is specified on the on the **Include Sender** tab), then click **Next**.



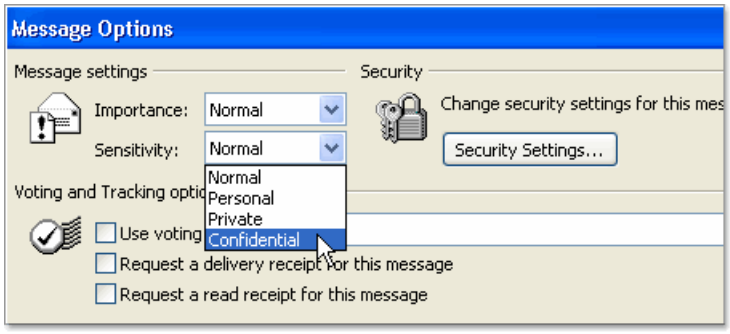
e) On the **Main Action** page of the wizard, select the message action **Encrypt the message using SPX**. From the **Template** drop-down list, select the template you created. Select the **Attach original email to PDF** check box. Select the **On failure, bounce to Sender** option, then click **Next**.



f) Now that you have finished configuring this rule, give it a descriptive name. Finally, be sure to select **Activate this rule**, and click **Save**.
You are now ready to test your SPX encryption setup.

5. **Testing your setup**

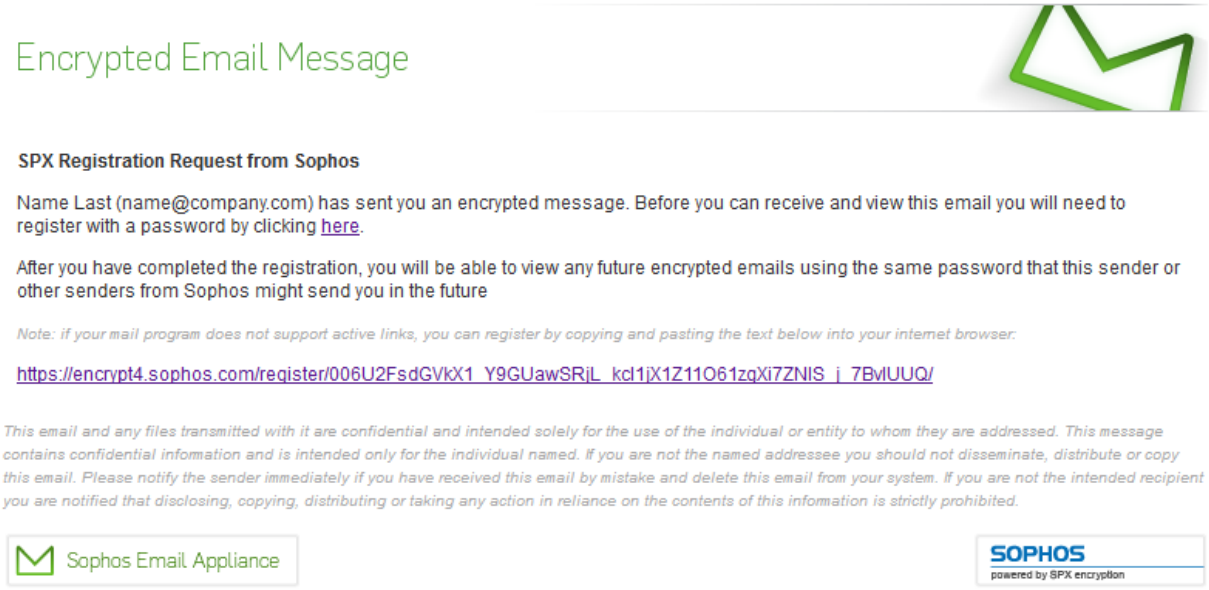
a) Compose a message. To test properly, send this message to an external email address that you can access. Since this example uses Microsoft Outlook, you must change the email client's settings to match those in the appliance. In Microsoft Outlook, click **New** to create a message. On the **Message** tab, click the dialog box launcher in the bottom right section of **Options** to open the **Message Options** dialog box. From the **Sensitivity** drop-down list, select **Confidential**. (If the email client is equipped with the Sophos Outlook Add-in, and configured to use Outlook's **Confidential** sensititvity, you can simply click the **Encrypt** button on the Outlook toolbar. For more information, see “Sophos Outlook Add-in” in the Appendix.)



After you have finished, send the message.

Note: If you are using a mail client other than Microsoft Outlook, see its product documentation for instructions on creating a mail header like the “Sensitivity: company-confidential” one used in this example.

b) Next, check for a new message at your test email address. You should receive a message that looks something like this:

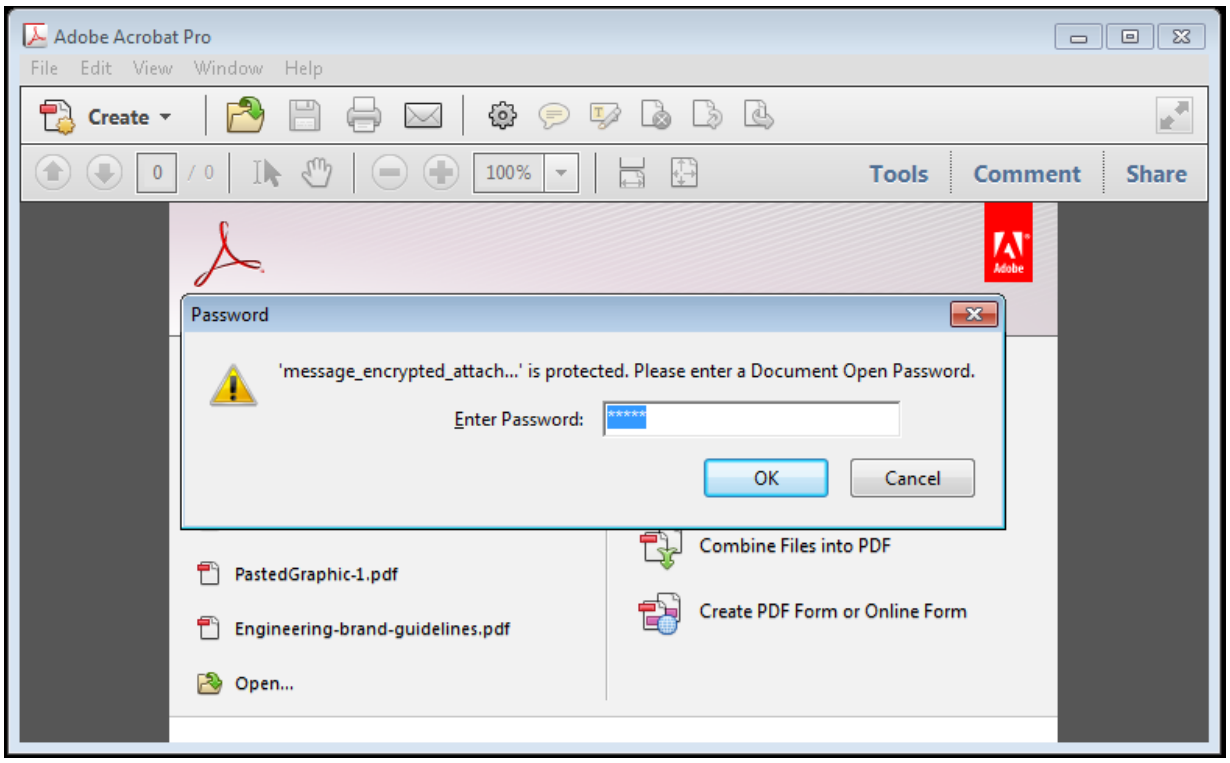


In this example, users need to set their own passwords through the SPX portal. The encrypted email will be held by the Email Appliance until recipients register a password.

Note: With both user-registration passwords and sender-communicated passwords, once the password is set, the email user can access any subsequent email messages from that sender, and messages are sent to the recipient(s) immediately.

c) After the password has been set, you will receive the original (but encrypted) message at your test account.

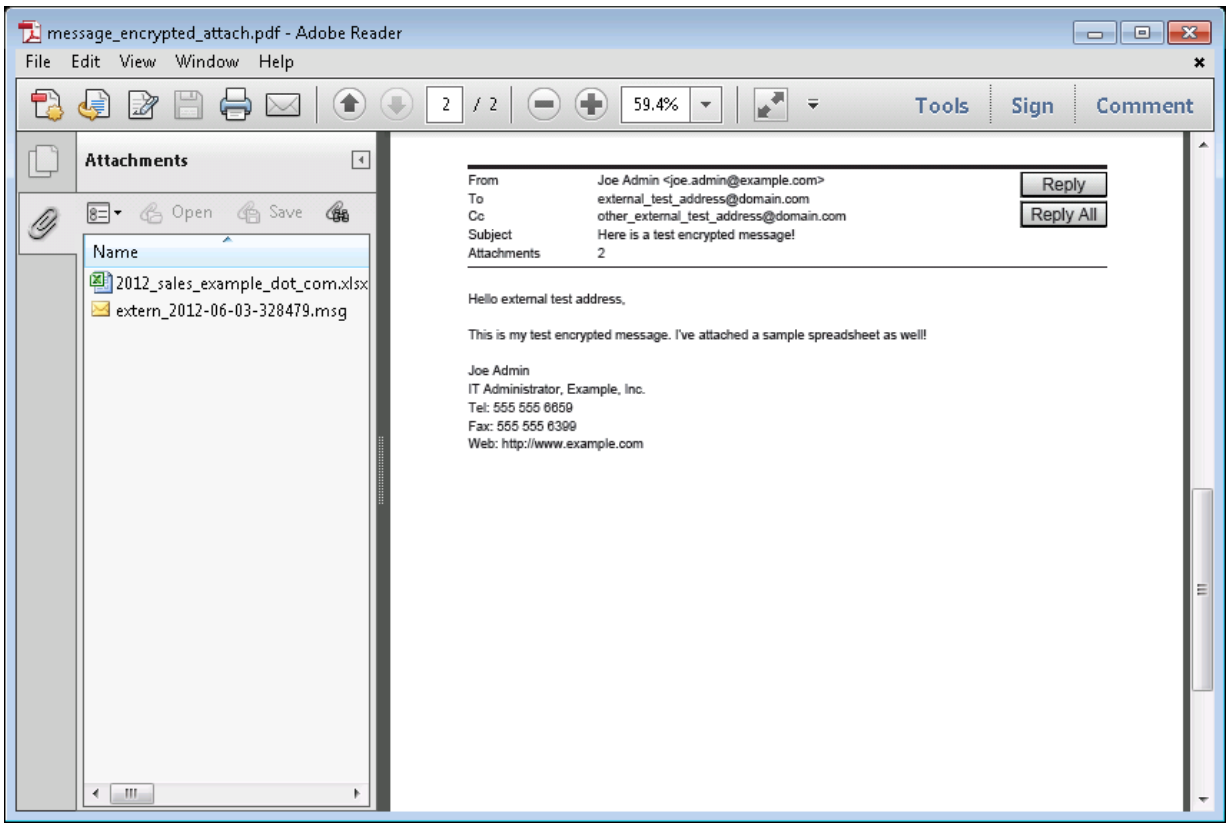
Double-clicking the attached PDF opens it in Adobe Reader, where you are prompted to enter the password:



d) After you enter the password, the PDF is decrypted, and the cover page is displayed. You can scroll past the cover page and read the original message, and download any attachments.

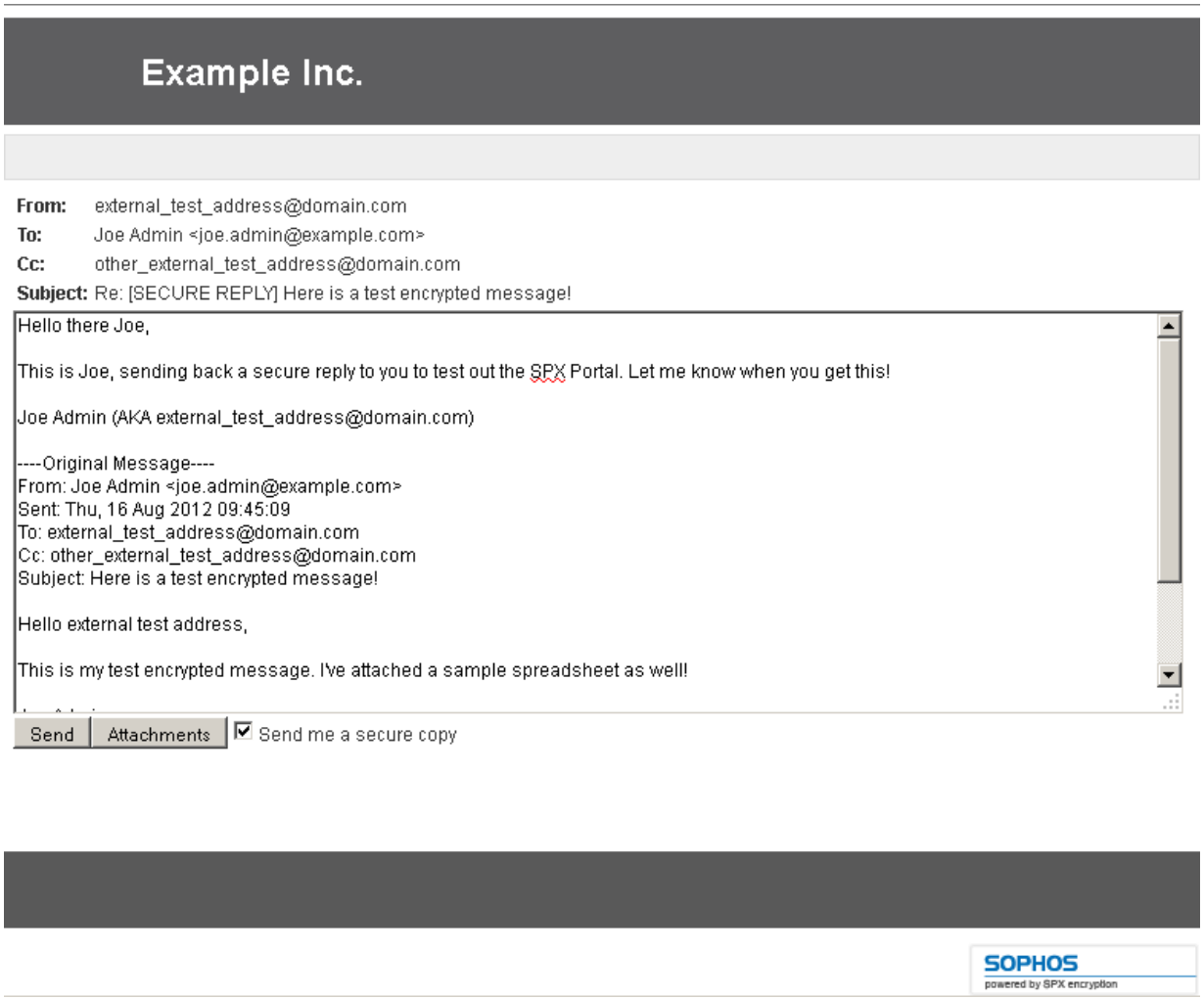
A **Reply** button is displayed in the message. This lets the recipient send a secure, encrypted reply to the sender using the SPX portal. Clicking the **Reply** button opens the recipient's default web browser and launches the secure reply portal.

If the optional **Reply All** feature is configured and a message has been sent to multiple addresses, each recipient has the option to send a secure, encrypted reply to both the sender and to all of the original recipients using the SPX portal. Clicking the **Reply All** button opens a recipient's default web browser and launches the secure reply portal.



Note: Recipients can also choose to reply directly from their email client. This form of reply is not encrypted, but may be suitable in instances where a secure reply is not essential.

e) In the secure reply portal, you should compose and send a response to the original email message.



After you have sent it, confirm that you received a response at your internal address. You have now confirmed that all aspects of your SPX deployment work correctly. The setup is ready for active users.

Example Deployment: Sender-Communicated Password

An example of SPX deployment in which individual senders communicate passwords to the recipients of SPX email messages.

This example uses many of the default template settings. If you need to customize any of these to suit your needs, see the SPX Encryption documentation for detailed descriptions of each option.

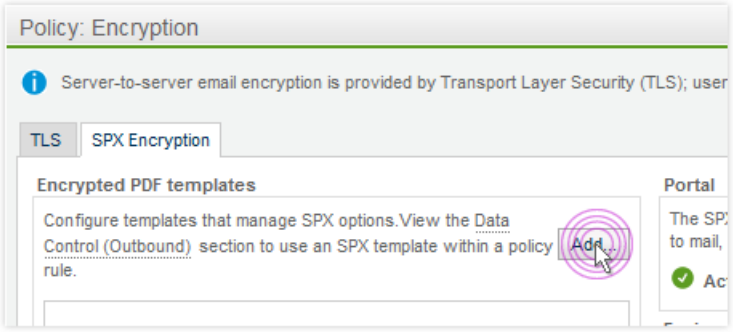
Deploying SPX to allow your senders to communicate passwords to recipients requires the following steps:

1. Creating a template
2. Configuring the portal that recipients use to register their passwords
3. Configuring expiry times and password strength
4. Configuring a policy rule
5. Testing your configuration

Configuring SPX: Passwords Communicated by the Sender

1. **Creating a template**
   a) First, create a template. This includes customizing the appearance of encrypted messages, setting up the SPX Secure Email Portal, defining the content for messages, and specifying the method used to set passwords.

   On the **Configuration ➤ Policy ➤ Encryption** page, select the **SPX Encryption** tab, and click **Add**.



The template wizard launches.

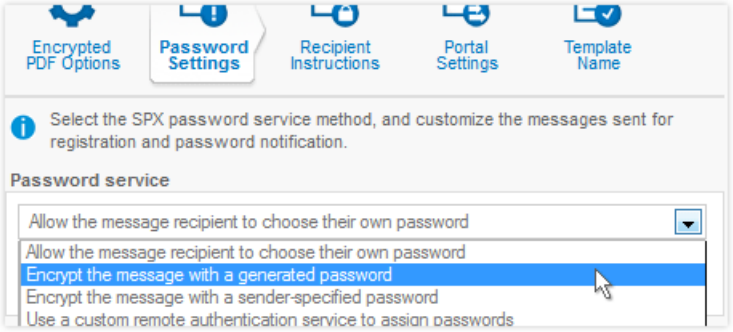
b) On the **Encrypted PDF Options** page of the wizard, you can set the properties of encrypted messages, including the cover page and the page size for the page(s) containing the body of the message.

In this example, you will upload a Sophos cover page, and accept the default settings for **Page size** and **Template language**.

c) Click **Preview**. A sample PDF loads, allowing you to view the SPX cover page and the email layout.

d) Click **Next**.

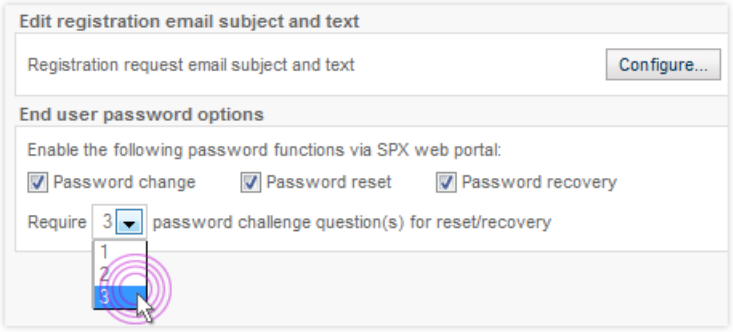
e) On the **Password Settings** page of the wizard, select **Encrypt the message with a generated password**.



Leave the **Always generate a new password for each message** check box unselected. Accept the default **Subject** line for encrypted messages. Although you can customize both the body and subject of the email message that notifies SPX recipients of encrypted email messages, make sure that the text does not suggest contacting the sender for password information. If user registration is selected, senders do not manage recipient passwords. Click **Next** to proceed to the **Recipient Instructions** page.

f) You can edit the text as necessary to convey decryption instructions. For the sake of this example, however, accept the default text.

g) Under **End user password options**, select **Password change**, **Password reset**, and **Password recovery**.This will create links in the recipient instructions (next wizard page) that allow recipients to access password management pages on the SPX portal. Accept the default number of password challenge questions (3). Recipients will be prompted to set a series of questions that they must answer if they need to reset or recover their password. Click **Next**.

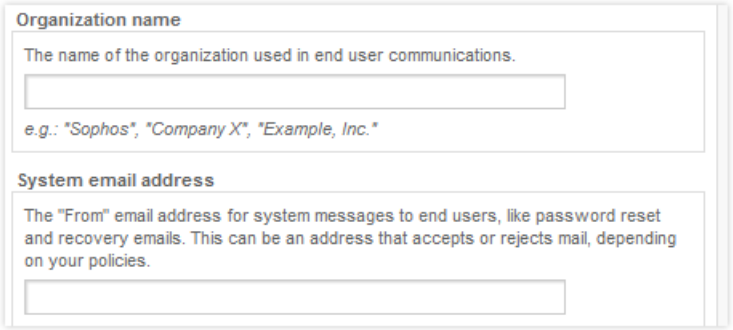


h) On the **Recipient Instructions** page is default text that provides directions for the recipients of encrypted messages. Notice that the some of the text is tagged with HTML. You can format the text as desired using basic HTML tags. Although you can edit this page, accept the default text, and click **Next**.

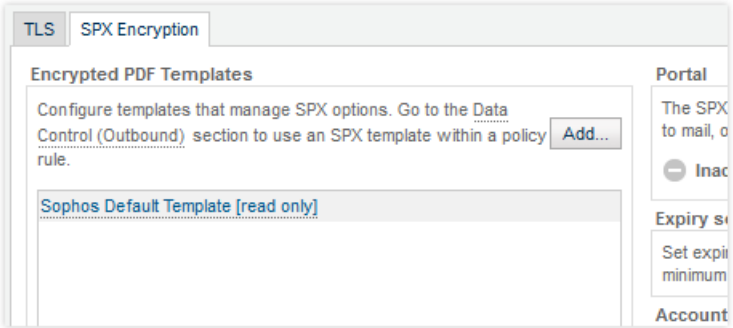
i) On the **Portal Settings** page, configure the settings for the SPX portal. Make sure that **Enable Secure Reply** is set to **On**, then select the **Sophos** option for both the header and footer images. Click **Next**.

Note: See the references at the end of this example for information about creating PDF cover pages, and custom header and footer images.

j) On the **Template Name** page, enter a descriptive name for the template you have just created. This is the name that is displayed in the list of templates. In the **Organization name** text box, enter the name that you want to be displayed in instructions to recipients. The text specified here is used by the %%ORGANIZATION_NAME%% template variable. In the **System email address** text box, enter the address that you want to appear in auto-generated communications sent by the appliance. Click **Save**.

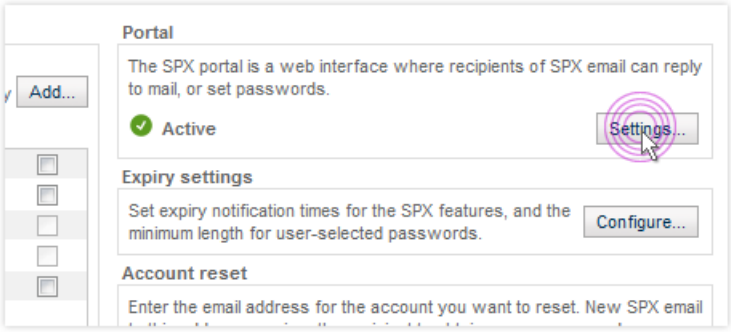


View the **SPX Encryption** tab. You will see the new template that has been created. If you want to change anything, you can click the name of the template to edit it. Note that the SPX portal is now active, indicated by the green icon.

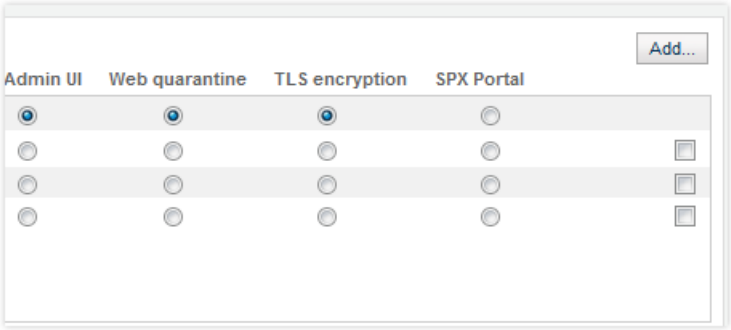


2. **Configuring the SPX Secure Email Portal**

a) On the **SPX Encryption** tab, click the **Settings** button.



The **Configure SPX Portal** dialog box is displayed.

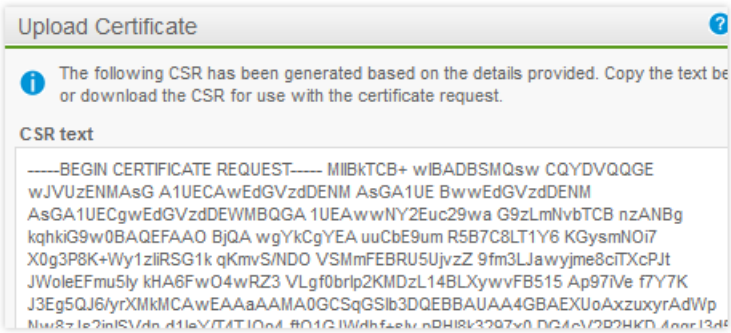


The dialog box shows that the Email Appliance is using its default, self-signed certificate. Sophos recommends never using the default certificate for services exposed to the internet. Instead, obtain a valid certificate. This ensures that the appliance references the desired hostname rather than the internal hostname that it uses by default.

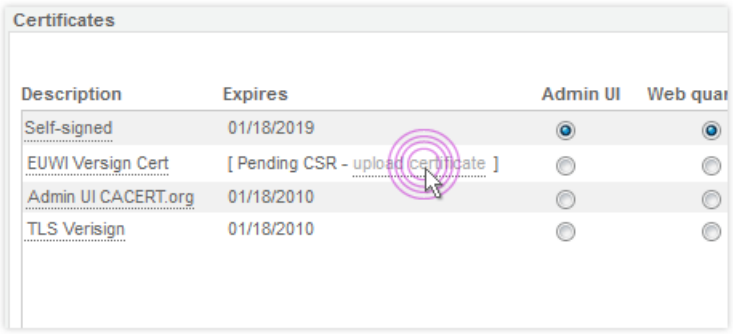
b) To obtain a certificate for the appliance, close the **Configure SPX Portal** dialog box, then on the **Configuration ➤ System ➤ Certificates** page, click **Add**. This opens the **Add certificate** dialog box, where you select **Initiate Certificate Signing Request**. Click **Next**.

c) Enter the information required to obtain a certificate. In this example, use `msgportal.example.com` for the **Hostname/Domain**, then click **Next**.

d) A certificate signing request (CSR) will be generated that you can send to the certificate authority (CA) of our choice in order to purchase a valid certificate. In the **CSR text** box, click **Download**. Use your web browser to save the text as a `.pem` file. Click **Close**.



e) In the list of certificates shown on the **Configuration ➤ System ➤ Certificates** page, the new certificate request is shown as a *Pending CSR*. Next to its description will be an **upload certificate** link. After you've obtained your new certificate from the authority, click this link to upload it.



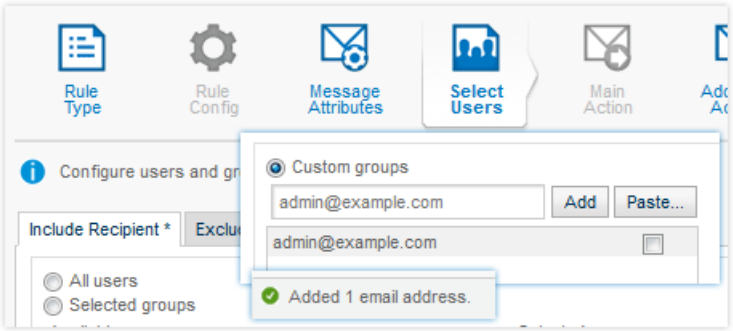
The **Upload Certificate** dialog box will be displayed, and you can either paste or upload your new certificate. This completes the certificate creation process.

Note: Although this example shows how to use the appliance's built-in capabilities to obtain a new certificate, you can also use an existing certificate for your appliance.

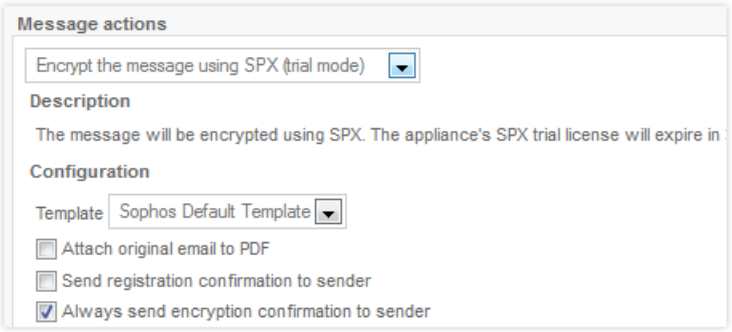
f) Now, configure your SPX portal to use the new certificate. On the **Configuration ➤ Policy ➤ Encryption** page, select the **SPX Encryption** tab. Under **Portal**, click **Settings**. In the **Configure SPX Portal** dialog box, select the **Use hostname from SSL certificate** option, and port **10443**. Click **OK**.

Important: You should ensure that your firewall allows access to port 10443.

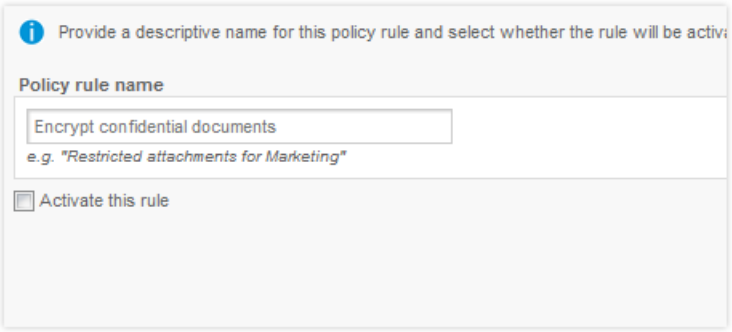
3. **Configuring expiry settings and password strength**
   a) Under **Expiry and user password settings**, click **Configure**. Confirm that the expiry settings are correct, accept the default password length, and click **OK**.
4. **Configuring a policy rule**
   a) Create a policy rule that uses the SPX template and the portal settings. You can configure multiple rules associated with SPX encryption, but an extremely useful rule is one that allows internal users to specify that a message be encrypted by setting a "confidential" option in the sender's mail client (for example, Microsoft Outlook). To do this, on the **Configuration ➤ Policy ➤ Additional Policy** page, select the **Outbound** tab, then click **Add**. This opens the Policy wizard. Select the **Use only message attributes** option, then click **Next**.
   b) In the **Identify message attributes** section, click **Add**. This opens the **Add Message Attribute** dialog box. Since setting the "Confidential" option in Outlook creates a mail header called "Sensitivity", with a value of "company-confidential", the policy rule must use these keywords too. Select the **Header** option from the drop-down list. Then, in the **Name** text box, add a header `Sensitivity`, and select **is (exact match)**.
   c) In the **Value** text box, enter `company-confidential`. Click **Apply**. In the list of message attributes, you will now see a single, new attribute that is based on your selections. Click **Next** to set user and group options.
   d) Before applying this new rule to active users, you should ensure that it works. To do this, on the **Select Users** page of the Policy wizard, add a custom group. This should consist of a single, internal email address that you can use for sending test messages. Make sure it is included in this policy rule (ensure that the address is specified on the **Include Sender** tab), then click **Next**.



e) On the **Main Action** page of the wizard, select the message action **Encrypt the message using SPX**. From the **Template** drop-down list, select the template you created. Select the **Attach original email to PDF** check box. Select the **On failure, bounce to Sender** option, then click **Next**.



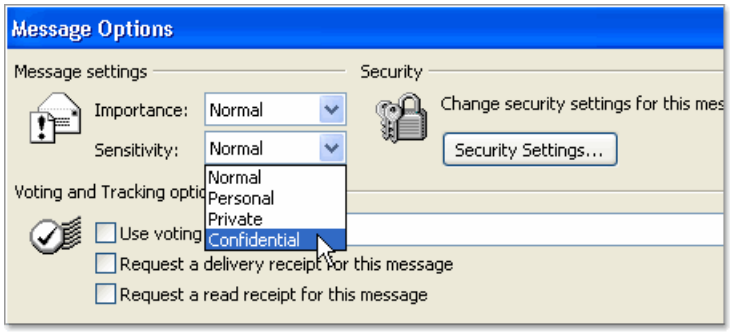
f) Now that you have finished configuring this rule, give it a descriptive name. Select **Activate this rule**, and click **Save**.



You are now ready to test your SPX encryption setup.

5. **Testing your setup**

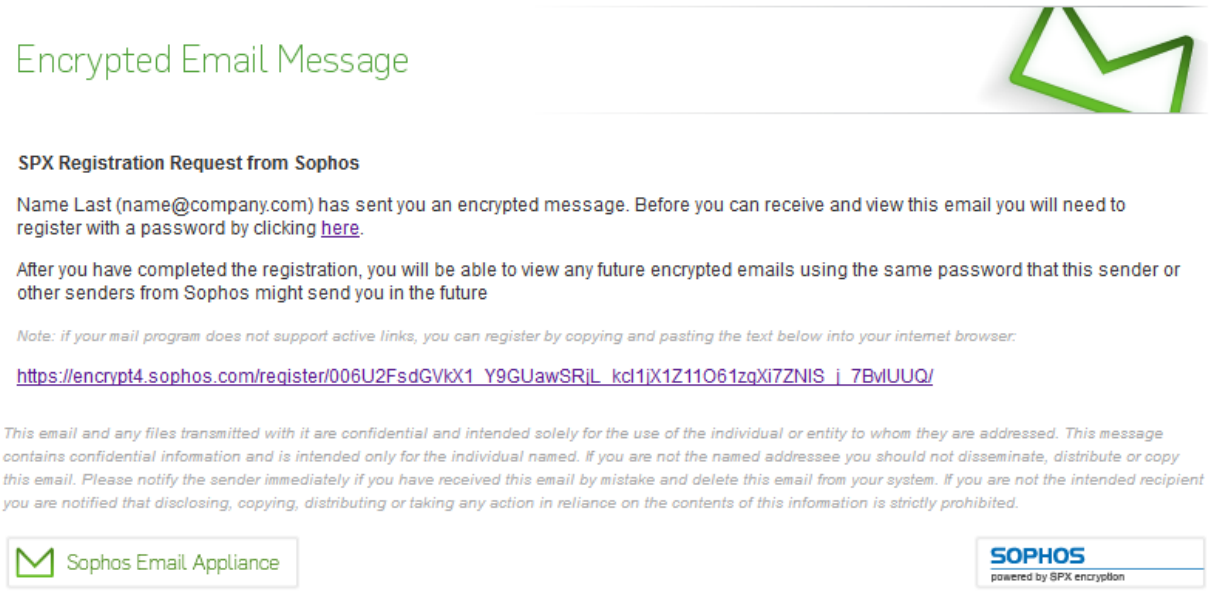
a) Compose a message. To test properly, send this message to an external email address that you can access. Since this example uses Microsoft Outlook, you must change the email client's settings to match those in the appliance. In Microsoft Outlook, click **New** to create a message. On the **Message** tab, click the dialog box launcher in the bottom right section of **Options** to open the **Message Options** dialog box. From the **Sensitivity** drop-down list, select **Confidential**. (If the email client is equipped with the Sophos Outlook Add-in, and configured to use Outlook's **Confidential** sensititvity, you can simply click the **Encrypt** button on the Outlook toolbar. For more information, see “Sophos Outlook Add-in” in the Appendix.)



After you have finished, send the message.

Note: If you are using a mail client other than Microsoft Outlook, see its product documentation for instructions on creating the “Sensitivity: company-confidential” mail header.

b) Next, check your messages at your test email address. You should receive an email message that looks something like this:



In this example, users need to set their own passwords with the SPX portal. The encrypted email will be held by the Email Appliance until the recipient registers a password.

Note: With both user-registration passwords and sender-communicated passwords, once the password is set, the email user can access any subsequent email messages from that sender, and messages are sent to the recipient(s) immediately.

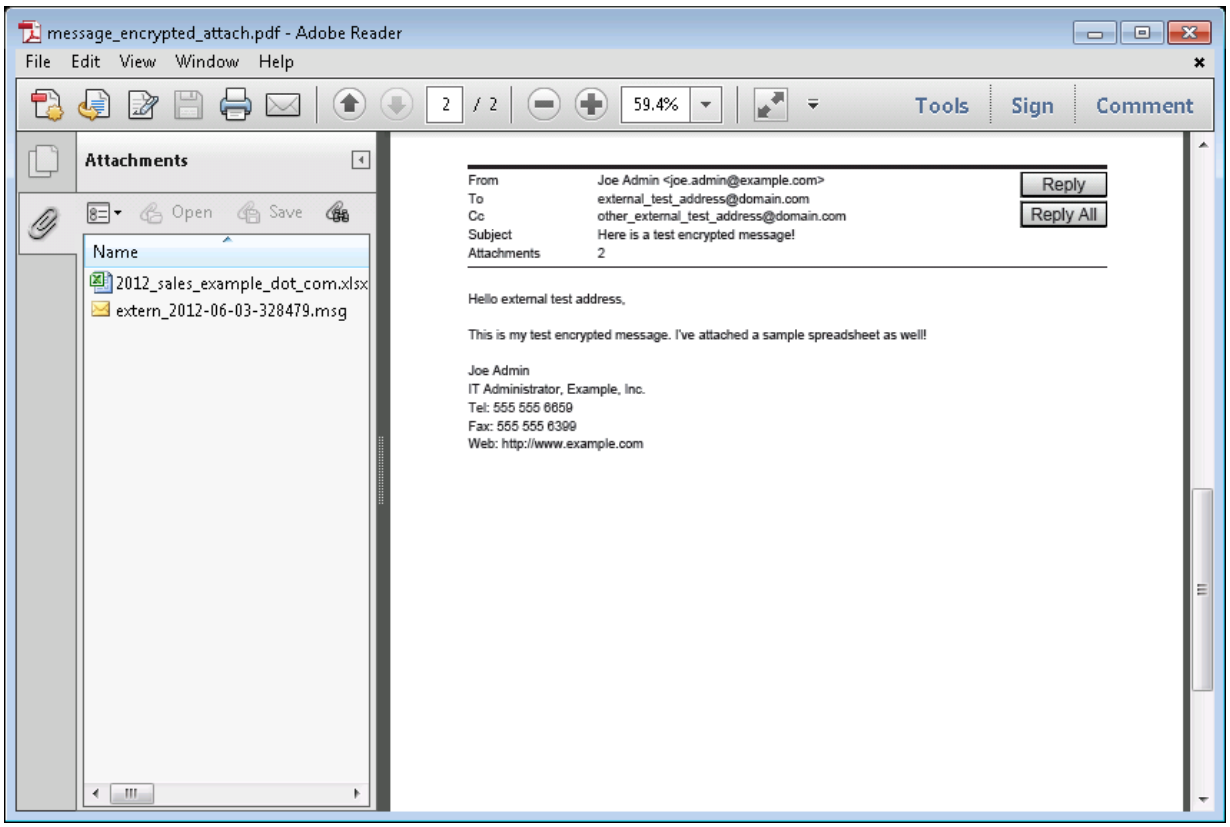
c) After the password has been set, you will receive the original (but encrypted) message at your test account.

Double-clicking the attached PDF opens it in Adobe Reader, where you are prompted to enter the password that was set.

d) After you enter the password, the PDF is decrypted, and the cover page is displayed. You can scroll past the cover page and read the original message, and download any attachments.

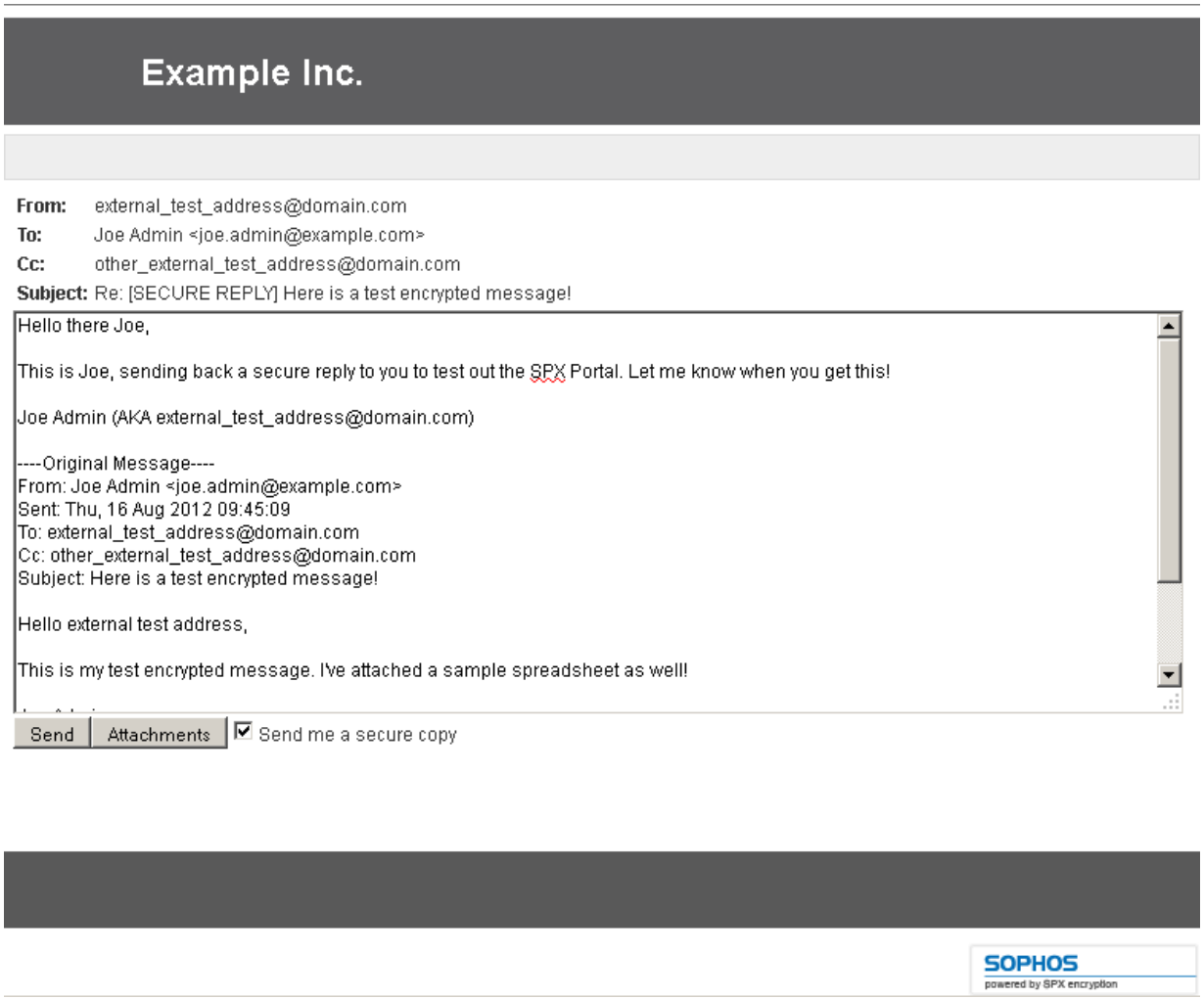
A **Reply** button is displayed in the message. This lets the recipient send a secure, encrypted reply to the sender using the SPX portal. Clicking the **Reply** button opens the recipient's default web browser and launches the secure reply portal.

If the optional **Reply All** feature is configured and a message has been sent to multiple addresses, each recipient has the option to send a secure, encrypted reply to both the sender and to all of the original recipients using the SPX portal. Clicking the **Reply All** button opens a recipient's default web browser and launches the secure reply portal.



Note: The recipient can also choose to reply directly from their email client. This form of reply is not encrypted, but may be suitable in instances where a secure reply is not essential.

e) In the secure reply portal, compose and send a response to the original email message.



After you have sent it, confirm that you received a response at your internal address. You have now confirmed that all aspects of your SPX deployment work correctly. The setup is now ready for active users.

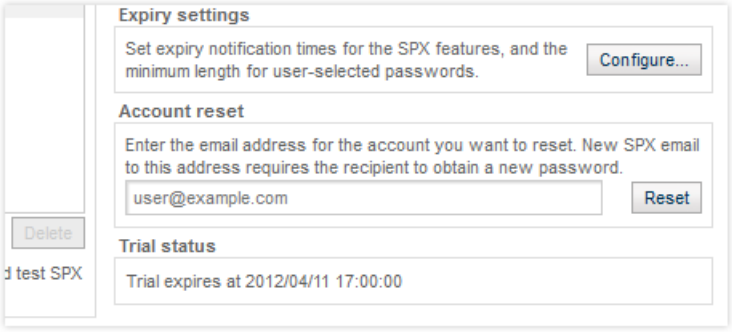
Password Management

Considerations and guidelines for SPX passwords.

Best Practices

There are various considerations when managing passwords:

- You should encourage people using the password service to avoid obvious passwords, such as names, important dates and common words.
- When using sender-communicated passwords, the message sender should not email the password to the recipient. Instead, a more secure method should be used, such as telephoning or talking in person.
- In the **SPX Expiry and Password Limits** dialog box (opened by clicking **Configure**), you can set the number of days an SPX password will remain valid. If the recipient does not use the password to access email within the given time period, the password will expire.
- Also in the **SPX Expiry and Password Limits** dialog box, you can set the minimum length for a password. Users receive an error message if their chosen password does not meet this requirement.



Password Management Comparison

Password Method	Advantages	Considerations	Best Practices
User Registration	Scalable Automated Easy to use	Can be susceptible to man-in-the-middle attacks. Initial registration email messages could be perceived as a phishing attempt.	Ensure that the senders' first encrypted message to new recipients does not contain any sensitive information. The introductory message will trigger automatic delivery of a registration email requesting that the recipient create a username/password for the purpose of decryption. The first message should inform the recipient that the confidential message has yet to be delivered. The sender should then confirm that the registration was successful before sending a message containing confidential information.
Generated Password	Secure. Ensures that messages cannot be intercepted, and only intended recipients have access to those messages.	Requires a phone call or other secure communication method by the sender to communicate the password to the recipient.	Inform senders of how this method works, and provide suitable methods for communicating the generated password. In particular, they should never forward the email that contains the generated password.
Sender-specified Password	Reduces adminstrator workload with sender-managed passwords. Secure. Ensures that messages cannot be intercepted, and only intended recipients have access to those messages.	Requires a phone call or other secure communication method by the sender to communicate the password to the recipient. Senders should select passwords that are difficult to guess. If a message is sent to a recipient who is not in a group that triggers the policy rule for sender-specified passwords, the message will not be encrypted. The password will remain in the subject line of the email delivered to this recipient. Message subjects that contain passwords may be displayed when performing log searches.	Inform senders of how this method works, and provide suitable methods for communicating the generated password. In particular, when the **Notify password sender by email** option is selected, senders should not forward the email that contains the password. It is also recommended that senders understand how to select strong passwords.

Password Method	Advantages	Considerations	Best Practices
		Message subjects that contain passwords may be displayed if a message is in the mail queue when a queue search is performed. Messages sent to multiple recipients will be encrypted using the same sender-specified password. The sender must communicate the password to each of the recipients.	
Custom Web Service	Integrates with existing authentication systems or user/password stores using a web service.	Requires custom web development.	Implementing this method is usually accomplished by working with Sophos Professional Services.

SPX Best Practices

Registration Email

Custom registration email messages should include several important elements. Registration email messages should clearly indicate:

- The name of the sender.
- Your company name (as specified on the **Template Name** page of the wizard).
- An indication of when the recipient can expect to receive the message.
- Contact information, or a link to a FAQ in case the recipient has questions.
- Information indicating that the recipient must register to obtain a password.
- Any additional information that will assist the recipient in understanding that they are receiving a legitimate request from a trusted sender.

Encrypted email - Unencrypted Message Content

Certain file types cannot be opened by opened by Acrobat Reader when attached to encrypted SPX email messages. These file types include, but are not limited to:

- .zip
- .exe
- .bat
- .dll
- class

If you select the **Attach original email to PDF** option when configuring the **Encrypt the message using SPX** on the *Main Action* (page 47) page of the wizard. It will ensure that recipients can save and easily reopen their own unencrypted copy once they have received and successfully decrypted an SPX message.

PDF Cover Pages

To make your own cover pages, you can use PDF creation software such as:

- Adobe Acrobat
- Cute PDF
- Primo PDF
- Microsoft Office (may require the “Microsoft Save as PDF or XPS ”add-in)

- PDF Creator
- Open Office

General guidelines for PDF cover pages include:

- Cover pages should be saved in PDF 1.5 (or newer) format.
- Text indicating that the content is included on following pages, and is encrypted.
- Information on how to view any included attachments.
- Information on whether the recipient can create a secure reply to the message, with instructions on how to do so.
- No more than two pages in length.
- Should include the name of your company, contact information, and your company logo.
- Should include an embedded link to your corporate website.
- The page should have graphics or text that span the full length of the page, so that it is always obvious that the cover page is not blank. This could occur, for example, when a user whose PDF reader default settings include opening at a high zoom. The cover might appear blank if opened and zoomed in on the whitespace at the bottom.
- Support contact information in the event that the recipient encounters any difficulties.

A sample cover page with our recommended elements can be viewed *here*.

Supported PDF Readers

Supported PDF readers include Adobe Reader 7.0 and later on Windows. Adobe Reader 9.0 or later is required if you select 256-bit encryption in the SPX Template Wizard. For more information, see “Encrypted PDF Options.” Other PDF readers may work, but are not supported.

SPX End User Experience

Once you have enabled SPX encryption on the Email Appliance, this functionality will be available to senders of encrypted messages and their recipients. They will have access to any features you chose to make available. For example, you can let recipients manage their own passwords. If these settings are enabled, recipients have access to features that allow them to recover, reset, or change their passwords using the appliance's SPX Secure Email Portal.

Any instructions that you want to convey to recipients must be included in the template text. If recipients are required to use the SPX portal, the individual pages of the portal will serve as a guide. Any images you selected for the portal are displayed on these pages.

Regardless of which password method you select, after a password has been established, the user experience for both sender and recipient is similar.

Configuring the Sender's Email Client

To trigger SPX encryption, senders must configure their email clients to correspond with the Email Appliance policy. Depending on what you have set on the appliance, this could simply be a matter of including a keyword, such as "confidential," in the subject line of the message.

Note: Alternatively, you can deploy the Sophos Outlook Add-in, which allows email senders to encrypt a message with one click of a button on their Microsoft Outlook toolbar. The encryption is then triggered according to what you have configured for the Add-in and the Email Appliance. For more information, see "Sophos Outlook Add-In" in the Appendix.

For step-by-step details of how to configure an email client to work with the Email Appliance, see either of the examples in the "SPX Deployment Guide."

Important: Regardless of your chosen method, you must inform senders about what is necessary to trigger the SPX encryption policy rule you have created.

Communicating with SPX: Basic Steps

Recipients access the SPX portal via the hyperlinks that you provide in the instructions accompanying all encrypted messages. If you opt to have recipients set their own passwords, an instructional message with a link to the portal is sent to the recipient. In both cases, the instructional messages will also include any images (for example, corporate logos) that you added through the wizard.

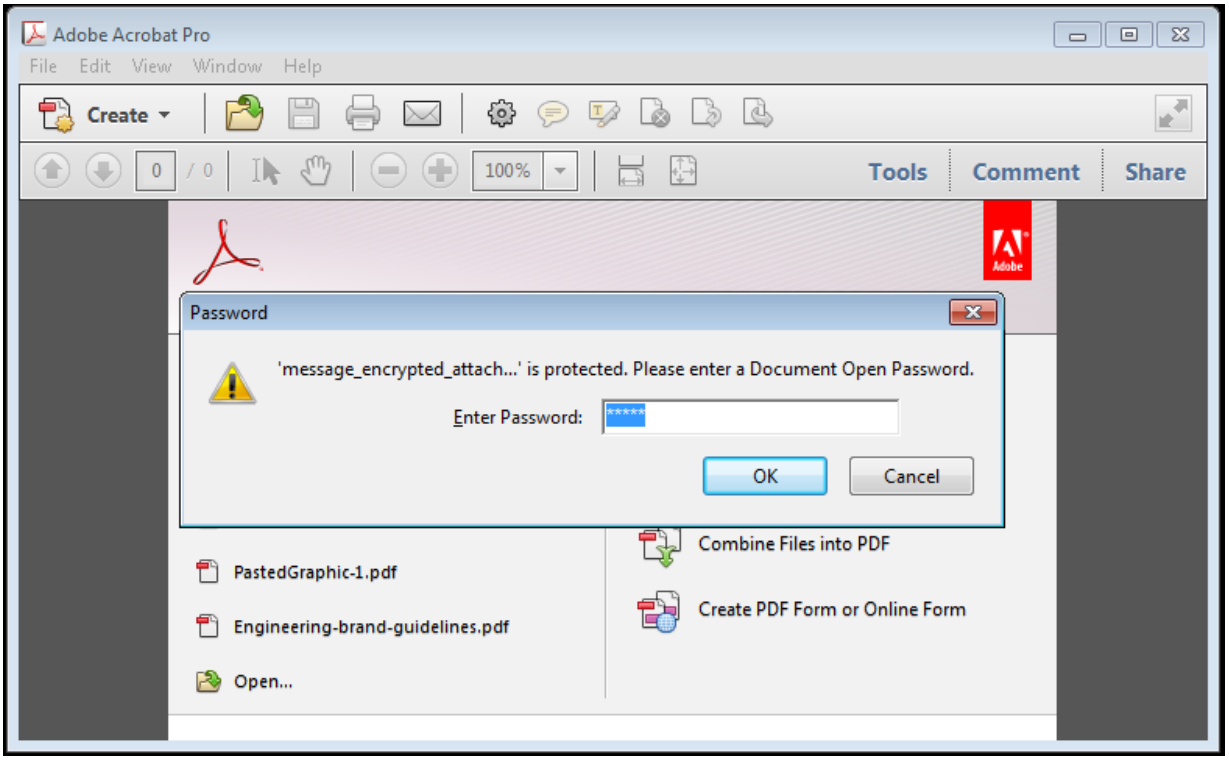
After a sender in your organization sends an SPX-encrypted email to a recipient, the following occurs:

1. A password is established for the recipient using one of three methods (see *Choosing an SPX Password Method* (page 78) for more information). When creating passwords, recipients should follow the guidelines laid out in the "Best Practices" section of *Password Management* (page 102).
2. The message is encrypted and sent to the recipient. The sender may also receive a confirmation that an encrypted message has been sent, if you have enabled that feature.
3. The recipient receives, decrypts, and reads the email.
4. [Optional] The recipient sends a secure response to the encrypted message. The SPX password may be required for a secure response, if you have enabled that setting.

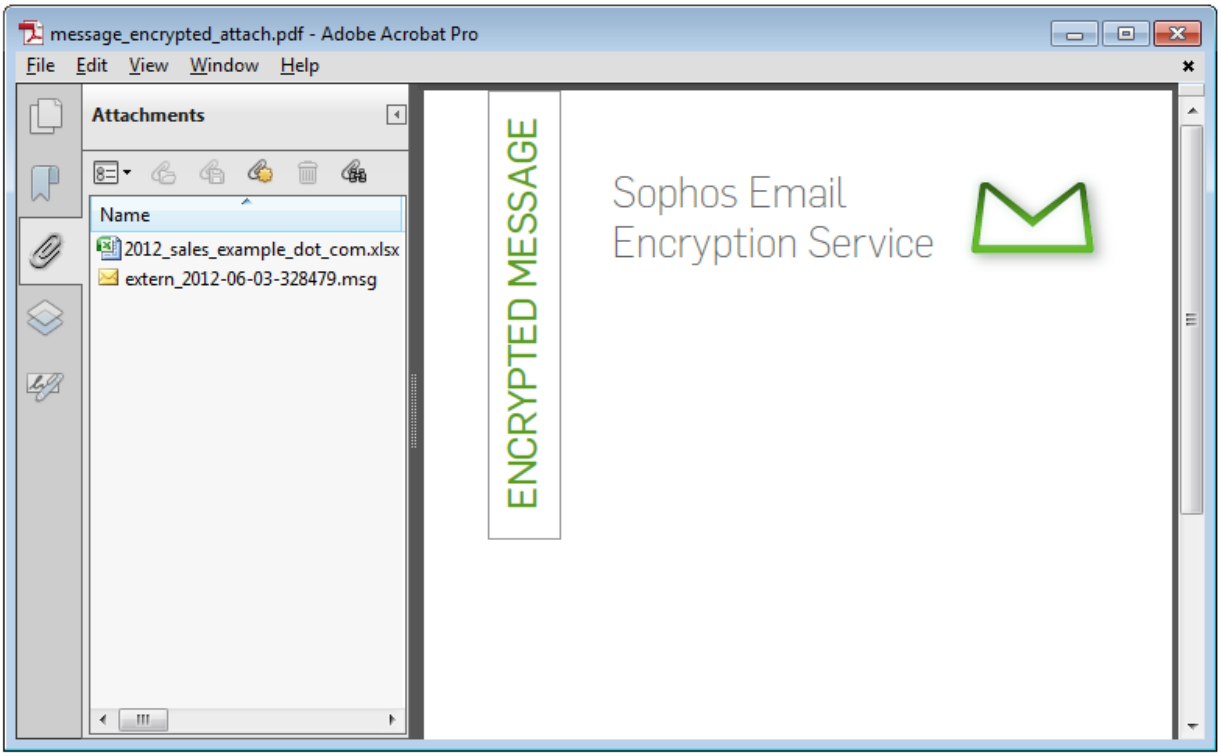
Receiving Encrypted Messages

After recipients are sent an encrypted message, they have several options. They can:

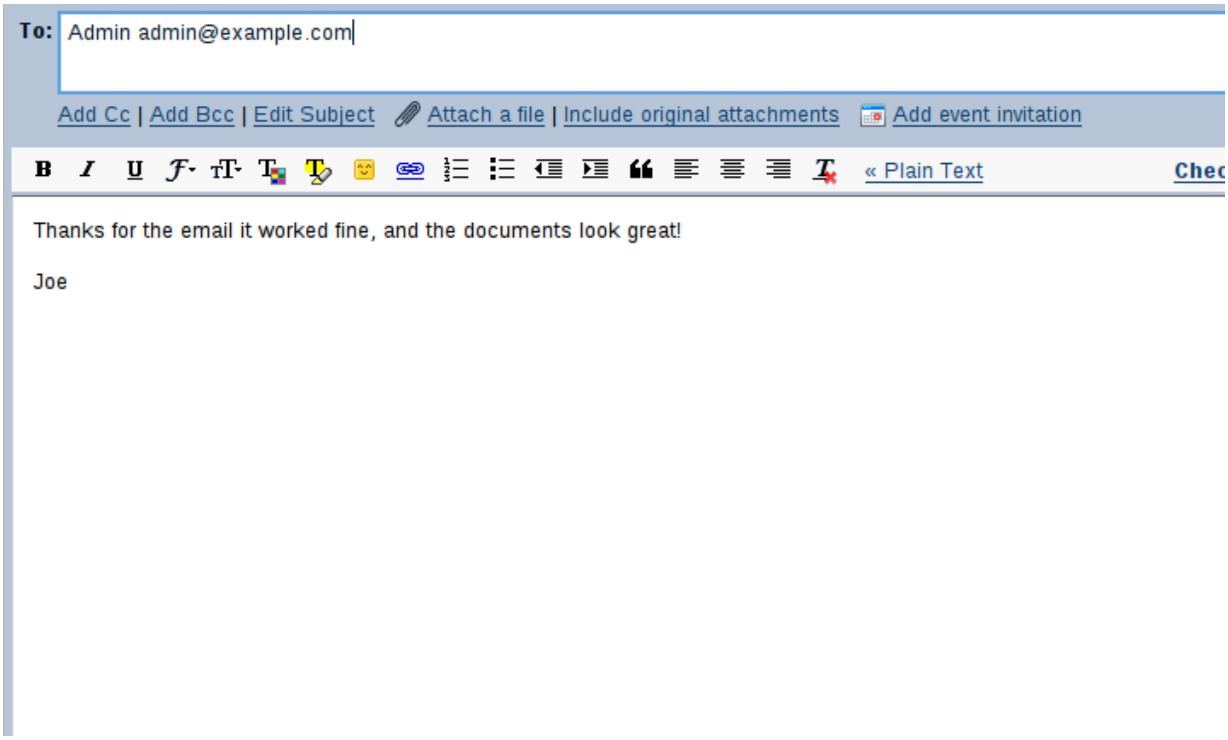
- Store the message in its encrypted format. This will always require the recipient to use a password to decrypt and view the message.



- Save a copy of the original message. If **Attach original email to PDF** is selected in the associated policy rule, the content will be included as an attachment to the encrypted PDF.



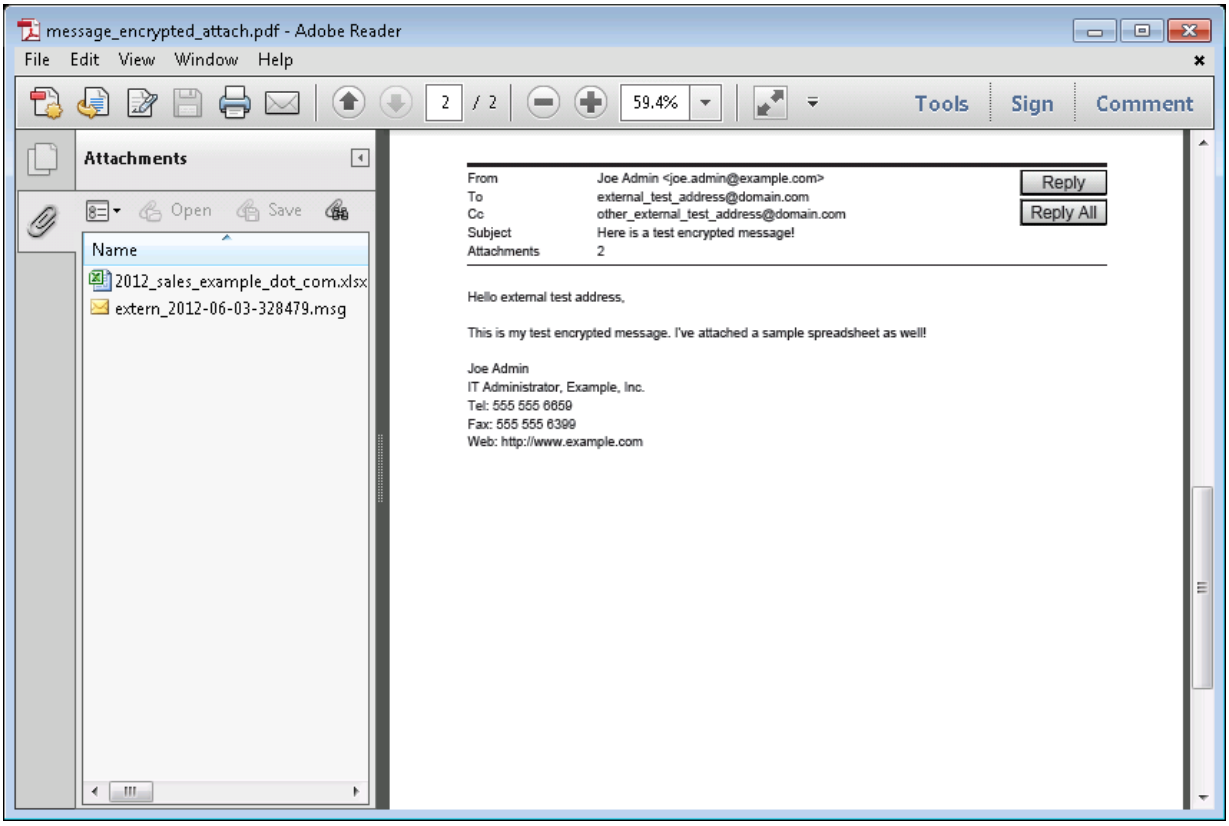
- If a secure reply is *not* needed, they can reply to the encrypted message using their mail client.



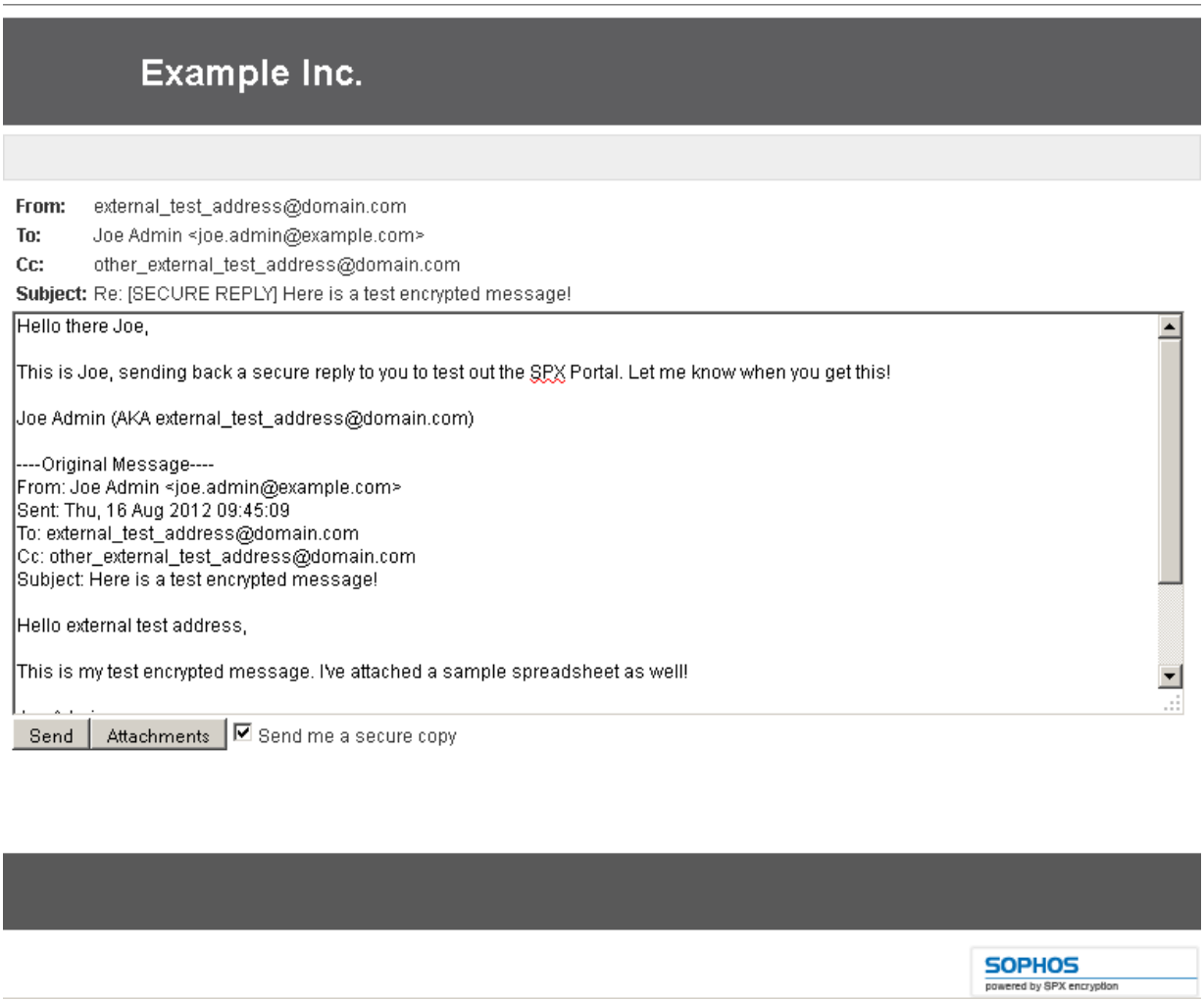
Responding with Secure Reply

If secure reply is enabled on the **Portal Settings** page of the SPX Template wizard, recipients have the option of responding securely to an encrypted message. Secure reply works as follows:

1. Encrypted message is delivered to recipient.
2. Recipient uses password to open encrypted PDF.
3. Recipient clicks **Reply**. If there are multiple recipients and the **Reply All** feature has been enabled, the recipient can click **Reply All** to respond to the sender and all recipients.



4. Recipient gains access to the SPX portal via the default web browser. (The SPX password may be required, if you have enabled that setting.)



Note: When recipients are required to enter a password to access the SPX portal, they are allowed six login attempts. Following that, they are locked out of the portal for 24 hours.

5. Recipient sends secure reply, which is delivered to the original sender through the Email Appliance over HTTPS, maintaining the security of the communication. If the recipient clicked **Reply All**, secure replies will be sent to all recipients of the message.
6. Optionally, original sender continues the secure communication by sending a response within another encrypted PDF.

Using SPX Passwords

- **What can email recipients do to recover, restore, or change their passwords?**

  Depending on which features you have made available, recipients may have a variety of options, or none at all. When you select one or more **End user password options** on the **Password Settings** page of SPX Template wizard, text containing template variables is automatically inserted in the instructional text that is delivered to recipients with each encrypted message. Links are created in the text that recipients can use to visit password management pages on the SPX portal.

  Note: When recipients are required to enter a password to access the SPX portal, they are allowed six login attempts. Following that, they are locked out of the portal for 24 hours.

- **How do recipients view encrypted messages if they've lost their password?**

If you have enabled the **Password recovery** option, recipients can click the link included in each instructional message to access a page on the SPX portal where passwords are recovered and reset. Recipients are then prompted to answer a least one challenge question in order to retrieve the password.

If you deployed SPX encryption prior to the introduction of the password recovery and reset features, or if you did not enable these features during the initial deployment of the appliance, then there are two options:

1. If recipients know their existing password, they can use the SPX portal to change the password. If password recovery is enabled, they can then set a question or questions that can be used for future recoveries.
2. If a recipient has forgotten the current password, you can establish a new password using the **Account Reset** option on the **SPX Encryption** tab. The recipient can then choose a password question or questions that can be used for future recoveries.

Recipients who were issued passwords prior to the availability of the recovery feature, will *not* have access to previous encrypted messages if they have forgotten their password. Encrypted messages cannot be read without the password that was active during the period that those messages were sent.

Customizing SPX

SPX can be customized to meet the specific needs of your organization. You can make your own cover pages for SPX email messages using a variety of PDF tools, including Adobe Acrobat. You can add custom logos to your recipient instructions message and the SPX portal. These are displayed in the form of headers and footers that portal visitors see. You can also use certificates with an internet-facing SPX portal to ensure that connecting recipients can verify the authenticity of your site.

Creating Custom Logos

You can add custom logos, so that they are displayed in the SPX Secure Email Portal, and/or the recipient instructions message that accompanies encrypted messages. To do this, you should navigate to the **SPX Template Wizard**, and select either the **Portal Settings** or **Recipient Instructions** page. Then:

- Create custom header and footer images. It is recommended that these include your organization's logo, web address, and other distinct identification information that you want users to see.

  Header and footer images must be JPG, GIF or PNG format. The portal and recipient messages are optimized to use images that are 752 pixels wide by 69 pixels high. Other image sizes may be used, though results may vary.
- Use the **Header image** option buttons to select to select the **Custom** option, then click **Upload** and select your custom header image.
- Use the **Footer image** option buttons to select to select the **Custom** option, then click **Upload** and select your custom footer image.

Certificates, Load Balancers and the SPX Portal

How to use encryption certificates and load balancers with the SPX Secure Email Portal.

Using Certificates With Internet-facing SPX Portal Deployments

Sophos strongly recommends certificates that use the Email Appliance's external hostname, especially if the appliance is accessible through the internet. This ensures that recipients who connect to your SPX portal will be able verify the authenticity of your site's identity. There are several possible scenarios, depending on how many appliances you use, and how they are configured:

- **Single appliance, facing the internet**: You can choose to expose only one appliance's SPX portal to the internet, even if you use multiple appliances in a clustered scenario. This is the simplest choice, and the easiest to manage, but it lacks redundancy. In this case, you need only a single external hostname and a matching certificate.
- **Multiple appliances with no load balancer**: If you use multiple appliances with no load balancer, they must be carefully configured to act as a single SPX portal. If they do not appear as the same host, PDF reply links may not direct recipients to the correct host. Each appliance must be configured to use the same external hostname, and must use the same certificate. You will need multiple **A** records configured in your DNS server.
- **Multiple appliances using a load balancer**: When an external load balancer is used, configuration is simpler. While all the appliances must still use the same certificate, the load balancer will manage any requests, and the SPX portal

hostname should be associated with it instead. Note that the hostname on the certificate should match the hostname associated with the load balancer.

SMTP Authentication

If you want to grant your end users the ability to send email through the appliance from an external network, you can enable SMTP authentication. With SMTP authentication configured, authenticated users are treated as if they were sending mail from inside the network, and the same outbound policy rules apply.

It is strongly recommended that you also enable Transport Layer Security (TLS) to encrypt the credentials required for SMTP authentication because SMTP authentication alone does not provide a secure connection.

Only users with a valid username and password will be able to connect from an external network.

Use the **Configuration ➤ Policy ➤ SMTP Authentication** page to enable and configure SMTP authentication.

Important: You must configure directory services before you can enable SMTP authentication. For more information, see "Directory Services." End users must also configure their email clients in order for SMTP authentication to take effect. See the Sophos Knowledgebase for instructions on *Configuring SMTP Authentication in Outlook 2007*.

To configure SMTP authentication for end users:

1. Select the **Enable SMTP Authentication** check box to begin configuring the appliance so that users can send email from an external network using SMTP authentication. (This check box cannot be selected if Directory Services have not been configured.)

   The grayed out SMTP authentication options become available.

2. **Authentication**: Confirm that directory services are configured. If they are not, click **Configure directory services settings** to access the **System: Directory Services** configuration page. You must configure directory services for SMTP authentication to take effect.

   If directory services are configured, a drop-down list containing all configured directory servers is displayed. If you have configured multiple directory servers, the appliance can only perform SMTP authentication for one of them. Select this server from the list.

3. **TLS Encryption**: Enable and configure TLS.
   a) **Status**: If TLS is not enabled, it is strongly recommended that you enable it to protect authentication credentials and other potentially sensitive data. Click **Configure TLS settings** to access the **Policy: Encryption** configuration page.
   b) **Enforce TLS**: It is strongly recommended that you select this check box to make TLS mandatory for your end users. When it is selected, end users who are sending email via SMTP authentication must encrypt it using TLS, or their connections will be rejected.

4. **Ports**: Select one or more of the available ports to use for SMTP authentication. Port 587 is selected by default. Whichever port(s) you choose, the network must also be configured to permit remote access to the appliance over the designated port(s). An alternative port is 465. You must select at least one port.
5. Click **Apply**.

SMTP Options

On the **Configuration ➤ Policy ➤ SMTP Options** page, you can configure a variety of SMTP settings using the **General**, **Perimeter Protection**, and **Advanced** tabs.

Configuring General SMTP Options

You can configure a variety of SMTP options using the **General** tab.

To configure general options:

- **Method of recipient validation**: Recipient validation can be done using either SMTP look-ahead, Configuration Synchronization, or directory services. It can also be turned off, but this is not recommended unless you have a specific requirement.
  - **Via downstream SMTP look-ahead** (recommended): The Email Appliance's mail transfer agent (MTA) uses SMTP recipient validation. The MTA will connect to the internal mail server to confirm that an address exists.

    In most cases, this form of recipient validation is preferable because it does not require an LDAP query that is comprehensive enough to include all addresses that should be accepted. Instead, the Email Appliance accepts or rejects messages, based on a response from the Microsoft Exchange server about whether the recipient is valid.
    - **Advanced**: Click this button to open the **Advanced Recipient Validation Settings** dialog box, and configure options for caching of recipient data. The default settings are applicable for most organizations. Do not adjust these settings or clear the cache unless there is a special requirement.
      - **Expire negative responses after**: Enter the frequency with which failed address verifications are expired from the cache. The default is 3 days.
      - **Refresh negative responses every**: Enter the frequency with which failed address verifications are refreshed. The default is 3 hours.
      - **Expire positive responses after**: Enter the frequency with which successful address verifications are expired from the cache. The default is 31 days.
      - **Refresh positive responses every**: Enter the frequency with which successful address verifications are refreshed. The default is 7 days.
      - **Clear Cache**: Deletes all cached results, positive and negative.
      - **Reset to Defaults**: Restores the factory settings.

  - **Via Configuration Sync**: You can maintain lists of some configuration data, including recipient validation, in text files. With Configuration Synchronization you can use the SCP protocol to sync those lists to the Email Appliance.

    Note: If you are setting recipient validation using Configuration Synchronization, you should SCP a copy of your `SOPHOS_RECIPIENT_VALIDATION` file to the Email Appliance before setting **Method of recipient validation:** to **Via Configuration Sync**. For more information, see the *Configuration Sync* (page 139).

  - **Via directory services**: The Email Appliance's mail transfer agent (MTA) uses directory services queries to determine if messages are addressed to valid recipients. You should ensure that your directory services settings are configured correctly.
  - **Disable recipient validation**: Turns off recipient validation. It is recommended that you do not disable recipient validation, unless you have specific requirements.

- **Global Message Size Limit**: Reject attachments that exceed a maximum size. It is recommended that you choose the smallest possible size limit because processing multiple large attachments at the same time may reduce the performance of the appliance.

  Note: Selecting **Unlimited** is not recommended, and should be avoided if possible.

- **MTA banner string**: Optionally, enter a banner string that replaces the default string. This setting has two available template variables: %%HOSTNAME%% and %%VERSION%%. By default, the hostname of the Email Appliance is displayed, along with the appliance version.
- **MTA HELO string**: Optionally, enter a HELO string (hostname or IP address) that replaces the default string. This setting has one available template variable: %%HOSTNAME%%. By default, the hostname of the appliance is displayed.

Configuring Perimeter Protection

Use the features on the **Perimeter Protection** tab to defend against denial of service and directory harvest attacks and to block mail from non-existent domains.

Note: The options on this page are turned on by default, and the threshold settings for denial of service and directory harvest protection are appropriate for most organizations. It is not recommended that you make adjustments unless you have advanced knowledge of mail transfer agents and SMTP.

- **Block mail from non-existent domains**: This option, selected by default, prevents the receipt of mail from external senders with DNS or MX records that are non-existent or malformed. It is recommended that this option always remain enabled. It should only be turned off if you have specific needs, such as a requirement to receive email from a sender who is unable to configure a valid DNS entry for their domain.
- **Denial of service and directory harvest protection**: This option, selected by default, enables MTA-level throttling, which rejects messages from mail relays that exceed the configured limits.
  - **Maximum simultaneous connections for each connecting SMTP relay**: Messages from such relays are rejected until traffic from the relay drops below the limit. This option should not be enabled in network configurations where the Email Appliance is not at the gateway (that is, it has trusted SMTP relays between the Email Appliance and the internet). The default is 50 connections.
    - **Within a time window of** : The amount of time in seconds for which the settings below apply. The default is 60 seconds.

      Note: Setting any of the following options to "0" means that there is no maximum. The number of connections, requests, recipients, or sessions becomes unlimited. Each of the following settings is per client.

      - **Max connections**: The number of connections permitted within the defined time window. The default is 1000 connections.
      - **Max delivery requests**: The number of requests permitted in the defined time window. The default is 100 requests.
      - **Max number of recipients**: The number of recipients permitted within the defined time window. The default is 5000 recipients.
      - **Max number of TLS sessions**: The number of new TLS sessions permitted within the defined time window. This does not include any cached sessions. The default is 0.
  - **Reset to Defaults**: Returns all of the “session count” and “rate controls” to their default values.

After you have made any necessary changes you can:

- Click **Apply** to save your changes.
- Click **Cancel** to discard your changes.

Configuring Advanced SMTP Options

Use the options on the **Advanced** tab to fine-tune the mail queue, queue monitoring, and SMTP server settings.

Note: The default settings on this page are optimal for most organizations. It is not recommended that you make adjustments unless you have advanced knowledge of mail transfer agents and SMTP.

To configure advanced SMTP options:

If necessary, adjust the value of any of the following settings.

Mail queue settings

- **Queue run delay**: The time between deferred queue scans by the queue manager. The deferred queue contains mail deliveries that have failed for a reason that may be temporary. This value should be less than or equal to the next two settings (“Min backoff time” and “Max backoff time”). The default is 180 seconds.
- **Minimum backoff time**: The minimum amount of time between attempts to deliver a deferred message. The default is 180 seconds.
- **Maximum backoff time**: The maximum amount of time between attempts to deliver a deferred message. The default is 4000 seconds.

- **Maximum queue lifetime**: The maximum amount of time that a message is queued before it is returned as undeliverable. The default is 5 days.
- **Bounce queue lifetime**: The maximum amount of time that a bounce message is queued before it is treated as undeliverable. The default is 5 days, which matches the default setting for “Max queue lifetime.”
- **Queue manager message recipient limit**: The maximum number of recipients held in memory by the mail transfer agent's queue manager. The default is 20000.
- **SMTP destination concurrency limit**: The maximum number of parallel deliveries to the same destination. The default is 20 connections.
- **SMTP destination recipient limit**: The maximum number of recipients per message. The default is 50 recipients.
- **Delay warning time**: The amount of time before the sender receives the mail headers of mail that is still queued. The default is "0".

Queue monitoring

- **Queue warn threshold**: The number of messages that must accumulate in the mail queue before the “Pre-filter message queue alert” is displayed as a warning on the System Status tab.
- **Queue error threshold**: The number of messages that must accumulate in the mail queue before the “Pre-filter message queue alert” is displayed as an error on the System Status tab.

SMTP server settings

- **Incoming connection timeout**: The time limit for sending an SMTP server response and for receiving a remote SMTP client request. The default is 300 seconds.
- **Mail filter timeout**: The amount of time that the mail filter will attempt to process a message before it times out. After the specified time, the message is quarantined, and an email notification is sent to the administrator. The default is 1200 seconds. The message can be found in the quarantine by searching with the reason "Processing failure."
- **Maximum number of recipients**: The maximum number of recipients that the appliance accepts per delivery request. The default is 1000.
- **Header size limit**: The maximum amount of memory (in bytes) that is used to store a message header. The default is 102400.
- **Disable VRFY command**: Stops some techniques used to harvest email addresses. The default is "Yes" because the appliance uses other methods to protect against directory harvest attacks.
- **Soft bounce**: Continues to queue mail that would otherwise be returned to the sender. This option disables locally generated bounces, and prevents the permanent rejection of the mail. The default is `No`.
- **Reset to Defaults**: Restores the factory settings.

After you have made any necessary changes you can:

- Click **Apply** to save your changes.
- Click **Cancel** to discard your changes.

Configuring the Delay Queue

Use the options on the **Delay Queue** tab to configure options that control delayed messages. Delayed messages are suspect emails that are held for a specified period of time. By delaying delivery, the appliance creates a timed interval during which new anti-spam definitions created by Sophos Labs can be received, after which the appliance can rescan the messages using the most up to date information possible.

To configure delay queue options adjust the value of any of the following settings:

Delay queue settings

- **Status**: When set to **Collect**, the appliance will collect information in the delay queue database, but no delay action will be taken. When set to **On**, messages will be delayed once the database has enough information to delay based on IP, or if a message is otherwise categorized as suspicious. When set to **Off**, messages will not be delayed, and any messages already in the delay queue will be delivered when the **Maximum delay time** is reached. The default is **Collect**.
- **Minimum delay time**: The minimum amount of time to delay a message. The default is 10 minutes.
- **Maximum delay time**: The maximum amount of time delay a message. The default is 60 minutes.

- **Delay queue size limit**: The maximum allowed size of the delay queue. The default is 1024 MB.
- **History DB minimum threshold**: The minimum number of message records collected in the delay queue history database before the appliance begins to delay messages. The default is 1000.
- **History DB expiry threshold**: The maximum number of message records stored in the database before queued messages are expired. The default is 1 000 000 records.
- **History DB expiry age**: The maximum age in days before records expire. The default is 180 days.
- **Reset to Defaults**: Restores the factory settings.

After you have made any necessary changes you can:

- Click **Apply** to save your changes.
- Click **Cancel** to discard your changes.

System

Use the **System** pages of the **Configuration** tab to review or modify preferences for maintaining the system software on the Email Appliance. You can configure how frequently upgrades and patches are applied, who receives automatic email alerts, how configuration data is backed up, whether directory services integration is enabled, and which time zone is applied to time-related data.

Updates

The **Configuration ➤ System ➤ Updates** page displays the versions and dates of the current threat definition package and the software engine, and advises if newer versions are available. If a software engine update is available, there are also details about the nature of the update and the time and date of the next scheduled automatic update.

Software engine: The latest available software engine version is displayed. To subscribe to an RSS feed of information about appliance software updates, click the RSS icon to the right of the title. The version number is divided by decimal points into four parts, for example *2.13.2.0*. Reading from left to right, the parts signify:

Version Type	Version Element
major release	***2***.*13.2.0*
minor release	*2.**13**.2.0*
maintenance release	*2.13.**2**.0*
hotfix release	*2.13.2.**0***

Click **Check for Updates** to refresh this information.

Threat definitions: New threat definitions from SophosLabs (including anti-virus, anti-spam, and IP-blocking data) are automatically downloaded and installed throughout the day.

- An icon is displayed on the left side of the **Threat definitions** section, indicating the status of automatic updates (turns red if the Email Appliance is unable to connect to Sophos).
- **Installed**: Version number of the current threat definitions.
- **Auto Update Schedule**: The frequency with which the appliance checks for updates.
- **Last updated**: Date and time of the most recent update.

Software engine: System software updates (including critical and maintenance updates) are installed automatically, but the installation can be delayed for a limited time so that they can also be installed manually using the **Update Now** button.

- An icon is displayed on the left side of the **Software engine** section, indicating the 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 available update (if an update is available).
- **Update type**: Indicates if an update is available, and the nature of the update (for example, a critical update).
- **History**: Clicking on the history icon will display a list of all software updates that have been installed on the appliance since the history was last cleared.
- **Auto update schedule**: Date and time that the 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.

Software engine update schedule:: Displays the dates and times that the appliance's software engine will apply updates. There are two types of updates:

- **Critical updates**: these are updates that affect functionality and usability of the appliance.
- **Non-critical updates**: these are updates that may affect the appearance, or introduce new functionality, but are not necessary for the appliance to continue operating properly.

To change the software engine update schedule, click **Configure**.

Running/Configuring Updates

- To download and apply a new update before the next scheduled update window:

  Click **Check for Updates** to retrieve any available updates for an appliance or cluster of appliances.

  Click **Update Now** to install any downloaded updates for an individual appliance. If available updates are installed, the button is grayed out.

  Note: If you are running multiple appliances in a cluster, an **Update Entire Cluster** button is displayed instead of **Update Now**. Clicking it updates all listed appliances. If no updates are available, the button is grayed out

- To specify your preferred software update window:

  Use the **Software engine update schedule** to set the time window in which automatic software updates are installed.

  Critical updates (for example, security-related patches) are applied automatically within 24 hours of availability during the update window. Maintenance updates are applied automatically during the update window, but only on the days of the week specified in the check boxes.

  1. Click **Configure**.
  2. In the **From** and **to** drop-down lists, specify the window of time in which to apply automatic updates.
  3. Select the day of the week check box(es) to specify the day(s) on which non-critical automatic updates are applied.
  4. Click **OK**.

Alerts & Monitoring

Use the **Configuration ➤ System ➤ Alerts & Monitoring** page to do the following:

- Configure who in your organization should receive Email Appliance-generated email alerts regarding the health of the Email Appliance.
- Temporarily turn off alerts sent to Sophos during periods when you are evaluating or testing the Email Appliance.
- Set the contact information for the person in your organization that Sophos should contact if they detect problems with your Email Appliance.
- Specify a postmaster address.
- Enable and configure simple network monitoring protocol (SNMP).

The Email Appliance is self-monitoring, and it can notify administrators via email whenever there is reason for concern. The full list of possible alerts can be viewed on the **System Status** tab.

Email

Use the **Email** tab on the **Configuration ➤ System ➤ Alerts & Monitoring** page to configure the recipients of local alerts.

- *To add an entry to the **Local alert contacts***:

  1. Enter an email address to which you want alerts to be sent in the **Local alert contacts** text box.
  2. Click **Add**.

- *To remove an entry from the **Local alert contacts***:

  1. Select the check box next to the address that you want to remove.
  2. Click **Delete**.

- *To configure the postmaster address*: Enter the email address in the **Postmaster address** text box.
- After you have made any necessary changes you can:
  - Click **Apply** to save your changes.
  - Click **Cancel** to discard your changes.
  - Select the *Support* (page 117), *SNMP* (page 117) or *Syslog* (page 118) tab to configure additional options.

Support

- To activate support alerts, select the **Appliance support alerts** check box.
- For **Critical alerts**, provide the **Name** and **Email** of the person who should receive these messages.
- 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.

SNMP

- If your appliance is part of a cluster, from the **Appliance** drop-down list, select which system in the cluster you want to configure.
- To enable the appliance to be monitored using the simple network monitoring protocol (SNMP), select the **Enable SNMP Monitoring** check box.
- To add a new community string/network that is allowed to monitor the appliance, go the **Enable SNMP Monitoring** panel of the **SNMP** tab, then:

  1. In the **Community String** text box, enter the community string.
  2. In the **Network** text box, enter the network .
  3. Click **Add**.

  The new community string/network is displayed in the list.

  Note: The additions are saved only after you click **Apply**. The changes can be reverted by clicking **Cancel**.

- To remove one or more community strings/networks from the list of those allowed to monitor the appliance, go the **Enable SNMP Monitoring** panel of the **SNMP** tab, then:

  1. Select the check box next to the community strings/networks that you want to remove.
  2. Click **Delete**.

  The deleted community strings/networks is no longer displayed in the list.

  Note: The changes are saved only after you click **Apply**. The changes can be reverted by clicking **Cancel**.

- **Note:** To edit information about a community string/host, it is necessary to delete it, then add a new entry with the updated information.

- Select the **Enable SNMP Notifications/Traps** to allow specified hosts or community strings to be notified of alerts via SNMP.
- To add a new community string/host that will be notified of appliance alerts via SNMP, go the **Enable SNMP Notifications / Traps** panel of the **SNMP** tab, then:

  1. In the **Community String** text box, enter the community string.
  2. In the **Hostname/IP** text box, enter the hostname or IP.
  3. From the **Version** drop-down list, select the SNMP version.
  4. Click **Add**.

  The new community string/host is displayed in the list.

  Note: The additions are saved only after you click **Apply**. The changes can be reverted by clicking **Cancel**.

- To remove one or more community strings/hosts from the list of those that will be notified of appliance alerts via SNMP, go the **Enable SNMP Monitoring** panel of the **SNMP** tab, then:

  1. Select the check box next to the community strings/hosts that you want to remove.
  2. Click **Delete**.

  The deleted community strings/hosts are no longer displayed in the list.

  Note: The changes are saved only after you click **Apply**. The changes can be reverted by clicking **Cancel**.

- **Note:** To edit information about a community string/host, it is necessary to delete it, and then add a new entry with the updated information.

- To ensure that the Sophos Email Appliance can be integrated with your SNMP monitoring infrastructure, it is recommended that you download the appliance's management information base (MIB). To download the appliance's MIB, click the **Download MIB** button. Note that the MIB references hardware sensors that may not be available in all hardware configurations. An "unknown" SystemStatus value will be returned for any SNMP value that references a sensor that is not available in your hardware profile.
- After you have made any necessary changes you can:
  - Click **Apply** to save your changes.
  - Click **Cancel** to discard your changes.
  - Select the *Email* (page 117), *Support* (page 117) or *Support* (page 117) tab to configure additional options.

Syslog

The appliance can send log information to a syslog receiver for auditing and analysis. For detailed information about the syslog capabilities of the Sophos Email Appliance, see the *Sophos Email Appliance syslog capabilities* (page 119).

Note: If you are configuring appliances that are part of a cluster, each appliance's syslog configuration must be appropriate for its specific location in your network.

To enable the appliance's syslog facility:

1. Select the **Enable Syslog** check box.
2. In the **Hostname/IP** text box, enter the address of the syslog receiver to which the appliance will send logs.

   Note: If the syslog receiver becomes unavailable to the appliance, some log information may be dropped before the receiver becomes available again. The amount of information dropped depends on the duration that the receiver is unavailable, and on the current mail volume. However, all logs will continue to be available in the appliance's automatic backups, if these have been configured.

3. In the **Port** text box, enter the port number that your syslog receiver uses. If there is a firewall between the appliance and the syslog receiver, ensure outbound access from the appliance to the syslog server.
4. Select a **Protocol** option button to select whether the appliance will send syslog data using UDP (faster, but delivery is not guaranteed) or TCP (reliable delivery).
5. Select the check box next to each log that you want to record:

   Note: The **Administrator audit log** cannot be disabled. It provides information about login and authorization attempts.

   - **System status log**: Provides information about system status events.
   - **SPX notice log**: Provides a record of failed SPX password login, change, and recovery attempts by users of the SPX portal. This log is only relevant if you have SPX encryption enabled, and you are using the user registration method of password management. For more information, see “Choosing an SPX Password Method”.
   - **Message policy log**: Provides a log of all message policy events, as well as any additional values you have set by configuring *Additional Message Actions* (page 196).
   - **Mail transfer agent log**: Provides information about email messages that the appliance has sent or received.

After you have made any necessary changes you can:

- Click **Apply** to save your changes.
- Click **Cancel** to discard your changes.
- Select the *Email* (page 117), *Support* (page 117) or *SNMP* (page 117) tab to configure additional options.

Sophos Email Appliance syslog capabilities

Information about the syslog capabilities of the Sophos Email Appliance.

Syslog is a tool for sending log messages from a client system to a server or receiver. The logs can be used for auditing and analysis. Syslog uses a standard protocol, described by RFC 5424. The Sophos Email Appliance can be configured to send log messages to a syslog receiver, where the information can be collected and analyzed.

The Email Appliance can produce several kinds of logs. Each has an associated category that indicates what facility generated the log information, and a value that indicates the severity of the log message. The following table lists the appliance's log types, and associated information:

Log	Facility	Facility Code	Severity	Severity Code	Notes
administrator audit	auth	4	Notice: normal but significant condition	5	Always logged when syslog is enabled. Provides information about system changes, authorizations and similar events.
system status	auth	4	Notice: normal but significant condition	5	Optional. Provides information about system events such as reboots and upgrades.
message policy	mail	2	Informational: informational messages	6	Optional. Provides information about policy events that the appliance has been configured to log.
mail transfer agent	mail	2	Informational: informational messages	6	Optional. Provides detail information about email messages sent or received by the appliance.

The following sections provide a number of examples of log entries for each type of available log. These can be used to aid in configuring analysis and auditing software.

Administrator audit log examples

- A log entry showing a successful login attempt:

```
Jan 11 22:34:14 somehost admin-ui[24874]: [NOTICE] [192.0.2.143] admin/en:
  logged in with tz=America/Vancouver window=1280x811
  screen=1280x1024 ua=Mozilla/5.0 (Windows; U;Windows NT 5.1;
  en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
```

- A log entry showing internal variable changes:

```
Jan 11 03:36:54 somehost3 admin-ui[1652]: [NOTICE] [192.0.2.96] admin/en:
  config: option 'proxy_enabled' set to '1' (was '0')
```

- A log entry showing a policy being updated to a new setting:

```
Jan 11 03:57:11 somehost admin-ui[1200]: [NOTICE] [192.0.2.96] admin/en:
  policy: outbound virus action set to discard (was quarantine)
```

- A log entry showing an administrator performing a log search:

```
Jan 11 06:33:34 somehost admin-ui[27250]: [NOTICE] [192.0.2.96] admin/en:
  Log search: atime='2010-01-09T08:00:00' count='1000' sort='-time'
  timezone='America/Vancouver' to='tlsuser1@somehost2.example'
  ztime='2010-01-11T08:00:00'
```

- Logging out of the appliance's admin interface:

```
Jan 11 22:32:39 esa10 admin-ui[24529]: [NOTICE] [192.0.2.125]
  admin/en: logged out
```

System status log example

- This example shows a selection of typical events that will be recorded in the system status log:

```
Jan 11 03:35:15 somehost3 shutdown: start: system starting up
Jan 11 03:38:08 somehost3 sophox-register[3350]: Updated license.
Jan 11 03:38:18 somehost3 sea-upgrade[5274]: factory_probe: no updates available
    on http://tankrepo/repo/esa/projects/trident/freebsd/
Jan 11 03:46:43 somehost3 shutdown: reboot: UI: register/update
Jan 11 03:47:43 somehost3 shutdown: reboot by root: UI: register/update
Jan 11 22:21:27 somehost3 data-update: appliance failed to retrieve data
  updates from Sophos
Jan 11 21:51:10 somehost3 sea-upgrade[99777]: download: no updates available on
  http://esa.sophos.com/es4000/delta
Jan 11 04:29:39 somehost3 appliance-status[20828]: appliance status changed to
  error from ok <System fans>
Jan 11 04:38:44 somehost3 appliance-status[26639]: appliance status changed to
  ok from warn
Jan 11 05:26:28 somehost3 sea-upgrade[79970]: download: found update 1.127
Jan 11 05:26:28 somehost3 sea-upgrade[79970]: starting download:
  http://127.0.0.1/1/120/tank-1.127-n.tar.gz
Jan 11 05:26:28 somehost3 sea-upgrade[79970]: finished download:
  http://127.0.0.1/1/120/tank-1.127-n.tar.gz
```

Message policy log examples

- A simple example of a message policy log entry, showing a message being quarantined:

```
Jan 11 20:26:14 q=4B4B8966_98410_2_1 f=<junk@example.com>:
  t=<tester2@host.example> Rule=Quarantine type=Legit b=ok action=quarantine
  inbound S=one fur= r=192.0.2.107 tm=0.22 a=d/eom
```

- A more complex entry, showing a spam message being processed:

```
Jan 11 20:11:36 q=4B4B85F4_90724_2_1 f=<junk@example.com>:
  t=<tester1@host.example> b=ok action=deliver h=BASE64_ENC_TEXT
  h=DATE_IN_PAST_96_XX h=FROM_NAME_ONE_WORD h=MIME_TEXT_ONLY_MP_MIXED
  h=SUPERLONG_LINE h=BODY_SIZE_10000_PLUS h=TO_NO_NAME h=__BAT_BOUNDARY
  h=__CT h=__CTYPE_HAS_BOUNDARY h=__CTYPE_MULTIPART
  h=__CTYPE_MULTIPART_MIXED h=__HAS_MSGID h=__MIME_TEXT_ONLY
  h=__MIME_VERSION h=__MOZILLA_MSGID h=__SANE_MSGID h=__STOCK_PHRASE_6
  h=__SXL_SIG_TIMEOUT h=__TO_MALFORMED_2 h=__USER_AGENT
  inbound S=?q?This_should_exceed p=0.112 fur= r=192.0.2.107 tm=4.11 a=a/eom
```

A mail transfer agent log example

- This is a selection from a the mail transfer log, showing an email message being received:

```
Jan 11 22:06:52 somehost3 postfix/smtpd[26327]: connect from
  test.example[192.0.2.107]
Jan 11 22:06:56 somehost3 postfix/smtpd[26327]: 3A3D12FE3F1C_B4BA100F:
  client=test.example[192.0.2.107]
Jan 11 22:06:56 somehost3 postfix/cleanup[26434]: 3A3D12FE3F1C_B4BA100F:
  message-id=<200106290254.f5T2sEO19584@smtp1.example.com>
Jan 11 22:06:56 somehost3 postfix/qmgr[2937]: 3A3D12FE3F1C_B4BA100F:
  from=<user@test.example>, size=16031, nrcpt=1 (queue active)
Jan 11 22:06:56 somehost3 postfix/smtpd[26327]: disconnect from
            test.example[192.0.2.107]
```

Syslog Monitoring

Syslog is a standard for forwarding log messages in an IP network.

Syslog is a client/server protocol. Logging information is sent as text-based messages from a client system to a syslog receiver or server. Log messages from several clients can be consolidated and analyzed by a syslog server. Syslog messages can be sent via UDP and/or TCP.

Backup

On the **Configuration ➤ System ➤ Backup** page, you can configure the Email Appliance to automatically upload system configuration data, log data, and quarantined email to an FTP site at regular intervals as backup.

Note: If you are running multiple appliances in a cluster, you can also manage configuration backups for other appliances in that cluster.

Ensure that the Email Appliance has access to a secure FTP location before applying the backup settings. Alternatively, you can click a **Download** button to immediately download a .zip file containing Email Appliance configuration data.

Important: Configuration backups are strongly recommended as a means of saving data about your Email Appliance settings. If configuration data has been backed up, Sophos Technical Support can use it to preserve your settings in the event of a hardware failure, or to transfer settings from one Email Appliance to another. This feature should not, however, be mistaken for a "restore" feature because it does not back up log files or quarantined messages. It is advised that you regularly back up configuration data using one of the two options described below.

- To configure the upload location for automated upload (FTP):

  1. Fill in the text boxes to configure access to the backup host:

     - **FTP location**: Enter the hostname or IP address for the system to which the data will be copied.
     - **FTP port**: Enter the port to connect to on the FTP server. The default is port 21.
     - **FTP path (optional)**: Enter the directory location to which the data will be copied. If no location is given, data will be copied to the default directory on the FTP server.
     - **Username (optional)**: Enter the username that will be used to access the system to which the data will be copied.
     - **Password (optional)**: Enter the user account password required to access the system to which the data will be copied.

2. Click **Verify** to ensure that the values entered in the preceding text boxes are valid.
3. Under **Configuration backup**, select backup options for configuration data:
   - **System configuration data**: Uploads all configurable settings and Email Appliance resources. Select the frequency with which the data will be backed up from the drop-down list: **Daily at Midnight**, **Weekly on Friday at midnight**, or **Monthly on the 1st at midnight**.

     Note: If you are running multiple appliances in a cluster, click the **Configure** button to select the individual appliances in that cluster for which configuration data will be backed up.

   - **Expired quarantined messages**: Uploads all quarantined spam messages. Messages are expired from the quarantine after 30 days, or when the disk becomes full.
4. In the **Data backup** section, select the desired check boxes to configure what data will be backed up:
   - **Quarantined messages**: Uploads all quarantined spam messages. Messages are expired from the quarantine after 30 days, or when the disk becomes full.
   - **System logs**: Uploads data from the message logs. Logs expire after 30 days, or when the disk becomes full.
5. From the corresponding drop-down list, select the frequency at which you want the automated upload to occur.
6. Click **Apply**.

- To manually download configuration data:

  Click **Download**, and use your web browser's download file feature to specify the download location. There is a slight delay as the configuration data is copied and archived into a file for download.

Directory Services

Use the **Configuration ➤ System ➤ Directory Services** page to configure access to your organization's directory server(s) so that the Sophos Email Appliance can use directory services data for user authentication, email aliases, and to apply mail-filtering policies to directory services user groups.

Configure directory services by using the wizard to create a profile for each directory server in your organization. The Email Appliance can integrate simultaneously with various LDAP implementations. For example, you could be using multiple Active Directory servers, or an Active Directory server and a Novell eDirectory server.

Important: If you are configuring your Email Appliance to integrate with multiple directory servers, and you have enabled SMTP authentication on the **Configuration ➤ Policy ➤ SMTP Authentication** page, you can only perform SMTP authentication for one of the configured directory servers. For more information, see “SMTP Authentication”.

Directory services settings can only be automatically detected for Active Directory servers. For all other LDAP servers, some manual configuration is required.

- *To launch the Directory Services wizard*, Click **Add**. Each profile you create is added to the list on the **System: Directory Services** page.
- *To manually synchronize the data on your directory server with your Email Appliance*, click **Synchronize Now**.
- *To delete a directory server*, select the check box next to the server entry, and click **Delete**.

  Important: Deleting a directory server will affect directory services groups as well as any Email Appliance settings that use directory services. Before deleting a server, it is recommended that you consider the consequences of that action. For more information about deleting any or all directory servers, see *Removing Directory Servers* (page 122).

Removing Directory Servers

Deleting a directory server will affect directory services groups as well as Email Appliance settings that use directory services. Before deleting a server, it is recommended that you review these sections on removal to understand the consequences of this action.

The results differ, depending on whether you remove one or more directory servers or all of the directory servers.

Removing *Some* Directory Servers

If you remove one or more (but not all) directory servers, the following will occur:

- If there are any directory services groups based on this directory server that are currently referenced by the appliance's policy, they will be migrated to manual groups and those policy references will be updated.
- Recipient validation will no longer include addresses from this directory server.
- If directory services alias maps are enabled, they will no longer contain aliases from this directory server.
- If authentication for the End User Web Quarantine is based on directory services, users from this directory server will no longer be able to log in.
- If SMTP authentication is being performed this directory server, SMTP authentication will be disabled.

Removing *All* Directory Servers

If you remove all directory servers, the following will occur:

- If there are any directory services groups currently referenced by the appliance's policy, they will be migrated to manual groups and those policy references will be updated.
- If directory services are used for recipient validation, this mode of validation will be disabled. Recipient validation will revert to using the SMTP look-ahead option.
- If directory services alias maps are enabled, they will be disabled.
- If authentication for the End User Web Quarantine is based on directory services, it will be disabled.
- If SMTP authentication is enabled, it will be disabled.

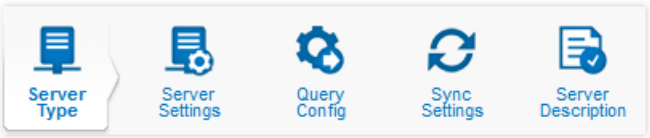
Directory Services Wizard

Use the Directory Services wizard to configure your directory server(s).

Although the wizard simplifies the process of configuring integration between the Sophos Email Appliance and directory services, some manual setup may be necessary. The wizard allows you to proceed to the next step, even if settings cannot be verified and if queries fail. Once you have completed all the steps in the wizard, you may need to return to one or more pages to correct the settings. It is important to ensure the appropriate settings to avoid unexpected results.

The five main steps of the wizard are described in the sections that follow.

Server Type



1. Select one of the following directory services types:
   - **Auto-detect Active Directory settings**:
     1. In the **Server** text box, enter the hostname or IP address of your organization's directory services server.
     2. In the **Username** text box, enter the username (if required) to access the directory services server.
     3. In the **Password** text box, enter that user's password (if required).

        Note: Detecting the directory services settings fails if the directory services server requires a username and password, but they are not provided.

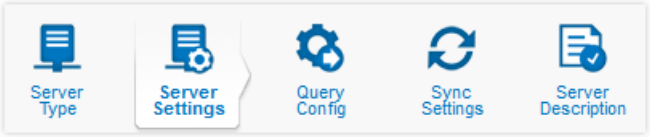
     4. Click **Detect Settings**. The progress of the auto-detection process is displayed on the right. If successful, the appliance will connect to the server, detect the settings, and then indicate that verification of the settings is complete.

- Or, select **Choose from a list of directory server sample profiles**, and then select your LDAP implementation from the list. This is not a complete list of LDAP implementations. It is intended to provide some examples of popular LDAP versions. If your version is not shown, choose the third option, and configure your settings manually.
- Or, select **Configure directory server settings manually** to proceed through the wizard and configure all of the settings yourself.

Note: If you choose the **Lotus Domino** sample profile, follow the Groups by Membership schema. If you choose the **Lotus (Groups by OU)** sample profile, follow the Groups by Organizational Unit schema.

2. Click **Next**.

Server Settings



Depending on the option you selected in the first step of the wizard, some or all of the settings may already be displayed on the **Server Settings** page. These values are only intended as a guide, and you must adjust them to match your directory server's requirements.

Note: If you are using an anonymous directory services server, it is not necessary to enter a distinguished name (DN) or password.

1. Under **Directory Services Settings**, review/set the following options:
   1. In the **Server** text box, enter the fully qualified hostname of the server used for directory services look-ups.

      Alternatively, enter a comma-separated list of failover servers.The first in the list should be the primary server. If the primary server fails, the appliance will attempt to use the other specified servers in the order that they are named.

      Important: If you specify multiple servers, you must ensure that each of the servers uses an indentical directory structure. Failure to do so could result in unexpected behavior.

   2. In the **Port** text box, enter the port number of the server used for directory services look-ups. The default port is 389, or port 636 for LDAPS. If the Active Directory global catalog (GC) is used, the port is 3268, or 3269 for a secure connection.
   3. From the **Protocol** drop-down list, select the type of LDAP used for user authentication. The default is standard **LDAP**, but LDAPS encrypts all communication between the appliance and the LDAP or Active Directory server with Secure Sockets Layer (SSL).

      Additional configuration is required for LDAPS. For example, in Active Directory, you must install a valid certificate to enable LDAPS. For more information, see the following Microsoft articles: "How to enable LDAP over SSL with a third-party certification authority," "Requirements for domain controller certificates from a third-party certification authority," and "Advanced Certificate Enrollment and Management."
   4. In the **DN to authenticate** text box, enter the distinguished name (DN) used to connect to the directory services server for authentication purposes (if required). Here are some examples of possible DN formats:

      - `CN=Administrator,CN=Users,DC=Server`
      - `DOMAIN\username` (Active Directory)
      - `user1.users.server` (Novell eDirectory)

      Note: Enter a DN appropriate for the directory profile you have selected.

   5. In the **Password** text box, enter the password for directory services look-ups (if required).
   6. In the **Base DN for users/groups** text box, enter the top directory services node from which searches are performed.

7. In the **Account attribute** text box, enter the directory services object attribute that is queried when logging in to the End User Web Quarantine.
8. In the **Email attribute** text box, enter the object attribute for email addresses in directory services.
9. In the **Email alias attribute** text box, enter the object attribute for proxy addresses in directory services.
10. In the **Group name attribute** text box, enter the directory services object attribute that specifies the group name for a group entry.

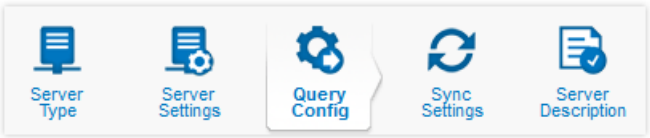
2. Click **Verify**.

   The appliance verifies that all of the values you entered are valid. If verification is successful, a green check mark is displayed beside each setting in the *Verify Settings* (page 207) dialog box.

   Note: If you specified multiple servers in the **Server** text box, a successful result is returned if any one of the servers responds. Each server is *not* verified separately.

3. If all settings are verified, click **OK**. Otherwise, correct any invalid settings, and repeat the verification.
4. Click **Next**.
   The queries run automatically, and the results are displayed to the right of each text box. Successful queries are indicated by a green check mark.

Query Config



The **Directory Services Queries** page allows you to edit directory services queries. Although queries are auto-generated by the Directory Services wizard for some LDAP implementations, these values are only intended as guidelines; you must adjust them to match your directory server's requirements.

The first time you access this page, the queries run automatically. If you go to a previous page and then return to the **Query Config** page, or if you edit the queries, you must click **Run Queries** to run them again. The icon next to each query indicates the result.

1. Edit existing queries or enter custom queries in the following text boxes:

   Note: To test the %%USERNAME%% or %%GROUP_DN%% associated with a specific query, enter it in **Verify Queries** section at the bottom of this wizard page.

   - **Valid Recipients**: Retrieve a list of every valid email address. This query uses the recipient validation method specified on the **Configuration ➤ Policy ➤ Filtering Options** page. See “Filtering Options” for a description of the recipient validation options.

     This query uses "Administrator" by default, unless you enter a different name in the query, or in the **Test %%USERNAME%%** text box in the **Verify Queries** section.

     Ensure that this query retrieves all valid email addresses to prevent valid messages from being rejected.
   - **Aliases**: Return a list of aliases and their addresses. If you have users with email aliases, this ensures that the mapping of one address to another is respected, so that mail is delivered to the correct address, recipients can log in to the End User Web Quarantine, and per-user settings are applied.
   - **Retrieve user**: Retrieve the Distinguished Name (DN) of the end user to use for End User Web Quarantine authentication. Testing a specific %%USERNAME%% in the **Verify Queries** section returns 1 result if it is successful and 0 results if it fails.

     Important: It is not necessary to provide this query if you have enabled **Via downstream SMTP look-ahead** for recipient validation. For more about this control, see “Filtering Options.” If, instead, you have enabled **Via directory services** for recipient validation, and this query is not specified correctly, the appliance will quietly reject mail.

- **User groups**: Retrieve a list of groups, which can then be included or excluded from certain policies.
- **Members of a group**: Retrieve a list of email addresses for users who are members of a specified group (%%GROUP_DN%%).
- **SMTP Authentication**: Retrieve the Distinguished Name (DN) of the end user that is required for SMTP authentication. Testing a specific %%USERNAME%% in the **Verify Queries** section returns 1 result if it is successful and 0 results if it fails.

  This query uses "Administrator" by default, unless you enter a different name in the query, or in the **Test %%USERNAME%%** text box in the **Verify Queries** section.

2. [Optional] Completely empty a query to disable that query on the appliance.
3. [Optional] Test individual queries by entering a specific %%USERNAME%% or %%GROUP_DN%% value from a query string into one of the text boxes described below. The resulting matches are displayed to the right of the query itself.

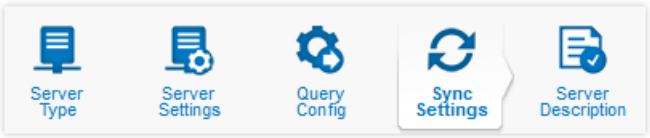
   - **Test %%USERNAME%%**: Enter a valid directory services username to see if the user is affected by the Retrieve user or SMTP authentication query.
   - **Test %%GROUP_DN%%**: Enter the distinguished name (DN) of a group that is used in the “Members of a group” query to retrieve a complete list of its members.

4. After you have finished entering queries, you can:

   - Click **Reset** to restore the original queries that were generated, based on the entries you supplied on a previous page of the wizard.
   - Click **Run Queries** to test queries. The number of results each query returns is displayed. This can be compared to the number of results you expect your directory services server to return. If no (0) results are returned, you should carefully check that the query is valid (unless you expected no results).
   - Hover your mouse pointer over the text of the status result to see a tool tip. The tool tip indicates reasons for warnings (indicated with a yellow exclamation mark icon) and errors (indicated with a red x-mark icon).
   - Click the status result of a valid query to download a text file containing the query results. The file consists of a header that contains the actual query (not variables), followed by one result per line. Each result has semicolon-separated fields, and each field has comma-separated values.
   - Copy a group DN from the query results file and use it to run tests on the **Query Config** page.

5. Click **Next**.

Sync Settings



1. From the **Schedule** drop-down list, select how often you want the appliance to automatically synchronize its data with directory services.

   Note:

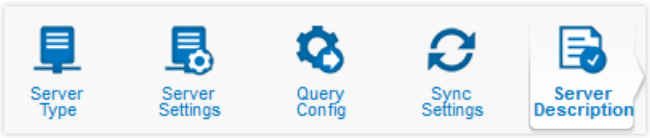
   If new users are added in directory services, and the **Via directory services** option is selected on the **Configuration ➤ Policy ➤ Filtering Options** page, then mail for the new users is rejected until a synchronization transfers the user data to the Email Appliance. It is therefore advised that you set the synchronization interval to a short time period, such as one hour, to reduce the number of rejected messages.

   The recommended alternative is **Via downstream SMTP look-ahead**, which is also set on the **Configuration ➤ Policy ➤ Filtering Options** page. See “Filtering Options” for a description of the recipient validation options. Although it is unlikely, there may be a delay of up to three hours before the Email Appliance will accept mail for a newly added valid email address. This results because the Email Appliance's mail transfer agent (MTA) caches the list of invalid recipients.

Once directory services integration is configured, synchronizations are performed regularly as set in the synchronization interval option. If the synchronization of a user group fails three or more times consecutively, then the group will disappear from the groups listed in the *List Selector* (page 202) dialog box. However, once a synchronization is performed successfully, the group will reappear in the list.

2. Click **Next**.

Server Description



1. In the **Directory Services name** text box, enter a meaningful name for your directory server.
2. Click **Save**. The server profile you added is displayed in the list of servers.

Directory Services Group Schemas

To retrieve the correct group information when you create queries, you must follow the directory services group schema that your organization has implemented (according to its business or network infrastructure needs). This is an overview of the two most common schemas, illustrating group layout.

Note: If you use Lotus Domino, and your organization follows the Groups by Membership schema, choose the **Lotus Domino** sample profile on the **Server type** page of the Directory Services wizard (**Configuration ➤ System ➤ Directory Services ➤ Add**). If you use Lotus Domino, and your organization follows the Groups by Organizational Unit schema, choose the **Lotus (Groups by OU)** sample profile.

Groups by Membership

This schema defines group membership by entries within user records. This schema is very common; it is often used in Active Directory and other common directory service deployments, such as Novell eDirectory. (However, the specific attributes and exact structure of your schema may be different from this example.)

The following is an example of an Active Directory deployment schema.

- o=Acme
  - ou=Users
    - cn=Bob_Bobson
    - cn=Jane_Johnson
    - cn=Tim_Thompson
      - memberOf=cn=Testers,ou=Groups,o=Acme
      - memberOf=cn=Developers,ou=Groups,o=Acme
      - mail=tim.thompson@example.com
    - cn=Dodd_Dobson
      - memberOf=cn=Testers,ou=Groups,o=Acme
      - mail=dodd.dobson@example.com
  - ou=Groups
    - cn=Managers

- cn=Developers
  - cn=Tim_Thompson,ou=Users,o=Acme
- cn=Testers
  - member=cn=Tim_Thompson,ou=Users,o=Acme
  - member=cn=Dodd_Dobson,ou=Users,o=Acme

In this schema, membership is primarily defined by entries in user records. (For example, the `memberOf` attribute contains the Distinguished Names (DN) of the groups to which a user belongs). In Active Directory, a group's records also contain cross-references to its members .For example, each `member` attribute in a group record contains the DN of a user who is a member of the group.

Note: Not all schemas have two-way references. Using `memberOf` attributes in user records is sufficient to correctly define group membership.

To retrieve the records of all members of a group, the Email Appliance begins queries at the root of the directory tree (in this case, by setting the base DN to `o=Acme`). For example, a query that retrieves the email addresses of members of the Testers group would retrieve the values of the `mail` attribute of every user who has a `memberOf` attribute with the following value: `dn=cn=Testers,ou=Groups,o=Acme`. The returned list of email addresses can be used to apply group policies on the **Configuration ➤ Accounts ➤ User Groups** page.

Groups by Organizational Unit

This schema defines group membership by a user's location within the directory tree. This schema is less common. (However, it is occasionally used in Lotus Domino and other customizable directory service deployments.)

The following is an example of a Lotus Domino deployment schema.

- o=Acme
  - ou=Europe
  - ou=North America
    - ou=Toronto
      - cn=Testers
        - cn=Tim_Thompson
          - mail=tim.thompson@example.com
    - ou=Vancouver
      - cn=Managers
        - cn=Bob_Bobson
          - mail=bob.bobson@example.com
      - cn=Developers
        - cn=Jane_Johnson

- `mail=jane.johnson@example.com`

- `cn=Testers`
  - `cn=Dodd_Dobson`
    - `mail=dodd.dobson@example.com`

In this schema, users are categorized by Organizational Units (OUs), corresponding to regional domains, that is, company branches and cities; user records are located within more specific OUs. The nested OUs, in turn, contain multiple levels of CNs, corresponding to groups of users and individual users. Each CN corresponding to a user should have an attribute that indicates his email address; this is typically the `mail` attribute.

In this schema, the Email Appliance must begin its queries at the location of the OU/group itself, since it is impossible to retrieve only the users within that OU/group using a query with a base DN set to the root of the directory. (In this schema, there are no cross-reference attributes such as `memberOf`.) Thus, the base DN must be set to the DN of the group, and the members of the OU/group must be all located within the group.

For example, a query that requests the email address attribute of every user who is a member of the North America group would have the base DN `ou=North America,o=Acme`, and it would retrieve the email addresses of all users within it (Tim, Bob, Jane and Dodd). However, a query that requests the email addresses of every user in the Toronto Testers group would have the base DN `cn=Testers,ou=Toronto,ou=North America,o=Acme`, and it would retrieve the email addresses of all users within it (in this case, only Tim Thompson's email address).

Note: In this schema users will only be members of their OU/group and any parents of that OU/group. For example, Dodd Dobson is a member of the Vancouver Testers group; he is also implicitly a member of the Vancouver and North America groups.

Similarly to the groups-by-membership schema, the returned list of email addresses can be used to apply group policies on the **Configuration ➤ Accounts ➤ User Groups** page.

Certificates

Use the **Configuration ➤ System ➤ Certificates** page to manage certificates and certificate authorities. These are used by the Email Appliance to manage encryption for the **Administrative User Interface**, the **End User Web Quarantine**, **DKIM**, and **Email Encryption**.

To fully configure certificates, it may be necessary to first add or configure a trusted certificate authority.

DKIM Settings

DomainKeys Identified Mail (DKIM) is an authentication framework used to sign and validate a message based on the domain of the sender. To configure DKIM to cryptographically sign outgoing mail, specify a private RSA key (in ASCII armor) and a "selector" string. For domains that you want to sign mail for, you also need to publish the public portion of the RSA key along with the selector in the DNS for those domains.

Adding a certificate to the Email Appliance

To add a certificate to the Email Appliance:

- On the **Certificates** page, click **Add**.

  The **Add Certificate** dialog box is displayed.
- Either:
  - Select *Upload Certificate* (page 130) if you already have a certificate pair.

- Select *Initiating a Certificate Signing Request* (page 130) if you need to obtain a certificate.

Upload Certificate

If you selected **Upload existing certificate and private key** in the **Add Certificate** dialog box, the **Upload Certificate** dialog box is displayed. Use this dialog box to add a certificate provided by a trusted certificate authority to make the certificate available for use on the appliance.

Note: A certificate of any size can be used, but it must be in **PEM** or **PKCS#12** format.

To add a certificate:

1. In the **Description** text box, enter a short description of the certificate. This is the name that will appear in the **Certificates** list.
2. Choose one of the following options:
   - Select **Paste certificate text** to copy and paste the certificate.
   - Select **Import certificate file** to import the certificate from a file.
3. Click **Next** to finish.

The certificate is displayed in the **Certificates** list.

Note: If you need to add an intermediate certificate, it should have a format similar to:

```
-----BEGIN RSA PRIVATE KEY-----
  <The private key>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
  <The SEA's server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
  <The intermediate certificate>
-----END CERTIFICATE-----
```

The SEA's server certificate can be downloaded by clicking on the certificate name, then clicking **Download**.

Initiating a Certificate Signing Request

The **Initiate CSR** dialog box is displayed if you selected **Initiate Certificate Signing Request** in the **Add Certificate** dialog box.

To generate a CSR:

1. Enter a **Description**. This is the name that will appear in the list of certificates.
2. In the **Hostname/Domain** text box, enter the hostname and domain of your server,

   Note: The hostname/domain that is presented to external hosts must exactly match the hostname/domain associated with the certificate.

3. In the **Organization name** text box, enter the name of your company or organization,
4. In the **City** text box, enter the name of your city ,
5. In the **State or Province** text box, enter the name of your state or province,

   Note: The state or province name must *not* be abbreviated.

6. From the **Country** drop-down list, select your country.
7. Click **Next** to finish generating the *Certificate Request* (page 131)

The Email Appliance will generate the Certificate Signing Request.

Certificate Request

The **Certificate Request** dialog box is displayed if you proceed after entering the required information in the *Initiating a Certificate Signing Request* (page 130) dialog box. It displays the CSR that the Email Appliance has generated for your certificate request.

To complete the CSR:

1. Save the CSR to your computer. Either:
   - Click **Download** to save the CSR:
   - Cut and paste the displayed CSR and save it as a text file.

   Important: The CSR's exact formatting must be preserved. Because of this, it is recommended that you use a text editor such as Notepad, and not a word processor or similar program to save the CSR.

2. Click **Close**.

   The CSR is now displayed in the **Certificates** section on the **Certificates** page. "[Pending CSR - upload certificate]" is displayed next to its description until you have completed the CSR process.

   You will now need to use the saved CSR to *Obtaining a Certificate for the Email Appliance* (page 134). After obtaining this from a certificate signing authority, you will need to *Complete CSR* (page 193).

Certificate Details

The **Certificate Details** dialog box is displayed if you click a certificate description in the **Certificates** section on the **Configuration ➤ System ➤ Certificates** page. It shows detailed information about the certificate, and also allows you to download the certificate, or the certificate and its private key.

1. To download the certificate, click **Download**.

   Your browser will prompt you to save the certificate on your local computer.

2. To back up a certificate and its corresponding private key, click **Backup**. Your browser will prompt you to save the certificate/private key pair on your workstation.

   Caution: It is important to not share this file with anyone. It contains a private key that can be used to allow anyone to masquerade as your organization.

Managing Existing Certificates

Existing certificates may be configured for the **Administrative User Interface**, **End User Web Quarantine** and **Email Encryption** roles.

After adding certificates to the Email Appliance, you can configure the certificates for different roles on the Email Appliance. A given role can only use one certificate at a time, but a particular certificate may be used for more than one role.

If you want to use a different certificate for the **Administrative User Interface**, the **End User Web Quarantine**, or for **Email Encryption**:

1. Navigate to the **Configuration ➤ System ➤ Certificates** page.
2. For clustered deployments, select the system you want to configure from the **Appliance** drop-down list.
3. Select the Email Appliance role for which you wish to use the certificate.
4. Click **Apply**. The certificate will now be used for the selected role.

Note: It is *not* possible to remove the self-signed certificate that is supplied with the Email Appliance.

Deleting certificates from the Email Appliance

1. On the **Certificates** page, configure the certificate so that it is not used for the **Administrative User Interface**, the **End User Web Quarantine**, or for **Email Encryption**.
2. Select the check box or check boxes in the rightmost column to select the certificates you want to delete.
3. Click **Delete**.

   Note: It is *not* possible to delete the Email Appliance's self signed certificate.

Configuring Trusted Certificate Authorities

Use the **Trusted Certificate Authorities** dialog box to view and manage your list of certificate authorities.

To manage trusted certificate authorities:

- In the **Trusted Certificate Authorities** section of the **Certificates** page, click **Configure**.
  The **Trusted Certificate Authorities** dialog box is displayed.

Trusted Certificate Authorities

The **Trusted Certificate Authorities** dialog box is displayed if you click the **Certificates** page.

To add a new trusted certificate authority:

1. On the **Locally managed** tab, click **Add**. The *Add Certificate Authorities* (page 193) dialog box is displayed.

   After you have added the trusted certificate authority, it will be displayed in the list of trusted certificate authorities on the **Locally Managed** tab.

   Note: The **Sophos managed** tab displays a list of certificate authorities managed by Sophos. This list cannot be edited.

2. Optionally, to delete a certificate authority from the **Locally managed** list, select the CA, then click **Delete**.
3. Click **Close**.

Add Certificate Authorities

The **Add Certificate Authorities** dialog box is displayed if you click **Add** in the **Locally managed** tab on the *Trusted Certificate Authorities* (page 206) dialog box.

To add a certificate authority:

1. Type a **Description**. This is the name that will be displayed in list of trusted certificate authorities.
2. In the **Paste certificate text** text box, paste the text of a valid certificate
3. Alternatively, upload a **valid certificate** by selecting **Import certificate file**, then clicking **Browse**.
4. Click **OK**.

   Note: A certificate of any size can be used, provided it is in **PEM** or **PKCS#12** format, and is of a **cipher type** supported by the Email Appliance.

Certificates and Certificate Authorities

Certificates

Certificates used by the appliance are public key certificates known as X.509 certificates. These encryption keys are associated with a specific identity or organization, and they allow the identity of the certificate holder to be verified. Identity verification

is an important component of ensuring secure communication. Without it, it is possible for even encrypted communication to be redirected or compromised by an untrustworthy third party.

To help prevent this, the Email Appliance can:

- Use certificates signed by an agency known as a trusted certificate authority (CA) to present a verifiable identity to other hosts. This helps ensure secure access to the Email Appliance's Administrative User Interface and End User Web Quarantine, and enables hosts that support *Transport Layer Security (TLS) Email Encryption* (page 73) to confirm the identity of the Email Appliance when exchanging encrypted email with it.
- Be configured to trust additional certificate authorities, by obtaining identifying certificates associated with them. This allows you to expand the range of identities that you would like the Email Appliance to communicate with.

  Note: The Email Appliance uses the certificates associated with CA's only to verify the identify of each CA. While similar to the certificates presented by the Email Appliance to other hosts, they are managed separately, and you should distinguish between them.

The Email Appliance can have up to four certificates at one time, including the default self-signed certificate (see below). Different certificates can be used for different roles, including the Administrative User Interface, the End User Web Quarantine, and TLS email encryption.

Certificates include information such as the hostname they are to be used with, a digital signature from a certificate authority, a start date, and an expiry date. To be considered valid, a certificate must:

- not yet be expired.
- have a digital signature from a trusted certificate authority.
- have a hostname associated with it that matches the hostname of the machine that is using the certificate.

  Note: If your Email Appliance has several hostnames associated with it, it is important that you ensure the hostname presented to other machines matches your certificate(s) exactly.

By default, the Email Appliance uses what is known as a self-signed certificate. A self-signed certificate is a certificate that has been signed by the creator of a certificate, rather than by a third-party CA. This can be useful for providing encryption functionality when verification of the host's identity by an external CA is not needed. In this case, the host acts as its own CA. This can be the case when the Email Appliance needs to verify its identity to a limited set of hosts, such as communication within a company, or with business partners.

About Certificate Authorities (CA's)

Certificate authorities are trusted third parties. They can be *root authorities* (i.e. explicitly trusted). They can have identities that can be verified by checking with other trusted certificate authorities (such as the root authorities). Or you can choose to designate a CA as trusted (such as an authority within your organization).

The list of trusted certificate authorities included with the Email Appliance is not exhaustive. For example, a new CA may have begun operations recently, but is still considered a trusted certificate authority. This does not mean the Email Appliance will be unable to use unknown CA's, only that you will need to add them to the Email Appliance's list of trusted CA's.

The Email Appliance's certificate authorities can be managed in the **Trusted Certificate Authorities** section of the **Configuration ➤ Policy ➤ Certificates** page.

Note: Sophos maintains a list of trusted certificate authorities for the Email Appliance . You can view, but can not add or delete CA's from this list . You can manage additional CA's from the **Trusted Certificate Authorities** section of the **Configuration ➤ Policy ➤ Certificates** page.

> You and a business partner want to exchange encrypted email, and it is important to you that you can always verify the identity of their mail relays. Since the business partner rarely uses encrypted email except when exchanging email with you, they do not wish to purchase a certificate from a commercial vendor. They also would like you to have the ability send encrypted email to other mail relays they plan to add in the future. By adding your business partner as a certificate authority, you will be able to

verify the identity of any new mail relay they decide to deploy, provided they have signed the new mail relay's certificate.

To add your business partner as a trusted certificate authority:

1. Obtain a copy of your business partner's certificate. This must be in Privacy-Enhanced Mail (PEM) format.
2. In the **Trusted Certificate Authorities** section of the **Configuration ➤ System ➤ Certificates** page, click on **Configure**. The **Trusted Certificate Authorities** dialog box is displayed.
3. Click on the **Locally Managed** tab. A list of trusted certificate authorities is displayed.
4. Click **Add**. The **Add Certificate Authorities** dialog box is displayed.
5. In the **Description** text box, enter a descriptive name for the CA (your business partner in this example) .
6. Either paste the CA certificate in the **Paste Certificate** text box, or select **Import Certificate** to import the CA certificate from a file.
7. Click **OK**.

Your business partner is now listed as a Trusted Certificate Authority.

Your organization has already purchased a certificate from a vendor for a previous mail relay, and now wishes to re-use it for the Email Appliance.

1. On the **Configuration ➤ System ➤ Certificates** page, click **Add**. The **Add certificate** dialog is displayed.
2. Select **Upload existing certificate and private key** and click **Next**. The **Upload certificate** dialog box is displayed.
3. In the **Description** text box, enter a descriptive name for the certificate.
4. Select **Paste** to copy and paste the certificate in the text box, or, select **Import Certificate** to import the certificate from a file.
5. Click **Next**. The certificate is now displayed in the list of available certificates.
6. To use the new certificate for email encryption, navigate to the **Trusted Certificate Authorities** section of the **System:Certificates** page, and select the **Encrypt Email** role for the new certificate.

Your Email Appliance will now offer the new certificate when another mail relay requests to send encrypted email to the Email Appliance.

Obtaining a Certificate for the Email Appliance

If you need the Email Appliance to use a certificate other than those already available, you must initiate a certificate signing request (CSR). Begin the process to initiate a CSR by clicking **Add** on the **Configuration ➤ System ➤ Certificates** page.

Note: The Email Appliance always generates a 2048-bit certificate signing request.

After you have generated a CSR, you can use the CSR to apply for an X.509 certificate from a trusted certificate authority (CA).

Note: Because each vendor has a different procedure for providing a certificate, you will need to contact them for information about their specific procedure.

You may have a business partner who requires that all email be encrypted using transport layer security (TLS). If the self-signed certificate provided with the Email Appliance is not recognized by your business partner, you may need to initiate a CSR and obtain a signed certificate.

You need a certificate from a trusted certificate authority so that your Email Appliance can be verified by any mail server requesting to communicate with your Email Appliance using TLS encryption.

1. Initiate a certificate signing request (CSR) by clicking **Add** on the **Configuration ➤ System ➤ Certificates** page. The **Add Certificate** dialog is displayed.

2. In the **Add certificate** dialog box, select **Initiate CSR**, then click **OK**. The **CSR request** dialog box is displayed.

3. Enter the required information and click **OK**. The CSR dialog box is displayed with the generated (CSR).

4. Save the CSR by pasting it into a text editor and saving it to a file, or by downloading it.

Note: It is important to use a text editor such as Notepad if you cut and paste the CSR. Most word processing programs will not save the CSR correctly.

5. After saving the CSR, you need to contact the certificate authority of your choice, and follow their instructions for uploading the CSR, purchasing a suitable certificate, and downloading the resulting signed certificate.

6. After you have obtained a signed certificate, you will need to upload it to the Email Appliance. On the **Configuration ➤ System ➤ Certificates** page, click **Add**. The **Add certificate** dialog box is displayed.

7. Select **Upload certificate** and click **OK**. The **Upload certificate** dialog box is displayed.

8. Select **Import Certificate** to import the certificate from a file, or, select **Paste**, then paste the certificate in the **Paste Certificate** text box. Click **OK**.

The certificate is displayed in the list of available certificates,

Note: The Email Appliance can have a maximum of three certificates in addition to the self-signed certificate. If you already have three certificates, you will need to delete at least one certificate before you can add a new one.

9. To use the new certificate for email encryption, in the **Certificates** list, select **Email Encryption**, then click **Apply**

.

Your Email Appliance will now offer the new certificate when another server requests to send TLS-encrypted email to the Email Appliance.

Clustering

Use the **Configuration ➤ System ➤ Clustering** page to manage a cluster.

Note: Using clustering requires that you have two or more Email Appliances with identical software versions that are connected to the same network and able to communicate using the ports specified on the *Configuration of Ports* (page 188) page. All appliances used in a cluster must be configured with static IP addresses, which are configured on the **Network: Network Interface** page. Clustering will not work if any of these appliances are configured for DHCP.

If your appliance is not yet part of a cluster, you can enable 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 **Join**.

Important: If an appliance joins an existing cluster, its configuration is overwritten by the configuration options it receives from the cluster.

If your appliance successfully joins or forms a cluster, a list of cluster members is displayed.

If your appliance is a member of a cluster already, you will see a list of all appliances in the cluster. You can:

- Click on the name of a cluster member to view its system status.
- Click **Remove** to remove an appliance from the cluster.

About Clustering

Clustering is a feature of the Sophos Email Appliance that allows two or more appliances to be joined in a group. Configuration data and other data is shared.

What Clustering Provides

- Centralized management of the systems in the cluster.
- The ability to use the interface of any appliance in a cluster to search and present a single view of the data collected by the clustered appliances.
- Sharing of configuration among the clustered appliances.

What Clustering Does Not Do

- Clustering does not provide high availability.
- Clustering does not provide load balancing. If you need to load balance your Email Appliances, you will need to use a hardware load balancing solution, or another suitable solution such as round-robin DNS.

When to Use Clustering

Clustering is useful in several scenarios:

- When you need improved performance and scalability that cannot be provided by a single appliance.
- When you have a multi-site installation, and need unified management and reporting.
- When you want redundancy and improved reliability.

How Clustering Works

Each appliance in a cluster is a completely independent system that processes messages and provides access to the End User Web Quarantine and the administrative user interface. When in a cluster, appliances continually communicate with each other. This is facilitated by one appliance that acts as a configuration manager, which coordinates the flow of configuration information between the appliances that are joined in the cluster.

With the exception of system-specific information (such as hostname and IP address), configuration changes made on one appliance are sent to the configuration manager, which in turn propagates the changes to the other appliances in the cluster.

If an appliance becomes unresponsive or unreachable after two minutes, the other appliances designate the unreachable system as down. Its status is displayed in red, and the System Status button will indicate that there is a problem.

If the appliance becomes reachable again, the other appliances in the cluster respond, usually within twenty seconds, and its status is again displayed in green.

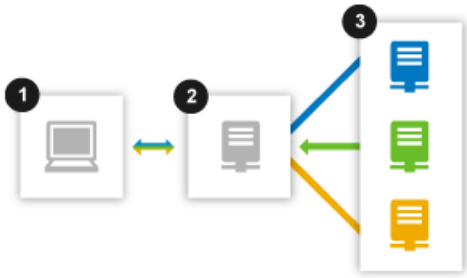
Note: In certain situations, network issues can result in an appliance becoming isolated from the rest of a cluster. The isolated appliance will be unable to reach the rest of the cluster, and will report this. The rest of the appliances in the cluster will continue to communicate with each other, and will only report that the isolated appliance is down.

Searching in a Cluster

You can use any appliance in a cluster to perform a search. If you search the quarantine logs or mail queue, you see data merged from the logs of all of the appliances in the cluster.

Note: if an appliance is unavailable when a full search of the cluster is performed, the results returned will not be complete. This will be indicated with a warning.

To perform a search of the quarantine logs or mail queue:



1. Select the appropriate search parameters on the **Search** tab ❶. You can also choose whether to search either the entire cluster, or just a specific appliance in the cluster.

2. Your search request will be processed by the appliance that is acting as the configuration manager ❷. The configuration manager will collect and merge data from the other appliances ❸ in the cluster.

3. These results will be then displayed on the **Search** tab.

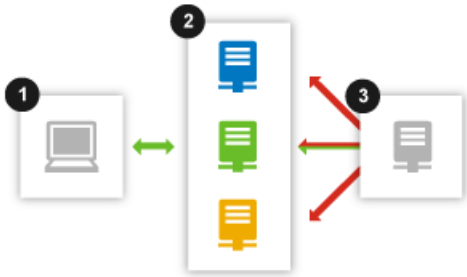
Once an appliance is a member of a cluster, additional functionality and configuration options become available. For an appliance that is a member of a cluster, there are a number of pages that may display additional information, or have options that require additional configuration. For more information, see "Configuring Clustering."

Configuring Clustering

Clustering is configured by navigating to the **Configuration ➤ System ➤ Clustering** page. If the system you are configuring is not yet a part of the cluster, you can use the controls on this page to join or create a cluster.

If the system you are configuring is already part of a cluster, you will see options and controls for managing the cluster, as well as the other systems in the cluster.

To manage the configuration of a cluster:



1. Use your browser to navigate to any system in the cluster ❶.

2. Make any configuration changes that you want.

3. The system you are accessing will then communicate these changes to the system that is acting as the configuration manager ❸ (see "How Clustering Works").

4. The configurations of the other systems in the cluster ❷ will be updated by the configuration manager.

Updates (Clustered)

The **Configuration ➤ System ➤ Updates** page displays a list of all appliances in the cluster, with information about their currently installed threat definition packages and software versions. If a software engine update is available, there are also details about the nature of the update and the time and date of the next scheduled automatic update.

Software engine: The latest available software engine version is displayed. To subscribe to an RSS feed of information about appliance software updates, click the RSS icon to the right of the title. The version number is divided by decimal points into four parts, for example *2.13.2.0*. Reading from left to right, the parts signify:

Version Type	Version Element
major release	***2***.13.2.0
minor release	2.***13***.2.0
maintenance release	2.13.***2***.0

Version Type	Version Element
hotfix release	*2.13.2.**0***

Click **Check for Updates** to refresh this information.

Cluster updating: Each appliance in the cluster is listed in table format:

- **Status icon**: Icon indicating the current status of this appliance (ni).
- **Appliance**: Name of the appliance.
- **Software engine**: Version of the currently installed software version.
- **History**: Clicking on this icon will display a history of all software updates that have been installed since the history list was last cleared.
- **Threat definition installed**: Version number of the current threat definition.
- **Threat definition last updated**: Date and time of the most recent update.
- Click **Update** to force an update of the threat definitions on the selected appliance.
- Click **Update Entire Cluster** to force an update of the threat definitions on all appliances in the cluster.

Note: If the text of an update button is gray, this indicates that no new updates are currently available.

Software engine update schedule: Displays the dates and times that the appliance's software engine will apply updates. There are two types of updates:

- **Critical updates**: these are updates that affect functionality and usability of the appliance.
- **Non-critical updates**: these are updates that may affect the appearance, or introduce new functionality, but are not necessary for the appliance to continue operating properly.

To change the software engine update schedule, click **Configure**.

Running/Configuring Updates

- To download and apply a new update before the next scheduled update window:

  Click **Check for Updates** to retrieve any available updates for an appliance or cluster of appliances.

  Click **Update Now** to install any downloaded updates for an individual appliance. If available updates are installed, the button is grayed out.

  Note: If you are running multiple appliances in a cluster, an **Update Entire Cluster** button is displayed instead of **Update Now**. Clicking it updates all listed appliances. If no updates are available, the button is grayed out

- To specify your preferred software update window:

  Use the **Software engine update schedule** to set the time window in which automatic software updates are installed.

  Critical updates (for example, security-related patches) are applied automatically within 24 hours of availability during the update window. Maintenance updates are applied automatically during the update window, but only on the days of the week specified in the check boxes.

  1. Click **Configure**.
  2. In the **From** and **to** drop-down lists, specify the window of time in which to apply automatic updates.
  3. Select the day of the week check box(es) to specify the day(s) on which non-critical automatic updates are applied.
  4. Click **OK**.

System Status (Clustered)

The **System Status** tab lets you monitor the health and performance of each Email Appliance in a cluster. For more about the system status of individual appliances, see *System Status* (page 161).

When an appliance is a member of a cluster, the **Cluster Status** page displays information about the status of each Email Appliance in the cluster.

Several icons are used to indicate status:

indicates that the status is normal.

indicates a warning that a problem has been detected.

indicates that a problem has recurred, and a critical alert message has been sent.

Note: The System Status icon will always indicate the most urgent condition (normal, warning or critical) of any of the systems in the cluster.

- The **Cluster members** panel displays information about each appliance in the cluster including its status, the name of the appliance, the last time it was contacted from the box you are currently logged into, and its current message load.
  - The status icon next to each system indicates the status of that specific system, and reflects the condition (normal, warning or critical) of the individual system.
  - Click on the name of a specific cluster member to view its **System Status**.

  Note: The system status icon will return to normal (green), provided there are no other warnings or alerts, if:

  - A system that is experiencing a warning condition or alert associated with a global function is rebooted.
  - The system experiencing the warning condition is removed from, then re-joined to the cluster.
  - An individual system that has experienced an issue executing a particular global function is configured so that it is no longer associated with that function.

  More information about configuring clustering can be found on the *About Clustering* (page 136) page.

- The **Global functions** panel displays status information about each function, including its name, a description of the last time a status change occurred, and a link to a history of events for the function.
  - Each global function's status icon shows the most recent status change (normal or alert) that has occurred.
  - If a system in the cluster experiences a problem executing a function, another system in the cluster will re-try the function (if one or more other systems in the cluster have been so configured). The **Global functions** icon will reflect the status of the last attempt to execute this function (normal or alert).
  - The **Description** shows the most recent status for each function. The history icon links to a complete list of all warnings and alerts associated with its respective function.

Time Zone

Use the **Configuration ➤ System ➤ Time Zone** page to set the local time that is used to indicate the time in quarantine information, logs, and reports.

To set the time zone:

1. Select a time zone from the drop-down list that is most appropriate for your organization.
2. Click **Apply**.

Note: Daylight Savings time adjustments are made automatically. The default time zone is Greenwich Mean Time (GMT).

Configuration Sync

Configuration Synchronization allows you to maintain some types of configuration data in text files on a system that is separate from your Email Appliance. You can then sync that data to the Email Appliance via SCP to update your configuration. The types of information you can maintain through Configuration Sync include:

- Internal Hosts
- Trusted Relays

- Recipient Validation
- Recipient Aliases
- Rewrite Senders
- Rewrite Recipients
- Mail Routing

The Email Appliance supports both OpenSSH and PEM public keys. Once you have generated and uploaded your public key, you can use use a command line SCP utility to sync lists and configuration files of the above-listed data to your appliance over port 1232. For more information about SSH, SCP and generating public keys, please visit the *OpenSSH* project web site.

Enable Configuration Synchronization

Use the **Configuration ➤ System ➤ Configuration Sync** page to enable configuration synchronization.

To enable Configuration Synchronization on your Appliance you will need to upload a valid public key. You must upload a public key that meets these requirements:

- Privacy-Enhanced Mail (PEM) or OpenSSH format
- DSA or RSA algorithm
- 1024 bit minimum key length

To configure SCP configuration synchronization:

1. Select **Enable configuration synchronization**.
2. Click **Upload**, and select a public key you want to add to the Appliance.
3. Optionally, select which appliances will use Configuration Synchronization in your cluster.

Example: Configuration Synchronization

With Configuration Synchronization you can maintain configuration data on a separate system and sync it to your Appliance. This example walks through the process of setting up Configuration Synchronization and syncing data to your appliance.

1. Generate a public key so you can configure SCP to transfer files to your appliance.
2. Create and maintain a file with the proper *Files for Configuration Synchronization* (page 140) for the configuration data you want to maintain.
3. Transfer the file using a command-line SCP utility to your appliance over port 1232, as the `sophosscp` user.

   For example:

   ```
   scp -q -i <private key> -P 1232 <filename> sophosscp@<appliance>:
   ```

   Note: You *must* use a command-line SCP utility instead and not a GUI application such as WinSCP. The `-r` option is not supported.

   If there is a problem with the formatting or syntax of your configuration file, you will get a syntax error on the command line once the file has uploaded.
4. Optionally, you can upload an empty file to overwrite an existing file you have transfered to the appliance using SCP.

   The empty file should look exactly like this:

   ```
   # <EMPTY FILE>
   ```

   It must contain the # symbol, followed by a space and then <EMPTY FILE> in all caps, including the angle brackets

Files for Configuration Synchronization

Files and syntax available to the Configuration Synchronization system.

Filenames

These files must have the correct filename and syntax to configure the Email Appliance through Configuration Synchronization. If the name or the syntax is incorrect you will get an error message at the command line when you use SCP to transfer the file to the appliance.

- `SOPHOS_INTERNAL_HOSTS`
- `SOPHOS_TRUSTED_RELAYS`
- `SOPHOS_RECIPIENT_VALIDATION`
- `SOPHOS_RECIPIENT_ALIASES`
- `SOPHOS_REWRITE_SENDERS`
- `SOPHOS_REWRITE_RECIPIENTS`
- `SOPHOS_MAIL_ROUTING`

SOPHOS_INTERNAL_HOSTS

The `SOPHOS_INTERNAL_HOSTS` file contains a list of internal mail relay servers. You can enter a list of hostnames, IP addresses, or IP address ranges. To maintain this data through the related appliance page, browse to: **Configuration ➤ Routing ➤ Internal Mail Hosts** . The syntax of this file is the same as in the **Internal Mail Hosts** page, and the file should contain one entry per line. For example:

```
mailhost.example.com
mailhost2.example.com
192.0.2.2
192.168.45.0/24
```

SOPHOS_TRUSTED_RELAYS

The `SOPHOS_TRUSTED_RELAYS` file contains a list of Trusted Relays: mail gateways between the internet and the Sophos Email Appliance. To maintain this list through the related appliance page, browse to: **Configuration ➤ Routing ➤ Trusted Relays** . This file should contain one IP address or range per line. For example:

```
192.0.2.2
192.0.2.3
10.99.0.0/16
```

SOPHOS_RECIPIENT_VALIDATION

You can use the `SOPHOS_RECIPIENT_VALIDATION` file to manage your recipient validation list. To configure the appliance to use Configuration Synchronization, browse to **Configuration ➤ Policy ➤ SMTP Options** and select **Via Configuration Sync** from the **Method of recipient validation**drop-down list. The file should contain one address per line. For example:

```
janedoe@example.com
bobsmith@example.com
postmaster@example.com
```

Note: You should upload a valid `SOPHOS_RECIPIENT_VALIDATION` file before you enable recipient validation using Configuration Synchronization. If you select **Via Configuration Sync** without uploading a file, the appliance will fall back to **Via SMTP look-ahead** until a valid `SOPHOS_RECIPIENT_VALIDATION` is in place.

SOPHOS_RECIPIENT_ALIASES

Use the `SOPHOS_RECIPIENT_ALIASES` file to copy an alias map list to the appliance through Configuration Synchronization. The file should include one entry per line, with the *from* and *to* portions separated by a colon with a space on each side. You can map either individual addresses or domains. For example:

```
admin@example.com : john.doe@example.com
administrator@example.com : john.doe@example.com
postmaster@example.com : john.doe@example.com
@examplesubsid.com : @example.com
```

To manage recipient aliases lists on your appliance, browse to **Configuration ➤ Accounts ➤ User Groups** , and click **Custom alias maps**. Aliases that have been uploaded through Configuration Synchronization cannot be viewed or edited

on the **Accounts ➤ User Groups ➤ Custom alias maps** page of the appliance. To remove outdated recipient aliases previously added to the appliance through Configuration Synchronization, use SCP to upload a `SOPHOS_RECIPIENT_ALIASES` file that contains only:

```
# <EMPTY FILE>
```

SOPHOS_REWRITE_SENDERS

Use the `SOPHOS_REWRITE_SENDERS` file to manage a list of sender email addresses to rewrite. The file should include one entry per line, with the *from* and *to* portions separated by a colon with a space on each side. For example:

```
admin@example.com : john.doe@example.com
John.doe@example.com : jdoe@example.com
bob.smith@example.com : bsmith@example.com
```

To manage address rewriting directly on the appliance, browse to **Configuration ➤ Routing ➤ Address Rewriting** . Address Rewriting information you have added to the appliance through Configuration Synchronization can be viewed and edited on the **Address Rewriting** page. The Email Appliance executes policy based on the original address before rewriting the sender.

SOPHOS_REWRITE_RECIPIENTS

Use the `SOPHOS_REWRITE_RECIPIENTS` file to manage a list of recipient email addresses to rewrite. The file should include one entry per line, with the *from* and *to* portions separated by a colon with a space on each side. For example:

```
John.doe@example.com : jdoe@example.com
bob.smith@example.com : bsmith@example.com
```

To manage address rewriting directly on the appliance, browse to **Configuration ➤ Routing ➤ Address Rewriting** . Address Rewriting information you have added to the appliance through Configuration Synchronization can be viewed and edited on the **Address Rewriting** page. The Email Appliance executes policy based on the new recipient after rewriting the recipient.

SOPHOS_MAIL_ROUTING

The `SOPHOS_MAIL_ROUTING` file allows you to push mail routing configurations to your appliance through Configuration Synchronization. The file uses an XML format to specify delivery and routing information for the appliance. Review the *Routing* (page 143) to configure the various configuration settings available in this file through the appliance's administrative interface. The example `SOPHOS_MAIL_ROUTING` file below gives examples of configuring A records, MX records, and routes.

```
<?xml version="1.0" encoding="UTF8"?>
<mail-routing>
  <delivery>
    <mta host="10.100.140.60:25" dns_type="A" desc="10.100.140.60:25"/>
    <mta host="HOST1:25" dns_type="MX" desc="Exchange servers - New York Data Centre">
      <mx pri="10" host="ny1.example.com"/>
      <mx pri="20" host="ny2.example.com"/>
    </mta>
    <mta host="HOST2:25" dns_type="MX" desc="Exchange servers - UK Data Centre">
      <mx pri="10" host="uk1.example.com"/>
      <mx pri="10" host="uk2.example.com"/>
    </mta>
  </delivery>
  <routes>
    <route domain="example.net" withsubdomains="yes">
      <scope>
          mail-ny.example.com
          mail-uk.example.com
      </scope>
    </route>
    <route domain="example.org" withsubdomains="yes" deliver_to="10.100.140.60:25">
      <exclude>
        ca.example.org
        fr.example.org
      </exclude>
      <scope>
```

```
        mail-ny.example.com
        mail-uk.example.com
      </scope>
    </route>
    <route domain="example.com" withsubdomains="no" deliver_to="HOST1:25">
      <scope>
        mail-ny.example.com
      </scope>
    </route>
    <route domain="example.com" withsubdomains="no" deliver_to="HOST2:25">
      <scope>
        mail-uk.example.com
      </scope>
    </route>
  </routes>
</mail-routing>
```

Routing

Messages passing through the Email Appliance are routed to their final destination according to the configuration specified on the **Routing** pages. Mail can be routed to specific internal hosts based on the domain to which it is addressed, outbound relays through the Email Appliance can be restricted to specific hosts, trusted external relays can be specified, and outbound SMTP proxies can be set.

Adding/Removing Mail Delivery Servers

On the **Configuration ➤ Routing ➤ Mail Delivery Servers** page, specify the internal mail servers that receive incoming mail from the Email Appliance.

You can add a single mail delivery server, add a group of mail delivery servers, and remove mail delivery servers or server groups.

- To add a single mail delivery server:

  1. Click **Add**.

     The **Add Mail Delivery Servers** dialog box is displayed.
  2. From the drop-down list, select **Add a single mail delivery server**.
  3. In the **Description** text box, enter a name or something else that helps you to identify the mail server.
  4. In the **Address** text box, enter the fully qualified hostname or IP address of the mail delivery server.
  5. In the **Port** text box, enter the port on which the server is listening for SMTP connections.
  6. From the **DNS type** drop-down list, select The type of DNS record used to lookup the host (**A** or **MX** record).

     Note: DNS A records are used for looking up hosts for most types of network connections (HTTP, FTP, etc). DNS MX records are used specifically for email routing and can be used to specify multiple hosts (for example, for failover or load balancing). If the mail delivery server does not have an MX record in DNS, set the **DNS Type** to **A**.

  7. Click **OK**.

     The new server information is displayed in the **Mail delivery servers** table.

- To add a mail delivery server group:

  1. Click **Add**.

     The **Add Mail Delivery Servers** dialog box is displayed.
  2. From the drop-down list, select **Add a mail delivery server group**.
  3. In the **Description** text box, enter a name or something else that helps you to identify the mail server.

4. In the **Port** text box, enter the port on which the servers are listening for SMTP connections.
5. In the **Address** text box, enter the fully qualified hostname or IP address of the mail delivery server. All mail delivery server groups use MX records.
6. From the **Priority** drop-down list, assign a value for the server. The lower the number the higher the priority. If, for example, you wanted to perform load balancing with four mail delivery servers, you could set the priority to "10" for each of them. Or, if you had two mail delivery servers, but you wanted to use the second as a backup in case the first became overloaded, you could set the first server to "10" and the second to "40."
7. Click **Add**.

   The server is added to the address list.
8. Repeat steps 6,7, and 8 for each server that you want to add. To remove a server from this list, select the check box next to the address, and click **Delete**.
9. When you have finished adding servers, click **OK**.

   The new server information is displayed in the **Mail delivery servers** table.

Adding/Removing Mail Domains

On the **Configuration ➤ Routing ➤ Mail Domains** page, you can specify hosts to which messages are routed for multiple domains.

- To add a mail-accepting domain:

  1. Click Add.

     The **Add Mail Domain** dialog box is displayed.
  2. In the **Incoming mail domain name** text box, enter the fully qualified domain name.
  3. From the drop-down list, select:

     - **Include sub-domains**: If you choose to include sub-domains, messages to a sub-domain will be delivered to the destination that you specify in step 6.

     or

     - **Do not include sub-domains**: If you exclude sub-domains, messages to a sub-domain will be rejected unless there is a separate record for the fully qualified sub-domain.
  4. [Optional] If you chose **Include sub-domains** in the previous step, you can make one or more exceptions by specifying any sub-domains that you don't want to include. To do so, select the **Exclude sub-domains** check box, enter a sub-domain, and click **Add**. Repeat these steps for each sub-domain that you want to exclude.
  5. Click **Next**.
  6. On the **Mail Delivery** page, under **Mail delivery settings**, select one of the following:

     - **Deliver using DNS MX records**: Mail is delivered according to MX records associated with the domain you specified in step 2.
     - **Deliver to the following server or group**: Mail is delivered to the server or server group that you select from the drop-down list. This drop-down list contains available delivery servers or server groups that were specified on the **Configuration ➤ Routing ➤ Mail Delivery Servers** page.
  7. Click **Next**.
  8. [Optional: clustered appliances only] On the **Cluster Settings** page, under **Appliances**, select one of the following:

     - **All appliances**: The domain applies to all appliances in the cluster.
     - **Only the following appliance(s)**: Select the check box next to the appliance(s) for which you want the domain to apply.
  9. Click **Save**.

The new domain-to-host mapping information is displayed in the **Incoming mail domains** table. (In a clustered environment, affected appliances are indicated in the **Applies to** column. Mouse over the displayed appliance name for the complete hostname or list of hostnames.)

- To remove a mail-accepting domain:
  Select the check box beside the domain that you want to remove, and click **Delete**.

Internal Mail Hosts

On the **Configuration ➤ Routing ➤ Internal Mail Hosts** page, you can specify which internal hosts are allowed to send outbound email through the Email Appliance.

Adding/Removing Internal Mail Hosts

- To add a mail relay server:
  In the **Internal hosts and networks** text box, enter the hostname, IP address, or IP address range, and click **Add**.

  Note: To set an IP address range, use CIDR notation (for example, 192.168.45.0/24).

  The new entry appears in the **Internal hosts and networks** table.
- To remove a mail relay server:
  Select the check box beside the mail relay server that you want to remove, and click **Delete**.

Setting an Outbound Mail Proxy

On the **Configuration ➤ Routing ➤ Outbound Mail Proxy** page, set the proxy server the Email Appliance will use to relay outbound mail to the internet. Optionally, you can use Transport Layer Security (TLS) to enforce a secure connection between the appliance and the mail proxy. You can also authenticate with a username and password if the proxy server requires them.

1. Select **Use outbound mail proxy** to enable routing via a proxy server.
2. In the **Hostname** text box, enter the IP address or hostname of the mail proxy.
3. In the **Port** text box, enter the port on which the server is listening for SMTP connections.
4. 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). If the mail delivery server does not have an MX record in DNS, set **DNS Type** to **A**.

5. [Optional] Select **Enforce TLS** if the proxy server requires connection via TLS.
6. [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.
7. Click **Apply**.

Adding/Removing Trusted Relays

Trusted relays are internal or external mail relays that you know are safe. Keeping the list of trusted relays accurate and up to date is an important component of spam detection. Any spam sent through unlisted trusted relays will have a much lower detection rate.

You can specify trusted relays on the **Configuration ➤ Routing ➤ Trusted Relays** page to improve the accuracy of the Email Appliance's spam detection. This will also improve the troubleshooting and reporting information provided by the Sophos Email Appliance.

Note: Detailed information about trusted relays can be found in the *About Trusted Relays* (page 146) reference.

If your network does not use a configuration of this kind, leave the **Trusted relay list** empty.

- To add a trusted relay:

  In the **IP address** text box, enter the IP address of the trusted relay, and click **Add**.

  The added IP address is displayed in the **Trusted relay list** table.

  Caution: It is important to ensure that a host never appears simultaneously in the **Trusted relay list** and the **Allowed Hosts** list.

- To remove a trusted relay:

  Select the check box beside the IP address that you want to remove, and click **Delete**.

  The IP address of the trusted relay is removed from the list.

  Note: If your network uses trusted relays to pass inbound messages to the Email Appliance, use policy-level blocking instead of connection-level blocking. Connection-level blocking will only work correctly if the Email Appliance receives messages directly from the internet.

About Trusted Relays

About Trusted Relays

Trusted relays are internal or external mail relay hosts that you know to be safe; that is, you trust that these hosts will not be the source of unwanted emails, although it is possible that unwanted emails could still be relayed through them. Trusted relays can exist both inside ("internal trusted relays") your network, and outside ("external trusted relays") of it.

Examples of internal trusted relays include:

- Site-specific email/webmail servers.
- Mailing-list management systems.
- Item-tracking servers.

Examples of external trusted relays include:

- Mail hosts managed by your organization.
- Mail relays owned by business partners that accept and relay a large volume of email on your behalf.
- Mail relays managed by your ISP.

It is important to note that, when trusted relays are configured, the appliance is able to identify the first untrusted relay (FUR). Otherwise, the FUR is set to the connecting relay. Additionally, when trusted relays are configured, the FUR can be identified by the use of the "Received" headers, when an email has been received from one or more trusted relays.

Note: Spammers can easily forge received headers; but the received header written by a trusted relay can, as the name implies, always be trusted. Even if a message was delivered through a number of trusted relays in sequence, you can still always extract the first untrusted relay from the received headers, then use that IP as the starting point for reputation checks, as well as for logging and reporting.

Advantages of Using Trusted Relays

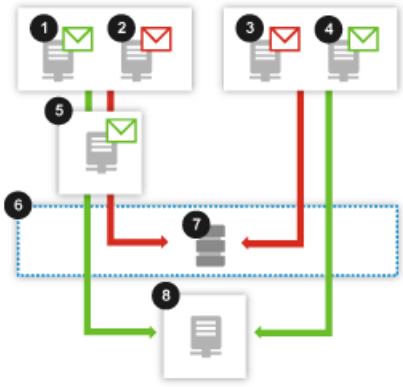
There are a number of benefits provided by configuring the Sophos Email Appliance to use trusted relays.

- **Facilitate reputation filtering in the policy:** Reputation filtering is one of the most effective forms of preventing unwanted email. If inbound email goes through one or more upstream relays, then reputation filtering cannot be done by an MTA based on the connecting relay. However, it is possible to do reputation filtering in the policy if these hosts are trusted relays, and they have been correctly configured in the trusted relays list.
- **Improved spam checking efficiency:** The appliance will not waste resources performing DNSBL and RBL checks on the IP address of the trusted relay, and will instead check the FUR and any subsequent relays in the received chain.
- **Improved spam catch rate:** A message is more likely to be spam if the first untrusted relay has a bad reputation, while it is unlikely that a trusted relay has a bad reputation. However, if a trusted relay is not configured as such, and a spam message is relayed to it from an untrusted relay, the appliance will use the trusted relay's reputation, rather than that of the untrusted relay that sent the spam. This reduces the likelihood that this message will be categorized as spam. If, instead, the trusted relay is configured correctly, the appliance will use the first untrusted relay's reputation instead. This will improve the spam catch rate.
- **More accurate reports:** The **Top Spam Relays** and **Top Virus Relays** reports always report the connecting relay. This is not very useful if the connecting relay is normally a single relay, through which a large portion of your email is routed. However, if that relay is configured as a trusted relay, the first untrusted relays in the received chain will then appear in reports. This can make it easier to identify the actual source of any unwanted emails.
- **Improved management of Blocked/Allowed hosts:** If a large number of incoming messages are routed through a single upstream relay, but this relay is not configured as a trusted relay, then it will appear as though most unwanted emails are originating from this relay. In this case, most messages sent by hosts in the **Allow/Block Lists** will not be correctly identified as coming from these hosts.

  However, if this relay is configured as a trusted relay, then the appliance will instead apply the **Allow/Block Lists** to the first untrusted relay, rather than to the now-trusted relay.
- **Trusted relays can be used in policy rules:** Similar to the allowed/blocked hosts lists, the "source ip" message attribute will not always trigger, unless trusted relays have been correctly configured.
- **Identification of internal spambots in your organization:** If the internal email servers that are authorized to send outgoing email are configured as trusted relays, any outgoing messages that are identified as spam can immediately alert you to the possibility of infected hosts within your organization. It can also allow you to identify any infected hosts. In a scenario such as this, Sophos recommends configuring your policy so that notifications will be sent to adminstrators or helpdesk operators if outgoing spam is detected.

Due to the advantages conferred, it is recommended that you configure the appliance to use trusted relays whenever possible.

Example 1: Trusted Upstream Mail Relay



You have an upstream mail relay 5 that accepts email from the internet for a number of domains. This relay distributes email to the mail servers in the regional offices of your organization, including your Sophos Email Appliance. You have configured the appliance to recognize this mail host as a trusted relay. This enables the appliance to provide:

- correct reputation filtering.
- better efficiency during spam checks.

- a higher spam catch rate.
- improved reporting (mail from their server will not appear on spam reports).

Valid emails, as well as spam messages relayed through your upstream mail relay ❺ will be received by the appliance ❻. Both will be identified as having been sent from a trusted relay.

This allows the Sophos Email Appliance to correctly identify which relays are the first untrusted relays (❶ and ❷). Correctly identifying the first untrusted relays enables more accurate reputation and spam checking, and significantly enhances reporting and troubleshooting.

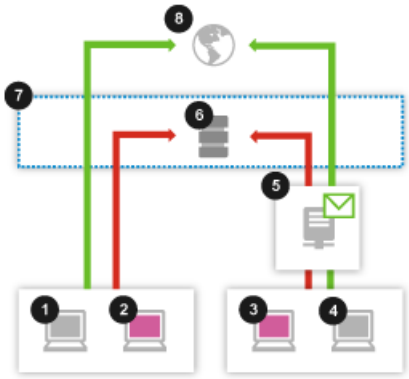
This, in turn, allows the appliance ❻ to effectively stop messages from external untrusted relays that are sending unwanted emails ❷, while still delivering valid messages to the appropriate mail delivery server ❽ that are sent by other external untrusted relays ❶.

Mail from other external (untrusted) relays (❸ and ❹) will continue to be received and correctly processed by the appliance ❻. Messages from servers sending unwanted messages ❸ will continue to be blocked, and messages from servers sending valid messages ❹ will continue to be delivered to the appropriate mail delivery server ❽.

A trusted relay is essentially transparent to the appliance. All incoming mail will appear to be coming directly from the internet. This helps ensure that reputation filtering, spam checking, reports, and logging will function accurately and efficiently.

Whenever a mail relay can be trusted to not be a source of spam, you should add it to the trusted relays list. Examples of trusted mail relays include corporate mail gateways, mail servers owned by business partners, or a mail relay managed by your ISP.

Example 2: Internal Trusted Relays



You have configured your Sophos Email Appliance ❼ to scan outbound messages for spam, and you have an internal mail server ❺ that is used to send, receive and store email for most users in your company. Your appliance processes all inbound and outbound email to and from this server. You have configured the appliance to recognize this mail host as a trusted relay. This enables the appliance to:

- identify that compromised hosts are present within your organization.
- provide reports that may help you to identify the IP address of any compromised hosts.

Any email sent through your internal mail server ❺ by internal hosts (❸ and ❹) will be received by the appliance ❼, and will be identified as having come from a trusted relay. This ensures that:

- First untrusted relays (❸ and ❹) will be correctly identified in reports and notifications, and for troubleshooting purposes.

- The appliance will more effectively block messages from any internal hosts sending spam ❸ through your internal mail server ❺.
- Messages from internal hosts that send valid emails ❹ will be delivered to the appropriate recipients ❽.

Mail from other internal hosts (❶ and ❷) will be received and then correctly processed by the appliance. Messages from internal hosts sending spam ❷ will be blocked, while messages from internal hosts sending valid messages ❶ will continue to be delivered to the appropriate recipients ❽.

The scenario described above only applies to internal hosts that relay mail through your internal mail servers. Frequently, users send and receive mail from their internal mail server using a local transport protocol (rather than SMTP). In such a case, it would not be possible to identify the IP address of a workstation that sent a message through the appliance.

About Address Rewriting

By rewriting addresses you can ensure that the Email Appliance processes messages using the addresses associated with the appliance's policy, while displaying the rewritten addresses to users. Address rewriting is particularly useful in cases when some or all of your email users are making the transition to a new address, or if you want any addresses that mail users see to be different from the addresses specified in the appliance policy.

Note: Address rewriting should not be confused with alias maps, which are also supported on the Email Appliance. An alias map is a method for substituting an email address with another for the purpose of policy filtering, quarantine summaries, and user block lists (for more information, see “Enabling/Disabling Alias Maps”). Address rewriting, on the other hand, alters the address (and, optionally, the message headers) of an email message either before or after it is processed by the policy.

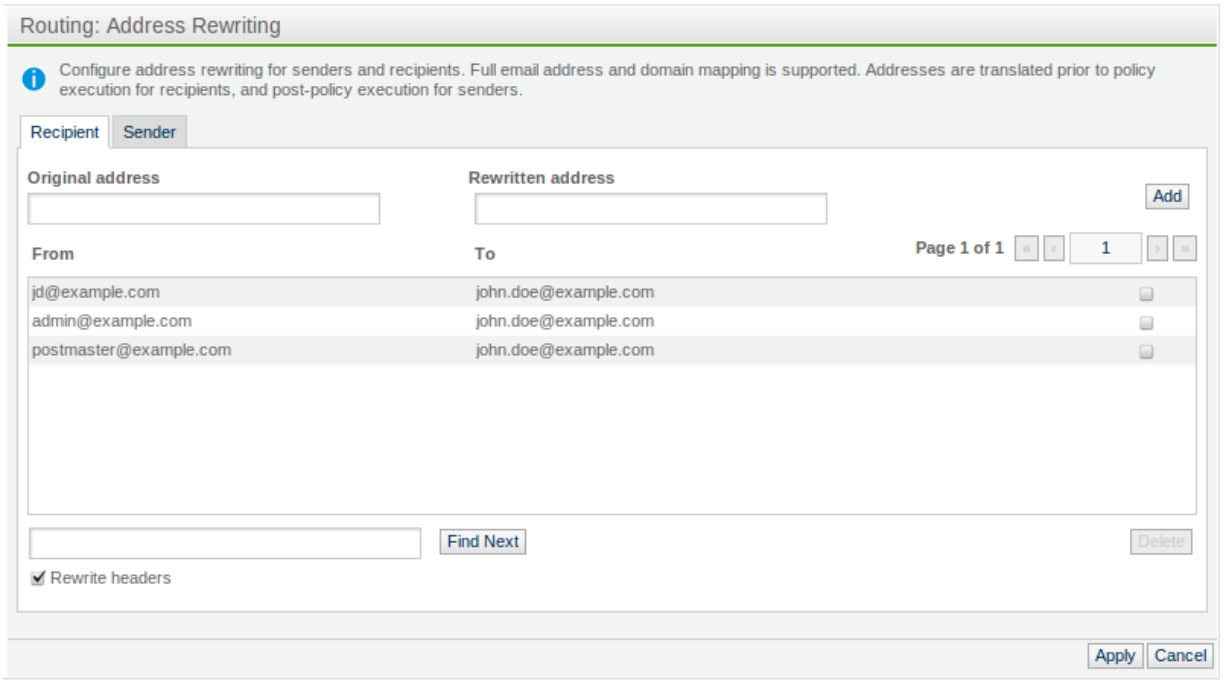
Regardless of your reason for rewriting addresses (examples are given below), you must provide valid entries for the **Original address** and **Rewritten address.** You can enter a complete email address, or just the domain portion of an address. All entries must include the “@” symbol. So, for instance, the following entries are valid:

- `user1@example.com`
- `@example.com`

These entries, however, are invalid:

- `user1`
- `example.com`

There are two rewrite types: “Recipient” and “Sender”. In some instances you may want to create corresponding recipient and sender entries. **Recipient** and **Sender** addresses are configured on separate tabs (as shown in the image below). When configuring addresses, it is assumed that "recipients" are destination addresses within your organization, and "senders" represent email accounts that are sending messages from within your organization.



There are a variety of reasons for rewriting email addresses. Here are some of the more common reasons:

- **Alternative/Vanity Addresses**: If the corporate standard for email addresses is *`FirstName.LastName`*`@example.com`, you can use address rewriting to specify that the format of an address displayed in email messages is different from the one that the Email Appliance uses to process mail. For example, you can abbreviate `John.Doe@example.com` to `JD@example.com`:

Rewrite Type	Original address	Rewritten address
Recipient	`JD@example.com`	`John.Doe@example.com`
Sender	`John.Doe@example.com`	`JD@example.com`

- **Replace Multiple Addresses with a Single Address**: A member of your organization may have multiple email identities (for example, `admin@example.com`, `webmaster@example.com`, `IT@example.com`); however, for the purpose of processing mail, it often makes sense to rewrite these various recipient addresses to one address (John.Doe@example.com), so that mail for all these addresses are directed to a single account. To configure this particular example, you would create three separate entries on the **Recipient** tab.

Rewrite Type	Original address	Rewritten address
Recipient	admin@example.com	John.Doe@example.com
Recipient	webmaster@example.com	John.Doe@example.com
Recipient	IT@example.com	John.Doe@example.com

- **Replace Subsidiaries with Parent Company**: Although a company may have one or many subsidiaries, it can create a consistent customer experience by making it seem as if all the email comes from a particular domain. So, if Company B (a subsidiary) provides support for Company A (a parent), you could rewrite the addresses so that customers direct their queries and comments to `support@CompanyA.com`, and they receive responses from the same address. In this case, messages addressed to `support@CompanyA.com` are rewritten by an Email Appliance at CompanyA and routed to `support@CompanyB.com`. Conversely, messages sent from staff using `support@CompanyB.com` are routed through the same appliance at CompanyA, rewritten to `support@CompanyA.com`, and sent back to the customer.

Rewrite Type	Original address	Rewritten address
Recipient	support@CompanyA.com	support@CompanyB.com
Sender	support@CompanyB.com	support@CompanyA.com

- **Domain Changes**: If your organization undergoes a merger, acquisition, or name change, there will likely be a transition period during which you want to continue accepting mail that is sent to old addresses while you are beginning to use the new addresses. Rewriting recipient and sender addresses allows you continue to honor the old addresses, even though those within the organization appear to be sending and receiving mail with the new addresses. For example, to rewrite addresses for everyone within a single domain who have been assigned to a new domain:

Rewrite Type	Original address	Rewritten address
Recipient	`@old.domain.com`	`@new.domain.com`
Sender	`@old.domain.com`	`@new.domain.com`

Configuring Address Rewriting

On the **Configuration ➤ Routing ➤ Address Rewriting** page, specify the email senders and recipients for which email addresses will be rewritten.

For recipients, addresses are rewritten before they are processed by the appliance policy; for senders, they are rewritten after they are processed by the policy. This way, whether the message is sent or received by the Email Appliance, the policy tests are applied to the original address rather than the rewritten address that senders or recipients see.

As an alternative to adding entries on the **Routing: Address Rewriting** page, you can create files containing address rewriting maps, and SCP them to the Email Appliance. For more information, see the Configuration Sync documentation.

On the **Recipient** or **Sender** tab:

1. In the **Original address** text box, enter the email address that is used to identify the recipient or sender in the appliance policy.
2. In the **Rewritten address** text box, enter the email address that will be displayed to users.
3. Click **Add**.
4. [Optional] The **Rewrite headers** check box is selected by default, causing the `From:` and `To:` message headers to also be rewritten to match the rewritten address. Clear this check box if you want to preserve the original address in the headers. A **Rewrite headers** check box appears on both the **Recipient** tab and the **Sender** tab, and they are configured separately.

   If you are managing address rewriting lists via SCP instead of using the **Routing: Address Rewriting** page, you still must clear the check boxes on these tabs if you want to preserve the original addresses in the headers.
5. Click **Apply**.

To remove a rewritten address, select the check box next to the address, and click **Delete**.

To search a list of rewritten addresses, enter a search string, and click **Find Next**. Use the page controls to navigate multiple pages of results, or click **Find Next** again to advance to the next page.

Network

Use the **Network** pages of the **Configuration** tab to reconfigure Email Appliance Network options that were set in the Setup Wizard.

Configuring Interface Settings

On the **Configuration ➤ Network ➤ Network Interface** page, you can configure your Email Appliance with a static IP address or have it assigned via DHCP. If **DHCP** is selected, the **IP Address**, **Network Mask**, and **Default Gateway** fields are grayed out (unavailable). The **Obtain DNS servers automatically** option button is selected automatically, but this can be overridden if necessary.

Note: Messages are sent and received via the primary network card only. The secondary network card uses a fixed IP address for failsafe administrative access to the Email Appliance.

To configure the primary network interface:

1. [Optional: clustered appliances only] From the **Appliance** drop-down list, select which system in the cluster you want to configure.
2. Select either **DHCP** or **Static IP**. You must use **Static IP** if you are configuring a system for use in a cluster. If you choose the **Static IP** option, you must also fill in the following text boxes:
   - Enter the **IP Address** for the primary network card.
   - Enter the IP address of your network's **Default Gateway**.
   - Enter the **Network Mask**. This is the range of addresses that the Email Appliance can connect to directly. IP addresses outside of this range are reached via the **Default Gateway**.

   If **Static IP** is selected, you can configure additional routes by clicking **Advanced**, which opens the **Additional Network Routes** dialog box. Additional routes can enable the Email Appliance to process requests from client machines whose IP addresses reside outside of the native subnet of the Email Appliance.

   Important: Adding routes is an advanced option and should only be used if you have a thorough understanding of both routing and your network topology. Adding routes incorrectly can make the administrative user interface inaccessible.

   If **DHCP** is selected, the **Obtain DNS servers automatically** option button is selected by default. This can be overridden if necessary. The **Speed and duplex** option is set to **Auto** by default. If you select another setting from the drop-down list, it must match the speed of your managed switch in order for the Email Appliance to operate correctly.

   The MAC address of the appliance is displayed under **Hardware Address**.

   If necessary, you can **Re-register a cloned virtual appliance**. If you are viewing settings for a hardware-based email appliance, this option is grayed out.
3. Select the appropriate **Speed and duplex** from the drop-down list.
4. Select **Obtain DNS servers automatically** or **Specify the DNS servers** to set which method the Email Appliance will use to find your DNS servers' IP addresses. If the **Specify the DNS servers** option is selected, enter the IP addresses of your network's DNS servers in priority order (Primary through Tertiary).
5. Click **Apply**.

Re-Registering a Virtual Appliance

If you clone a virtual appliance, each cloned instance ***must*** be re-registered before you can use it in live production mode.

Re-registration is necessary to take advantage of reporting and clustering features. If you do not re-register a cloned appliance, it cannot be distinguished from the parent appliance (the virtual machine it was cloned from) if both are used on the same network; properties such as the hostname and static IP address are identical to that of the parent virtual machine.

You can re-register a virtual appliance on the **Configuration ➤ Network ➤ Network Interface** page. Alternatively, you can use the command-line interface of the virtual appliance, which is available via the **Console** tab of your VMware client. See the Virtual Email Appliance Setup Guide for more information.

Important:

If the appliance you plan to clone belongs to an existing cluster of appliances, you must remove it from the cluster before cloning. Once you have cloned an appliance and re-registered it according to the steps that follow, you can join one or both of the appliances to the cluster.

Before re-registering, ensure that you have configured unique network and hostname settings for the cloned virtual appliance. See the Virtual Appliance Setup Guide for more information.

If you have configured certificates for the appliance on the **Configuration ➤ System ➤ Certificates** page, you must upload new certificates that bear the hostname of the cloned appliance. This is not necessary if you are using the default self-signed certificate.

To re-register a virtual appliance:

1. Click **Re-Register**.
2. In the **Re-Register Cloned Virtual Appliance** dialog box, You are prompted to erase duplicate data that has been copied to the cloned virtual appliance from the original image. Doing so removes duplicate logs, reports, and message store data. If you want to do this, select **Erase duplicate data**.

   Note: Before re-registering, ensure that you have configured unique network and hostname settings for the cloned virtual appliance. See the Virtual Appliance Setup Guide for more information.

3. Click **OK**.
   When re-registering is complete, you are returned to the **Network Interface** page, and the status is displayed at the bottom of the page.

Setting a Hostname and Proxy

On the **Configuration ➤ Network ➤ Hostname and Proxy** page you can set your Email Appliance system's domain name, configure HTTP proxy server access to the internet and set up a custom FQDN for Time-of-Click (ToC) URL rewriting..

Note: If you are also using a Sophos Web Appliance, you should not configure it as the HTTP proxy for your Sophos Email Appliance. Instead, on your Web Appliance, add the Email Appliance(s) to the list of exempt IP addresses on the Active Directory Exemptions page.

To configure a hostname, proxy and ToC server:

1. [Optional: clustered appliances only] From the **Appliance** drop-down list, select which system in the cluster you want to configure.
2. Type in the Email Appliance's **Fully qualified domain name** (FQDN).
3. Under **Proxy server configuration**, select either **Connect to the internet directly** or **Connect through a proxy server**.

   If you select **Connect through a proxy server**, fill in the following text boxes:

   - In the **Server address** text box, enter the IP address of the proxy server.
   - in the **Port** text box, enter the port number for proxy server.
   - If your proxy server requires a login, enter the **Username** and **Password**.

4. Under **Time-of-Click Protection server configuration** configure the FQDN to be used during URL rewriting. You can either select the default FQDN configured in step 2 OR mention a custom FQDN and port.

   Note:

   - If configuring a custom FQDN, make sure that FQDN can be resolved by a DNS server and is redirected to the IP Address of the Sophos Email Appliance.
   - Custom port should be unused, preferably greater than port 1023.

5. Click **Apply**.

Testing Network Connectivity

Use the **Configuration ➤ Network ➤ Network Connectivity** page to test the options set on the **Network: Interface Settings** page and **Network: Hostname and Proxy** page, to test the connectivity to specific hosts and to decode encoded URLs.

The **Network: Network Connectivity** page also provides access to the network connection troubleshooting utilities described below.

- [Optional: clustered appliances only] From the **Appliance** drop-down list, select the system in the cluster for which you want to perform tests.
- To test your Email Appliance's network configuration:

  Click **Test**.

  The test results are shown as the test proceeds. If the test is successful, a final "Test complete" message is displayed along with a check mark icon. If there are any problems establishing the connection, details about where the problem was encountered are displayed, as well as information to help you troubleshoot the problem.

  Note: If your appliance's ethernet ports are connected to the same network, you will see a warning that the network interfaces are **cross-wired**. You should either ensure they are connected to different network segments, or you can disconnect the **config** ethernet port.

- To test the connectivity to a specific host:

  1. in the **Hostname** text box, type the host's fully qualified Hostname or IP address.
  2. Select the type of test from the option list:
     - **Ping** checks whether it is possible to contact a specific host.
     - **Traceroute** provides a list of all hosts on the route between the appliance and the other host.
     - **DNS Query** displays the IP address associated with a given hostname, or, if an IP address was provided instead, the hostname associated with this IP (if any).
  3. Click **Submit**. The results of the selected test are displayed.

  Note: Establishing a working connection to your network and the internet is essential for the proper functioning of the Email Appliance. Connection to the internet is also necessary for automatic software updates from Sophos, as well as anti-spam and anti-virus data updates.

- To decode a URL which has been encoded by the Email Appliance due to a Time-of-Click Protection Policy:

  1. In the **Hostname** text box, enter the encoded URL.
  2. Select **Decode**.
  3. Click **Submit**. The decoded URL is displayed.

Reports

The **Reports** tab provides performance statistics in the form of graphs and tables.

Note: If you are running multiple appliances in a cluster, reports can be generated for that entire cluster, or for a specific appliance within a cluster. A single appliance from the cluster can be selected from the drop-down list at the top of the **Report Parameters** sidebar. Reports generated for the entire cluster merge data from all systems in the cluster. Reports generated for a specific appliance in the cluster show results for that appliance only.

The **Reports Home Page** contains summary information about key statistics, including mail volume, performance, alerts and frequent viruses. Data on specific aspects of Email Appliance activity is contained in the individual reports described in the **Report Categories** section.

There are also instructions on how to generate, print and export reports.

Report Categories

Click on a report name on the sidebar to view details for a specific report. Each report page contains additional options for setting the period covered by the report and the format of the report.

There are four main types of reports:

Mail Trends

- **Volume**: Displays the various types of messages as a percentage of the total mail volume. The types are Blocked connections, Legitimate, Other, Spam high, Spam medium, and Viruses.
- **Delayed Volume**: Displays the number of delayed messages. Delayed messages are messages that are suspected to be spam, and which are held until they can be rescanned with the most up to date information from Sophos Labs.
- **Message Actions**: Displays statistics on the actions performed on messages (Quarantined, Delivered, Routed or Dropped).
- **Sandstorm Volume**: Displays blocked and clean messages as a percentage of the total mail volume analyzed by Sandstorm.

  Note: If **Period** is selected as **Today**, the report is generated based on mail volume calculated from 12 AM (00:00 hrs) of that day.

- **Time-of-Click Protection**: Displays a list of the top 100 URLs that have been scanned due to ToC Protection policies.

Performance

- **Latency**: Displays the delay (measured in seconds per message) that the Email Appliance is imposing on message delivery.
- **Throughput**: Displays the rate (measured in messages per second) at which the Email Appliance is processing messages.

Senders

- **Virus Relays**: Displays the top ten virus relays during the specified time period.
- **Spam Relays**: Displays the top ten spam relays during the specified time period.
- **Blocked Connections**: Displays the top ten blocked connections during the specified time period.

Recipients

- **Spam Recipients**: Displays the email addresses of the top ten spam recipients during the specified time period.
- **Bulk Recipients**: Displays the email addresses of the top ten bulk email recipients during the specified time period.

Policy Analysis

- **Anti-Virus**: Displays data on messages containing viruses relative to data on suspect attachments, encrypted attachments, and unscannable attachments. In the **Mail Flow** drop-down list, select whether the report is for inbound or outbound mail.
- **Anti-Spam**: Displays messages identified as spam and categorizes them according to their spam scores (high or medium). Blocked connections are also displayed.
- **Content**: Displays data on messages identified using content rules and categorizes them according to the type of content rule they triggered. In the **Mail Flow** drop-down list, select whether the report is for inbound or outbound mail.

Creating and Running Reports

On the right side of each individual report page is a **Parameters** sidebar with options for specifying the time period covered by the report and the display format of the report. The options vary according to the type of report.

To create and run a report:

1. Set the desired parameters:
   - Select the **Period** that the report will cover.
   - Select the **Chart** format (**Line** or **Bar**).
   - Select the **Show data table** check box if you also want to display an accompanying table.
2. Click **Run Report**.
   The report is displayed in the Content panel.

Printing Reports

To print a report:

1. On the **Reports** sidebar, click the name of the report that you want to print.
   The report is displayed.
2. On the **Report Parameters** sidebar, use the available options to specify a **period** and **format** for the report.
3. Click **Print**.
   The report is displayed in a new window of your default browser.
4. Use your browser's print options to print the report.

Exporting Reports

To export report data in comma separated value (CSV) format:

1. On the **Reports** sidebar, click the name of the report that you want to export.
   The report is displayed.
2. On the **Report Parameters** sidebar, use the available options to specify a **period** and **format** for the report.
3. Click **Export**.
   A text file is generated that contains the report data in CSV format. You are then prompted to save the file or open it in the default associated program.

Adding Trusted Relays from a Report

The **Virus Relays** and **Spam Relays** reports can assist you in identifying trusted relays. If a mail relay you know to be trusted appears in these reports, you can add it to the list of trusted relays. This can improve the accuracy of the Email Appliance's spam detection.

To add a trusted relay from a report:

1. On the **Reports** sidebar, select either **Virus Relays** or **Spam Relays**.

The report is displayed.

2. Next to the relay that should be added as a trusted relay, click the **Add** button.

The relay is added to the trusted relays list. The **Add** button is replaced by a green "added icon". Data for the relay is no longer added to the report.

Search

Use the **Search** tab to search the quarantine and logs. Select the type of search to perform from the top drop-down list on the **Search In** sidebar. Different **Search Parameters** are displayed, depending on the type of search selected. There are three search types:

Note:

If you are running multiple appliances in a cluster, you can search the entire cluster, or you can select a single appliance in the cluster from the drop-down list at the top of the **Search Parameters** sidebar.

Searches performed across the entire cluster merge data from all systems in the cluster. Searches performed on a specific appliance in the cluster return results for that appliance only.

Quarantine Search

Quarantine is the default search type displayed on the **Search In** sidebar.

The quarantine is a repository of messages whose delivery has been suspended, typically because they were identified as spam or they have violated content rules. The messages in this repository can be searched, examined, and then released, deleted, or forwarded.

Searching the Quarantine

1. Define the search parameters for your quarantined message search by setting one or more of the following:

   Note: The text boxes support string-based searches.

   - **Sender**: Enter a full or partial sender's email address.
   - **Recipient**: Enter a full or partial recipient's email address.
   - **Subject**: Enter a full or partial subject line.
   - **Start Date Range**: Click in the text box to display the *Calendar* (page 198) dialog box. Select a start date and time, and click **OK**.
   - **End Date Range**: Click in the text box to display the *Calendar* (page 198) dialog box. Select an end date and time, and click **OK**.
   - **Relay**: Enter a full or partial hostname or IP address.
   - **Message ID**: Enter a full or partial Message ID. Message IDs are the alphanumeric identifiers assigned to email messages.
   - **Reason**: From the drop-down list, select the reason that the email was quarantined.

2. Click **Search**.
   The findings are displayed in the **Search Results** panel.

Viewing Quarantine Search Results

- Click the up and down arrow buttons beside a search results column heading to order the displayed results alphanumerically by the entry in that column. Click the up and down arrow button again to toggle the results between ascending and descending order.
- If multiple pages of search results are available, use the controls at the bottom of the content panel to view the additional pages.
- Click any of the displayed text about a quarantined message in the search results to view the **Relay**, **Spam Level**, and **Message-ID** for that message.
- To view details of a quarantined message:
  - On the **Search Results** panel, click any text in the row for the message that you want to view. A box with additional information is displayed.
  - In the box, click **View message details**. The *Message Details* (page 203) dialog box is displayed.
  - On the **View** drop-down list, click **Body** or **Headers** to view details.

Managing Quarantined Messages

1. Perform a search.
2. Perform any of the following actions upon the listed messages:
   - To delete quarantined messages:

     Select the check box(es) beside the message(s) that you want to delete, and click **Delete**. The message is deleted and its information is removed from the quarantine and the search results list.
   - To forward quarantined messages:
     1. Select the check box(es) beside the message(s) that you want to delete, and click **Forward**. The *Message Details* (page 203) dialog box is displayed.
     2. In the **Forward to** text box, enter the email address(es), and click **OK**. The message is forwarded to the specified email address, but it is not removed from the quarantine or the search results list.
   - To release quarantined messages:

     Select the check box(es) beside the message(s) that you want to delete, and click **Release**. The message is delivered to its intended recipient and its information is removed from the quarantine and the search results list.

     Note: To delete, forward or release all of the messages on a given **Search Results** page, select the **Select all** check box, and click the appropriate action button.

Logs Search

Select **Mail Logs** from the drop-down list at the top of the **Search In** sidebar to access the logs search parameters. The Logs search allows you to search the mail logs for records of past messages.

The mail logs maintain a record of how messages received in the last thirty days have been handled by the Email Appliance. This provides a means for evaluating the effectiveness of the current mail-filtering policy. Messages listed in the logs can be searched, examined, and released, deleted, or saved. Typical scenarios for why you would want to search and analyze the message logs are:

- You want to check that the policy options that you have set are working as expected.
- A user has reported that a message has not been delivered and wants to know why.

Searching the Mail Logs

1. Define the search parameters for your mail log search by setting one or more of the following parameters:

   Note: The text boxes support string-based searches.

   - **Sender**: Enter a full or partial sender's email address.
   - **Recipient**: Enter a full or partial recipient's email address.
   - **Subject**: Enter a full or partial subject line.
   - **Start Date Range**: Click in the text box to display the *Calendar* (page 198) dialog box. Select a start date and time, and click **OK**.
   - **End Date Range**: Click in the text box to display the *Calendar* (page 198) dialog box. Select an end date and time, and click **OK**.
   - **Client**: Enter a full or partial hostname, or an IP address.
   - **Relay**: Enter a full or partial hostname, or an IP address.
   - **Message ID**: Enter a full or partial Message ID. Message IDs are the alphanumeric identifiers assigned to email messages.
   - **Action**: From the drop-down list, select the action used to filter the message.

2. Click **Search**.
   The results are displayed in the **Search Results** panel.

Viewing Logs Search Results

- To view the log search results:
  - Click the up and down arrow buttons beside a search results column heading to order the displayed results alphanumerically by the entry in that column. Click that up and down arrow button again to toggle the results between ascending and descending order.
  - If multiple pages of search results are available, use the controls at the top of the **Search Results** panel to view the additional pages.
  - Click any of the displayed text about a log entry search result to view detailed routing information for that message in the log entry.

    In the detailed routing information:

    - The first entry is always the initial incoming message, and contains all of the original recipients.
    - Each policy rule hit that results in a message action is displayed with the associated rule name and message action.
    - If a policy rule hit results in an incoming message being routed to a different destination, the outgoing message will be displayed in its own section with the associated policy rule name.
    - If a policy rule hit results in notifications being sent to other addresses, the notification information will be displayed in its own section with the associated policy rule name.

    When you are finished viewing the detailed routing information, click any of the displayed text about that log entry search result again to close the display of that log entry.

Analyzing Message Logs

1. Perform a **Mail Logs** search by setting the search parameters as narrowly as possible to find specific results.
2. Browse the list of search results to find a message log entry that looks like it matches the criteria you seek, and click on that entry to view the details.
3. Look at the end of the message log entry details, which will show the action taken, followed by the reason for that action. The actions are:

- **Quarantine**: Messages are stored in the quarantine.

  Note: Quarantined messages for reason "blacklist" were quarantined as a result of user block lists.

- **Deliver**: Messages are delivered to their intended recipient(s).
- **Discard**: Messages were discarded without notice to the sender.

  Note: Discarded messages for reason "blacklist" were discarded as a result of administrator block lists.

- **Reject**: Messages that were rejected at the MTA level.
- **SPX Encrypt**: Messages that were encrypted using SPX or were sent as notifications of SPX encryption.
- **Route**: Messages that were re-routed to another server using the action specified on the **Main Action** page of the Policy Wizard.

Mail Queues Search

Select **Mail Queues** from the drop-down list at the top of the **Search In** sidebar to access the mail queues search parameters. The Mail Queues search allows you to search the pre-filter queue (messages waiting to be processed by the policy), delivery queue (messages that have been processed by the policy and are waiting to be delivered to the mail delivery server(s)), the delay queue (messages that have been categorized as suspicious, and that are waiting to be rescanned once updated anti-spam definitions become available from Sophos Labs), the Encryption Queue (SPX-encrypted messages waiting to be delivered to Recipient, if SPX password service method is selected as generated by recipient) and the Sandstorm Queue (messages waiting to be analyzed).

With the exception of the delay queue, messages are normally processed so quickly that they will appear in the queue only very briefly. Most entries should have a very recent time stamp, and they should disappear from the results list if you re-run your query. Messages that stay in the pre-filter or delivery queues for a long time are indicative of problems (messages may stay in the delay queue for up to sixty minutes, depending on how it has been configured). Typical problems are the inability to process an incoming message due to an inappropriate "To" address, or the stacking up of messages in the Delivery queue due to a mail delivery server that is down or having processing problems. The mail queue search allows you to examine the messages that are not being processed quickly, and understand the reasons for the processing delay.

Searching the Mail Queues

1. Define the search parameters for your mail queues search by setting one or more of the following:

   Note: The text boxes support string-based searches.

   - **Sender**: Enter a full or partial sender's email address.
   - **Recipient**: Enter a full or partial recipient's email address.
   - **Start Date Range**: Click in the text box to display the *Calendar* (page 198) dialog box. Select a start date and time, and click **OK**.
   - **End Date Range**: Click in the text box to display the *Calendar* (page 198) dialog box. Select an end date and time, and click **OK**.
   - **Queue**: From the drop-down list, select the queue that you want to search. The options are **All**, **Pre-filter**, **Delivery**, **Encryption**, **Delay Queue** or **Sandstorm Queue**.

2. Click **Search**.
   The results are displayed in the **Search Results** panel.

Viewing Mail Queues Search Results

- Click the up and down arrow buttons beside a search results column heading to order the displayed results alphanumerically by the entry in that column. Click that up and down arrow button again to toggle the results between ascending and descending order.
- If multiple pages of search results are available, use the controls at the bottom of the **Search Results** panel to view the additional pages.
- Click any of the displayed text about a mail queue search result to view detailed information for that message. Click any of the displayed text about that mail queue search result again to close the display of the detailed information for that message.

  The detailed information shows the name and IP address of the relay that the message is from (for pre-filter and delay queue messages), or the mail delivery server that the message is going to (for delivery messages). It will also give some indication of why the message is in the queue, although this will only represent a problem if the message has remained in the queue for a long time. For messages in the delay queue, it will also display the planned release time for each message, or indicate that is being rescanned with the "Under rescan" indication.

  Note: Occasionally, "No Information" may be displayed. This indicates that the mail queue was processed so quickly that the message left the queue before the search was finished, and the detailed information for it is no longer available.

Deleting Queued Messages

1. On the **Search Results** panel, select the check box beside the message that you want to delete.
   The **Delete** button changes from grayed out to available.
2. Click **Delete**.
   The message is removed from the mail queue.

   Note: If you try to delete a message from the delay queue that was being rescanned, and it has already been released or quarantined, you will be notified that the message has been expired.

Releasing or Rescanning Queued Messages

1. On the **Search Results** panel, select the check box beside the message that you want to release, or in the case of messages in the delay queue, messages you want to rescan immediately.
   The **Retry** button changes from grayed out to available.
2. Click **Retry**.
   The Email Appliance attempts to release the message. For messages in the delay queue that have not already been rescanned, the appliance will rescan the message(s) with the anti-spam engine with no further delay. If the attempt is successful, the message is released from the mail queue, or, for messages in the delay queue, it may instead be quarantined.

System Status

The **System Status** tab lets you monitor the health and performance of the Email Appliance. By default, only exceptions (warnings or critical alerts) are displayed. If there are no exceptions, the status page shows nothing. To view a complete list of status items, click **Show All** at the bottom right of the tab.

Note: On the **System Status** tab is a **Shutdown** button. If you click this button, a page is displayed with three additional buttons: **Reboot**, **Shutdown**, and **Cancel**.

Each item in the **System Status** panel displays the following information:

- **Status icon**: Shows a color-coded icon that indicates the alert status of the item as one of Normal (green), Warning (yellow), or Critical (red).
- **Monitor**: Names the item that is being monitored.
- **Message**: Provides details of the latest alert.
- **Potential remedies**: Describes possible solutions for the latest alert. In most cases, you are advised to contact Sophos Technical Support.
- **Last exception**: Shows the date in MM/DD/YYYY format and the time in 24-hour format for the latest unacknowledged alert.
- **Exceptions**: Shows the number of exceptions for that item. Click the "note" icon to open the *System Alerts* (page 206) dialog box, which contains a history of alerts for this item. Click **Delete All** to clear the alert(s).

The tab is organized into sections: **Mail Flow**, **Certificates**, **Quarantine**, **Hardware**, **License**, and **Software**.

Mail Flow

The **Mail Flow** section displays the following information:

- **Directory services synchronization**: A warning alert is triggered if there is one instance (or as many as five instances) of the following synchronization failures:
  - recipient aliases
  - groups
  - recipient validation

  A critical alert is triggered if there are six or more failures.
- **Delivery message queue**: A warning alert is triggered if the Email Appliance is having difficulty delivering messages. A critical alert is issued if it is extremely difficult for the appliance to deliver messages. This can occur if the Email Appliance is generating a high number of internal messages or if an external mail server becomes unavailable.
- **Mandatory TLS domains**: (This is only displayed if TLS encryption is enabled.) A warning alert is triggered if the appliance fails to establish a TLS connection for a domain where TLS is required.
- **Pre-filter message queue**: A warning alert is triggered if there is a high number of messages that have yet to be processed. A critical alert is issued if there is an extremely high number of unprocessed messages. This may be due to excessive mail traffic or an issue with the mail filter.
- **SMTP connections**: A critical alert is issued if your appliance has reached its maximum number of connections on port 25. This could result in delays in message processing. It may be the result of excessive mail traffic, or an issue with the mail filter. This condition is often caused by a sudden increase in SMTP connections due to typical day-to-day spikes, or potentially denial-of-service attacks. If this condition persists, consider adding another Sophos Email Appliance to deal with the increased traffic.
- **SPX encryption**: (This is only displayed if SPX encryption is enabled.) A critical alert is issued if there is an error while generating an encrypted PDF. The message is moved to the failed queue, and Sophos Technical Support is notified.
- **SPX encryption queue**: A warning alert is triggered if the number of unprocessed messages in the system is high. A critical alert is issued if the number of unprocessed messages reaches the maximum level. This is either because the password store is unavailable, or the appliance is unable to process messages at a sufficient rate that require encryption .
- **SPX password service**: (This is only displayed if SPX encryption is enabled, and at least some message recipients have the ability to choose their own password.) A failure alert is triggered if there is an error performing SPX password service. A separate alert is issued if the password service is disabled.

Quarantine

The **Quarantine** section displays the following information:

Message store size: When the quarantine disk space is close to capacity, a critical alert is displayed that advises you to contact Sophos Technical Support if the condition persists for more than 15 minutes.

Software

The **Software** section displays the following information:

- **Configuration FTP backup**: (This is only displayed if the appliance is set to create backups using FTP.) A failure alert is displayed if:
  - an invalid FTP hostname was configured.
  - the archive could not be created.
  - the archive could not be uploaded.
- **Connection to Sophos**: A warning alert is triggered after two hours if the Email Appliance is unable to connect to the Sophos site to receive threat definitions or software updates. A critical alert is issued if the Email Appliance is unable to connect to the Sophos site after six hours.
- **Data Installation**: A critical alert is issued if the appliance repeatedly fails to install data updates for 30 minutes. A second critical alert is issued if the appliance fails three times to install data updates.
- **Disk health**: A critical alert is issued if any disk hardware errors have been logged.
- **Process health**: A critical alert is issued if one or more processes is not starting properly.
- **Syslog connection status**: (This is only displayed if the appliance is set to record data using syslog.) A warning is triggered if the connection to the syslog server is lost. A critical alert is later issued if the syslog connection is not restored.
- **Syslog process status**: (This is only displayed if the appliance is set to record data using syslog.) A critical alert is issued if syslog is not running properly.
- **System load**: A warning alert is triggered if the load average rises to an excessively high level. Frequent or persistent system load warnings should be discussed with a Sophos Technical Support engineer.
- **System Reboot**: A warning alert is triggered if there are pending updates that will require a reboot. A critical alert is issued if the system will automatically reboot in the next available update window.
- **System updates**: A critical alert is triggered when a system software update fails or if the software is out of date.
- **Quarantined message archiving**: (This is only displayed if the appliance is set to back up quarantined messages.) A warning alert is triggered if there is an FTP backup failure. A critical alert is later issued if the problem is not addressed.
- **System log file backup**: (This is only displayed if the appliance is set to back up system logs.) A warning alert is triggered if the backup fails. A critical alert is later issued if the problem is not addressed.

Clustered Appliance Alerts

These alerts are only displayed if you are running two or more appliances in a clustered deployment.

- **Cluster Connection**: A critical alert is issued if an appliance in the cluster cannot be reached.
- **Cluster Sync**: A warning is triggered if configuration data cannot be synchronized with one or more appliances.

Virtual Appliance Alerts

This alert only applies if you have installed an appliance as a virtual machine and cloned it. The alert is displayed if you have cloned an appliance using a duplicate system ID.

- **Appliance cloned**: A critical alert is issued whenever a duplicate ID is detected. Once the appliance has been re-registered with a unique system ID, the status returns to normal.

Hardware

Note: There are several alerts that are not displayed on some models due to hardware differences:

1. **Right hard disk** and **Left hard disk**: Some models have only one disk, so disk failure renders the unit inoperable.
2. **Right power supply** and **Left power supply**: Some models have only one power supply, so a power supply failure renders the unit inoperable.
3. **Right power supply fans** and **Left power supply fans**: Some models have only one power supply fan, so a fan failure renders the unit inoperable.

The **Hardware** section displays the following information:

- **CPU**: A critical alert is triggered if there are problems with the appliance CPU that could affect the stability of your system.
- **Disk mirroring**: A warning or a critical alert is triggered, depending on the severity of a problem with the hard disks, that will affect the stability of the Email Appliance.
- **Right hard disk**: A warning alert is triggered if there is a problem with the right hard disk that will affect the stability of the Email Appliance. A critical alert is triggered if the right hard disk fails. This is the rightmost disk when the Email Appliance is viewed from the front. If it becomes necessary to replace this disk, the alert continues to be displayed on the System Status tab until the RAID controller has finished rebuilding the new drive. This could take several hours, depending on the amount of data and the system load at the time.
- **Left hard disk**: A warning alert is triggered if there is a problem with the left hard disk that will affect the stability of the Email Appliance. A critical alert is triggered if the left hard disk fails. This is the leftmost disk when the Email Appliance is viewed from the front. If it becomes necessary to replace this disk, the alert continues to be displayed on the System Status tab until the RAID controller has finished rebuilding the new drive. This could take several hours, depending on the amount of data and the system load at the time.
- **Right power supply**: A warning alert is triggered if the right power supply is removed. A critical alert is triggered when the right power supply is not functioning properly or is disconnected. In both cases, as long as the left power supply is operating normally, the appliance will continue to process mail. This is the rightmost power supply when the Email Appliance is viewed from the rear.
- **Left power supply**: A warning alert is triggered if the left power supply is removed. A critical alert is triggered when the left power supply is not functioning properly or is disconnected. In both cases, as long as the right power supply is operating normally, the appliance will continue to process mail. This is the leftmost power supply when the Email Appliance is viewed from the rear.
- **Right power supply fans**: A critical alert is triggered if one or more of the right power supply fans in the appliance has failed.
- **Left power supply fans**: A critical alert is triggered if one or more of the left power supply fans in the appliance has failed.
- **System fans**: A critical alert is triggered if one or more of the system fans in the appliance has failed.
- **System memory**: A warning alert is triggered if the appliance is consuming over 90% of available physical memory. This may indicate that it is handling unusually heavy mail volumes. Slower mail delivery should be expected.
- **System memory usage**: A warning alert is triggered when 98% of physical memory is used.
- **System temperature**: A warning or critical alert is triggered, depending on how much the appliance exceeds its normal temperature range.
- **System voltage**: A warning or critical alert is triggered, depending on how far outside of its normal voltage range the appliance is operating.

License

The **License** section displays the following information:

- **Sophos license**: A warning alert is triggered twice a week when the Email Appliance license is 30 days from expiry. A critical alert is triggered every day when the Email Appliance license is 7 days away from expiry.
- **Sophos SPX trial license** : A warning alert is triggered if the SPX trial period is nearing the end. A critical alert is issued if the appliance's SPX trial license has expired.
- **Sophos Sandstorm trial license** : A warning alert is triggered if the Sandstorm trial period is nearing the end. A critical alert is issued if the appliance's Sandstorm trial license has expired.

Using Help

The help system provides several tools for getting answers quickly while using the Email Appliance. On the sidebar, click the title of any of these utilities to access them.

- **Search:** Provides full text search of the Email Appliance help.
- **Table of Contents:** Provides a collapsible sidebar of hierarchically organized links to the sections of the Email Appliance help.
- **Sophos Support:** Provides a form for quick submission of a Sophos Technical Support request, as well as a mechanism for establishing a remote assistance session for Sophos support engineers. Only System administrators have access to this feature.
- **About:** Lists Email Appliance license information and links to other legal information. Only System administrators have access to this feature.

Searching the Documentation

1. In the **Search** text box, type the query.

   The following search refinements are supported:

   - To match phrases, set the phrase in double quotation marks.
   - To use Boolean operators, type in "AND", "OR", or "AND NOT" in uppercase letters.
   - Prepend a plus sign (+) to a term to require the presence of that term.
   - Prepend a minus sign (-) to a term to require the absence of that term.

2. Press **Enter** or click the arrow button to the right of the **Search** text box.

   The results are displayed in the text box that usually displays the **Table of Contents**. The search results have the following features:

   - Results are sorted by relevance.
   - Excerpts of the search results are displayed to help you assess the relevance of each result, and the search terms are highlighted.

3. Click on the page title of any search result to display that page in the content pane.

Using the Table of Contents

The **Table of Contents** is displayed in the scrollable box on the sidebar.

To use the table of contents:

1. Click on the title, **Table of Contents**, to refresh the table of contents list in the scrollable box or to re-display the table of contents after using the *Searching the Documentation* (page 165).
2. Click on the name of any section of the help in the table of contents list to display that section of the help in the content pane.

Getting Assistance

Note: Only System administrators have access to this feature.

The **Sophos Support** item on the sidebar provides two options for getting help from Sophos Technical Support. You can either submit a support request via email, or you can enable remote assistance to your system via an outbound SSH (secure shell) connection to Sophos Support Services.

Requesting Support by Email

To file a Sophos Technical Support request via email:

1. On the Email Appliance help window sidebar, click **Sophos Assistance**
   The **Sophos Assistance** form appears in the content panel.
2. In the **Support request via email** section, enter the following information:
   - **To**: "esasupport"
   - **Name**: your name
   - **Email Address**: your email address
   - **Company Name**: name of the organization to which the Email Appliance is registered
   - **Subject**: short descriptive subject line for the issue
   - **Additional Info**: information that is significant to understanding the problem
3. Once you have filled in all of the required and relevant information, click **Submit** to email the request.

Enabling/Disabling Remote Assistance

- To open a remote assistance session to Sophos Technical Support:

  Note: You should only open a remote assistance session when instructed to do so by a Sophos Technical Support engineer.

  1. On the Email Appliance **Help** window sidebar, click **Sophos Support**.

     The **Sophos Assistance** form is displayed in the content pane.
  2. In the **Enable/disable remote assistance** section, click **Enable** to establish the connection.

     A message is displayed on the status information bar (at the top of the administrator interface) that states "Remote assistance CONNECTED" while an outbound secure connection to Sophos Support Services is open. This connection will be closed by the Sophos Technical Support engineer who is working on your assistance request, or the session will be closed automatically within 72 hours. When the session is closed, the connection message will disappear from the status information bar.

- To close a remote assistance session to Sophos Technical Support:

  1. On the Email Appliance **Help** window sidebar, click **Sophos Support**.

     The **Sophos Assistance** form is displayed in the content pane.

2. In the **Enable/disable remote assistance** section, click **Disable** to terminate the connection. The "Remote Assistance CONNECTED" indicator on the status information bar (at the top of the administrator interface) is no longer displayed. The connection must remain open until Sophos Technical Support has finished working on your assistance request. If you disable remote assistance while a Support engineer is still troubleshooting your request, the connection will be terminated. The session will be closed automatically within 72 hours, but you can close it at any time.

Viewing License/Version Information

Note: Only System administrators have access to this feature.

1. Click **About** on the sidebar to display the following information:
   - Number of users licensed to use the Email Appliance
   - License term
   - License expiry date for the Email Appliance
   - The version number of the Email Appliance software engine
   - The date and version number of the Email Appliance threat definitions package
   - A brief copyrights and trademarks statement

Appendix

This Appendix includes supplemental information related to your Email Appliance.

Setup and Configuration Guide

Introduction

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. 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.

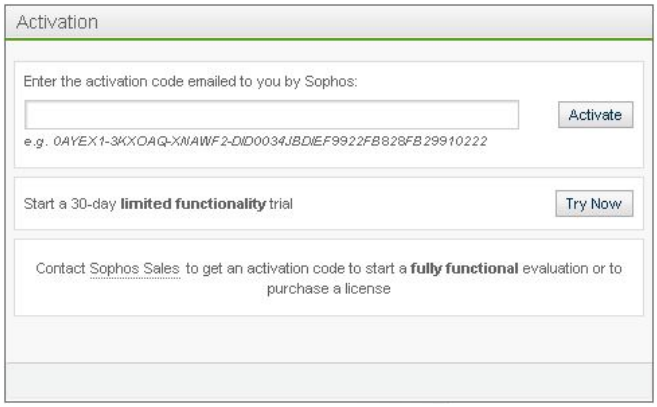
Initial Configuration

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.

Activating the Email Appliance

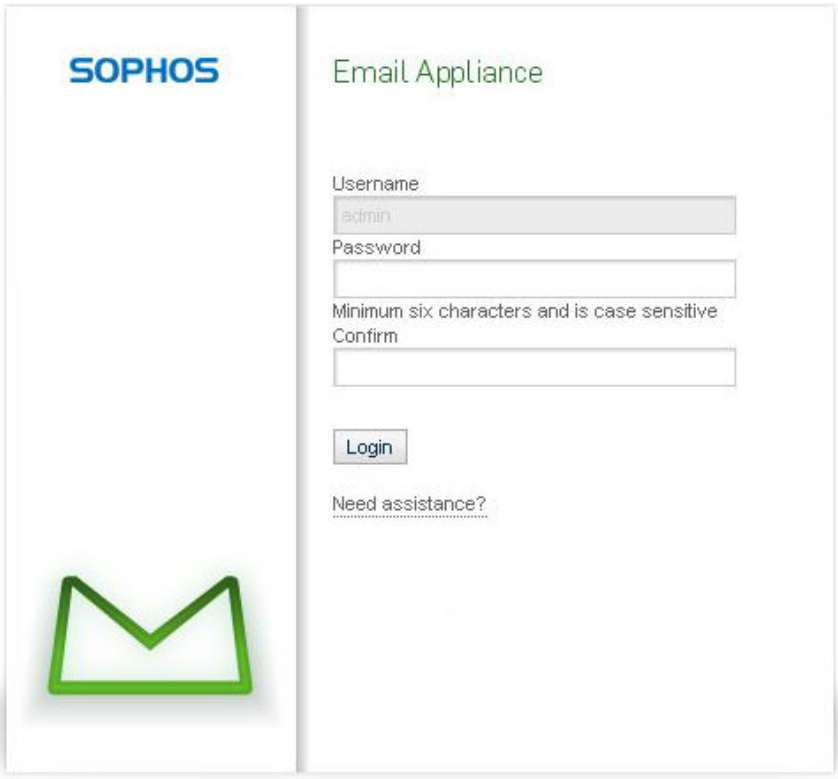
1. Using a supported web browser, connect to: `https://172.24.24.172`

   The Activation page is displayed.



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**.

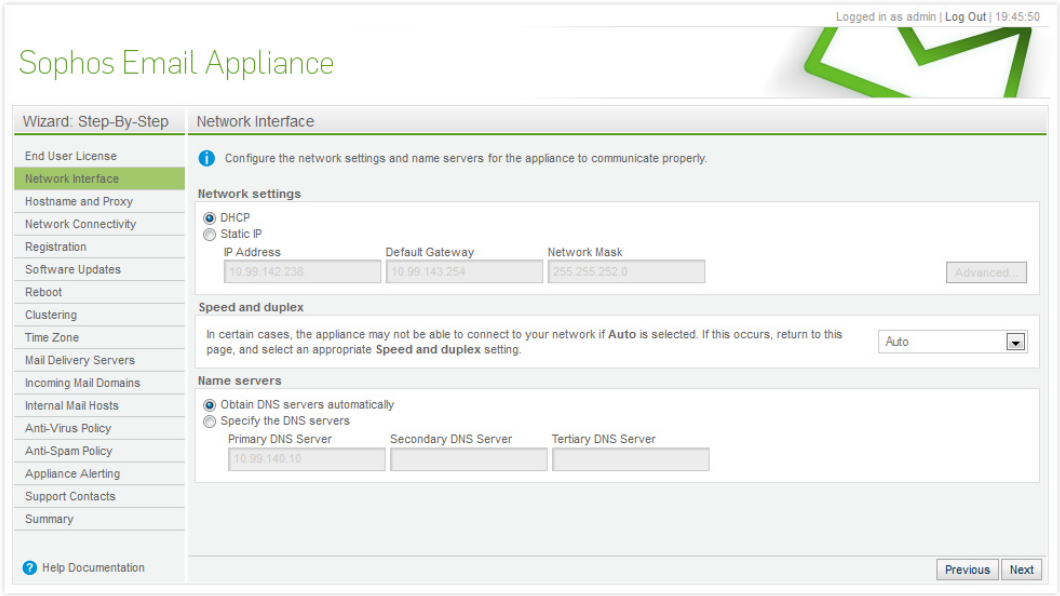
   The login page is displayed.



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.

Network Interface

The Email Appliance's network settings and name servers are configured on the Network Interface page of the wizard.



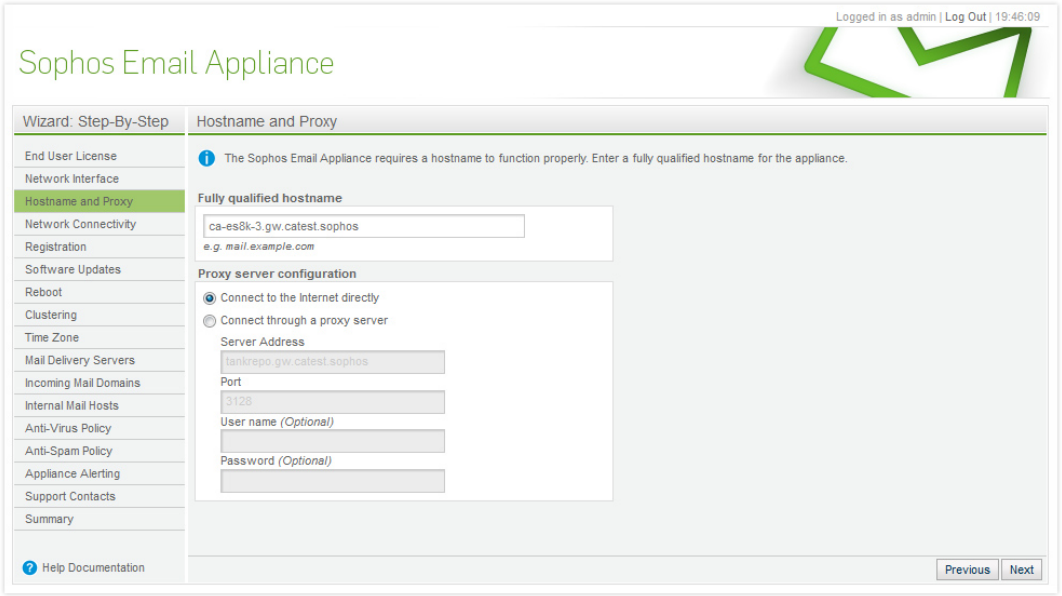
To configure network interface settings:

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*:
     1. In the **IP Address** text box, enter the address for the appliance.
     2. In the **Default Gateway** text box, enter the address of an external gateway server.
     3. In the **Network Mask** text box, enter the mask (for example, 255.255.0.0).
     4. [Optional] Click **Advanced** to open the *Additional Network Routes* (page 201) 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* (page 170) configuration page.

Hostname and Proxy

You must assign a hostname for the Email Appliance. Additionally, if you plan 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.

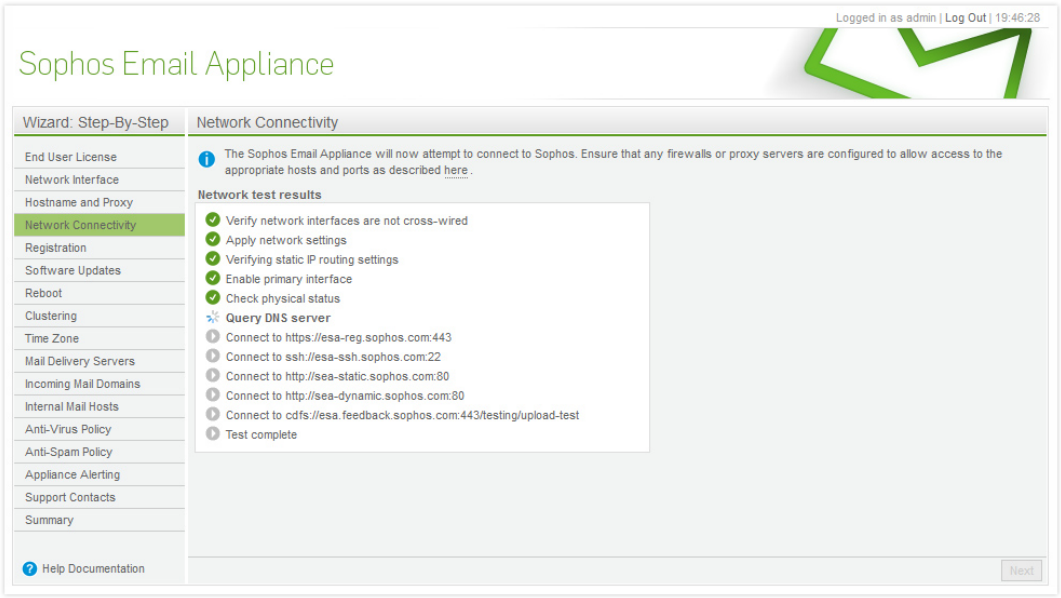


2. In the **Proxy server configuration** section, do one of the following:
   - If you plan to connect to the internet directly, accept the default setting.
   - If you plan to connect to the internet via a proxy, select **Connect through a proxy server**, specify a **Server Address** using a hostame 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 171) page.

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.

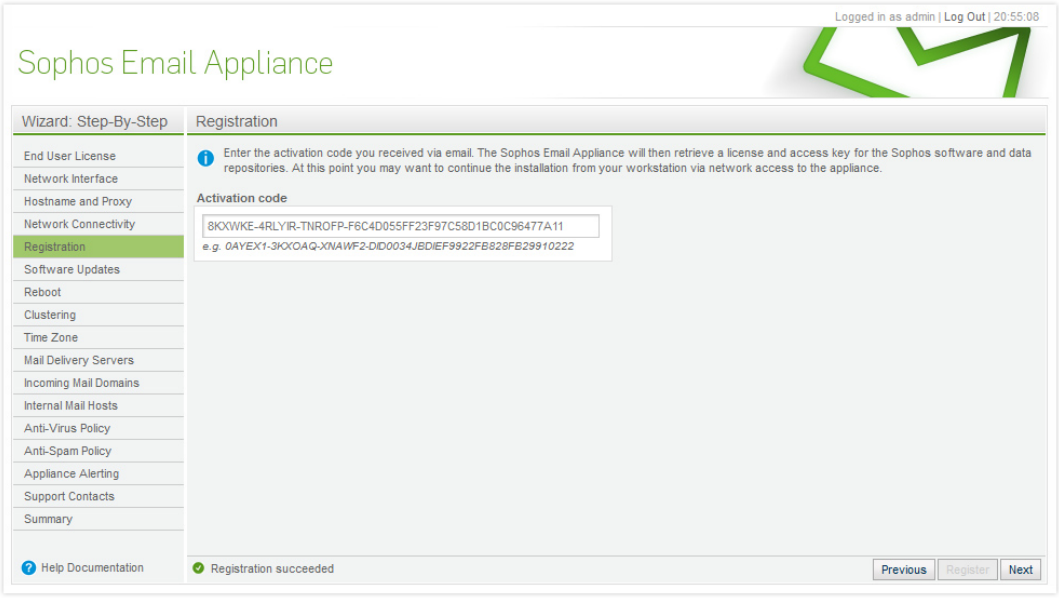


When the test has completed successfully, click **Next** to proceed to the wizard's *Register and Update* (page 171) page.

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.)

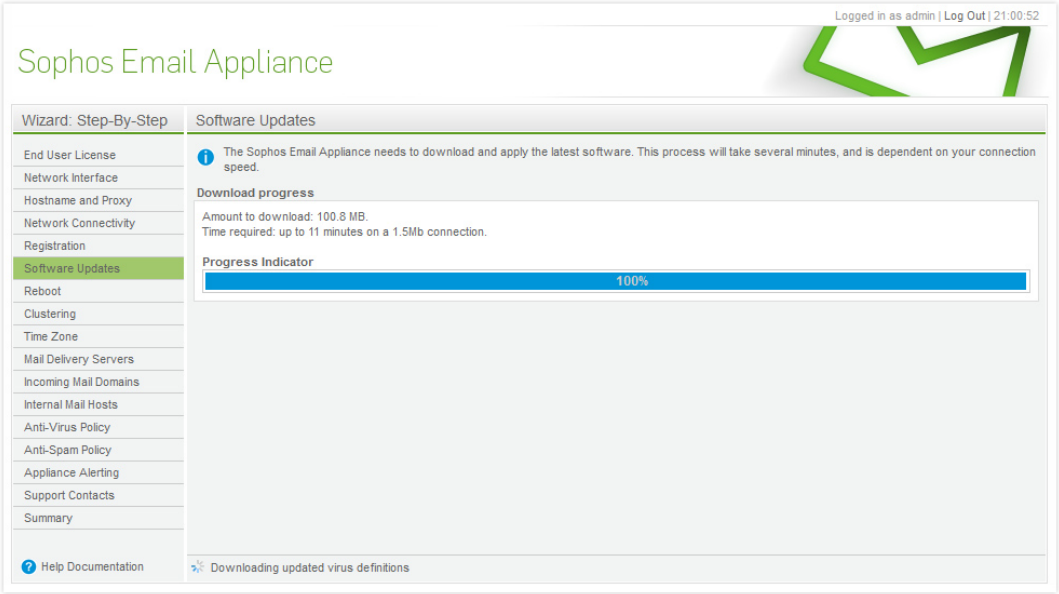


b) Click **Register**.
If registration is successful, a message is displayed in the status bar.

c) Click **Next**.

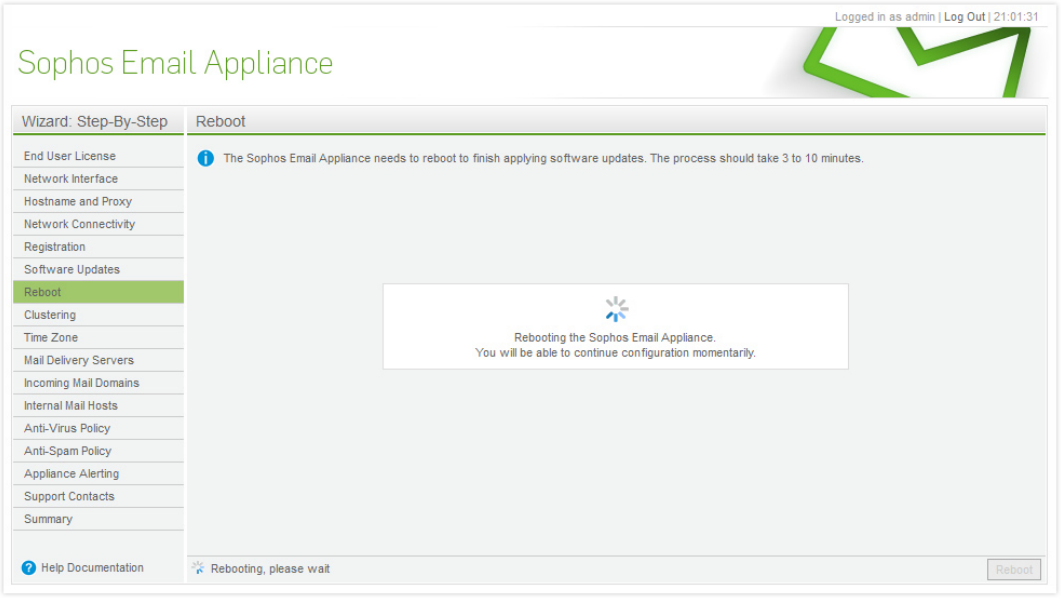
- To get the latest threat definitions and software updates:

a) Click **Update**.



The progress bar is displayed while the update time is calculated. Once updating is complete, the Email Appliance will request a reboot.

b) Click **Reboot**.



c) Following the reboot, click **Next** to proceed to the wizard's *Clustering* (page 173) page.

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 173) page.

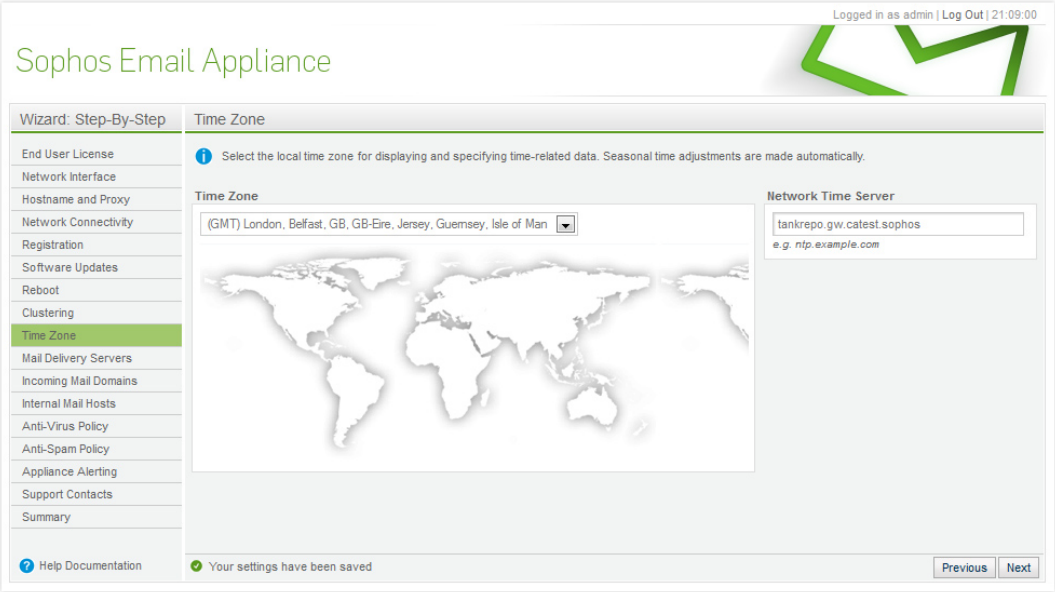
Configuring clustering is only an option if you have two or more Sophos appliances. The appliances must also have identical software versions, be connected to the same network, and have the ability to communicate via port 24 over both UDP and TCP.

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.

Time Zone

1. From the drop-down list, select the appropriate time zone for your region.



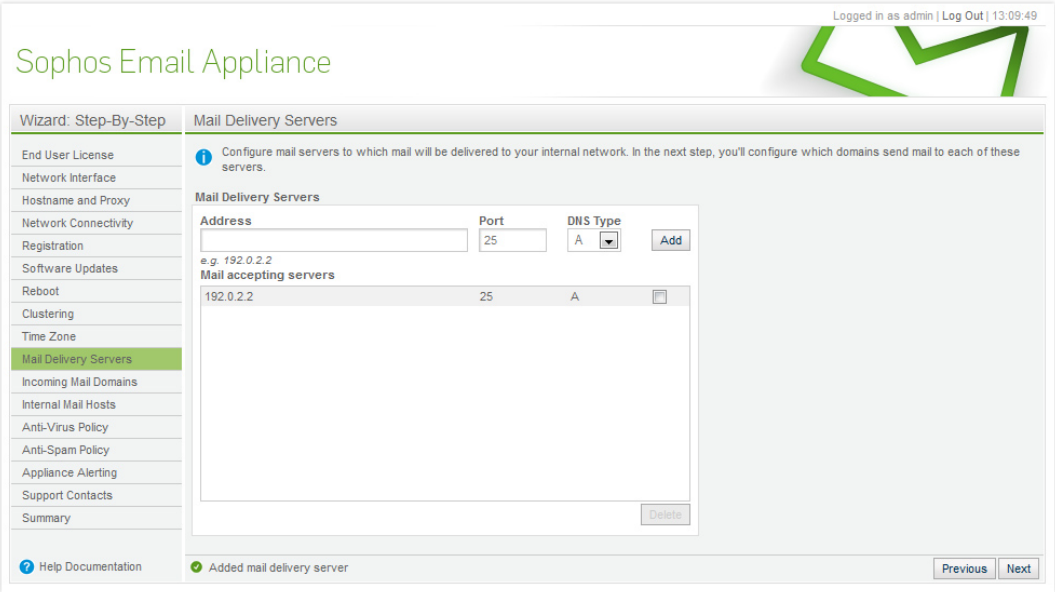
2. In the **Network Time Server** text box, enter the hostname of the Network Time Protocol (NTP) server from which you want to read the precise time of day or accept the default entry. This text box cannot be blank.
3. Click **Next** to proceed to the wizard's *Mail Delivery Servers* (page 174) page.

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**.

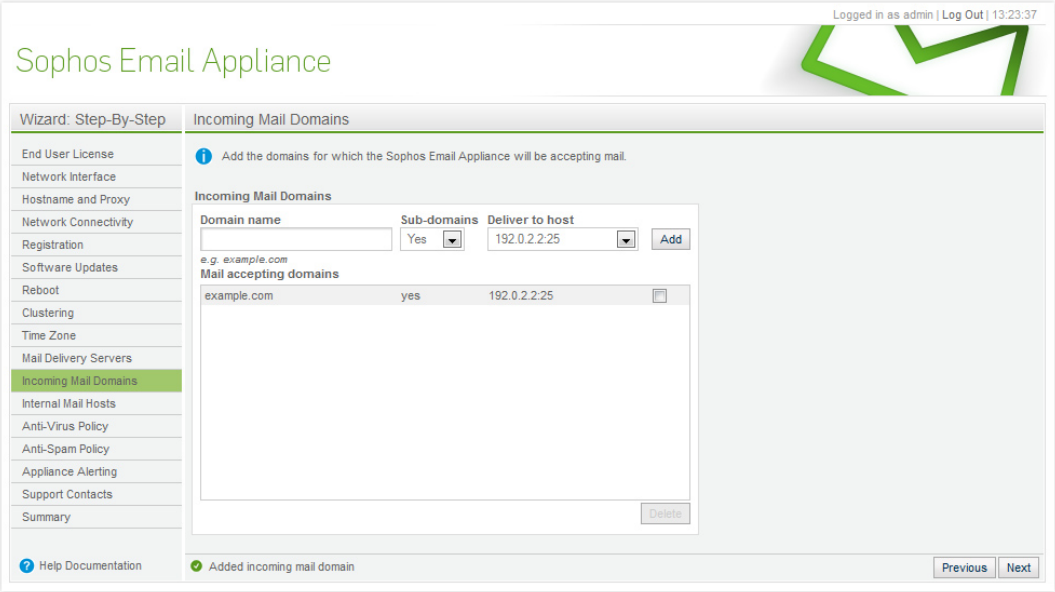
4. Click **Add** after each entry.
   Entries are displayed in the **Mail Delivery Servers** list. To remove a server from the list, select the check box beside the entry, and click **Delete**.
5. When you have finished adding servers, click **Next** to proceed to the *Incoming Mail Domains* (page 175) page of the wizard.

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.



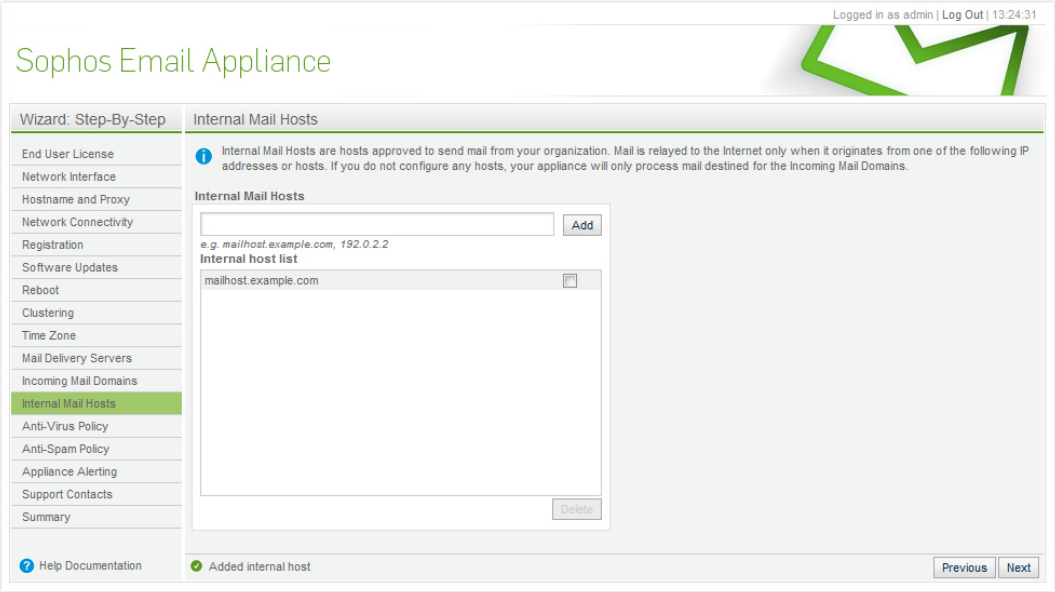
2. On the **Sub-domains** drop-down list, select **Yes** or **No**, depending on whether you want the host to accept mail bound for sub-domains as well.
3. On the **Deliver to host** drop-down list, enter the IP address of the machine.
4. Click **Add** after each entry.
   Entries are displayed in the **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 175) page.

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 176) page.

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 178) page.
   - *To configure advanced settings*: Select **Advanced Configuration**, and click **Next** to proceed to the configuration pages for inbound and outbound anti-virus settings.

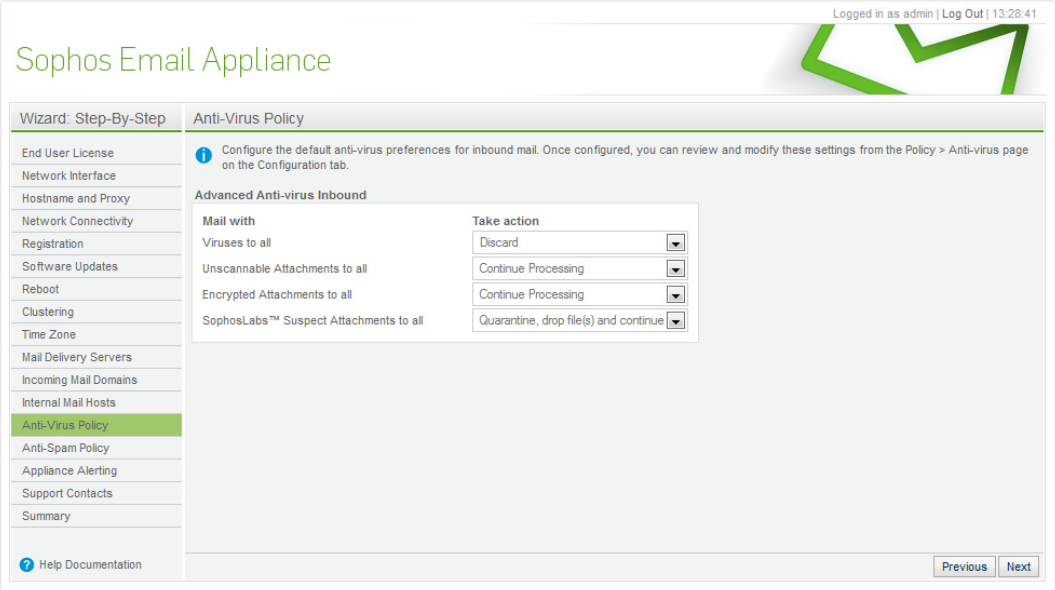
   There are five threat categories that apply to both inbound and outbound messages:

   - **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

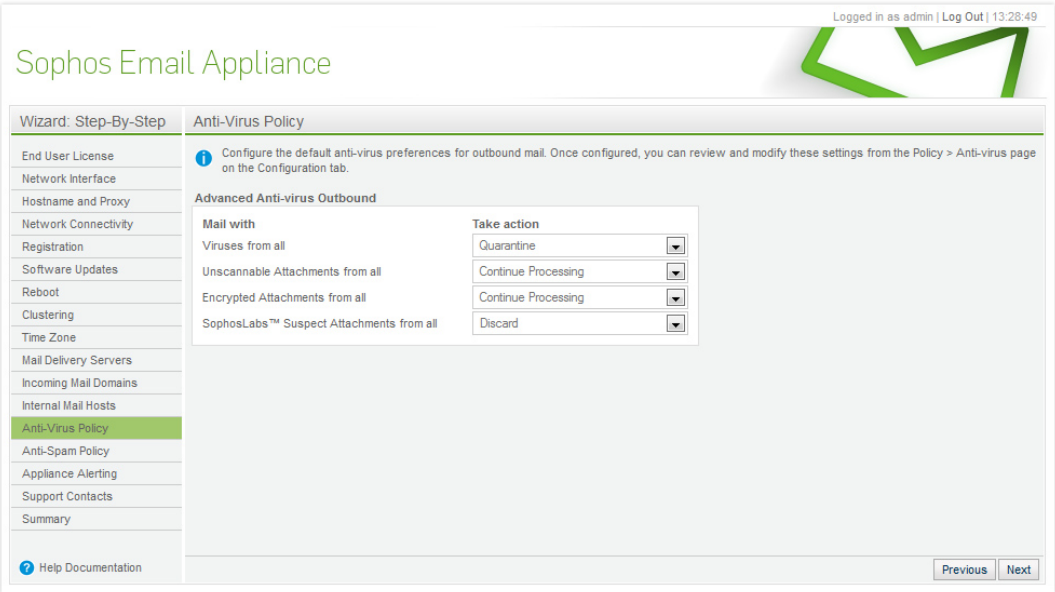
were identified and removed. A list of attachment types can be configured by clicking the **Restricted Attachments** link.

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).

Anti-Virus Inbound Advanced



Anti-Virus Outbound Advanced



Choose from the following actions:

- **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.

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 178) page.

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.

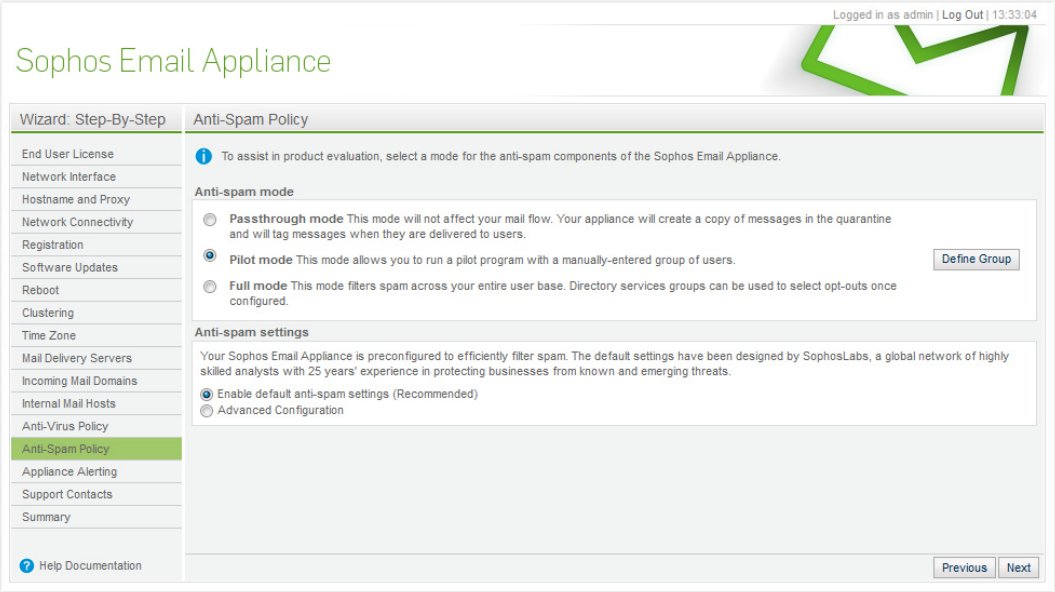
To configure anti-spam settings:

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 to 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* (page 200) 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.



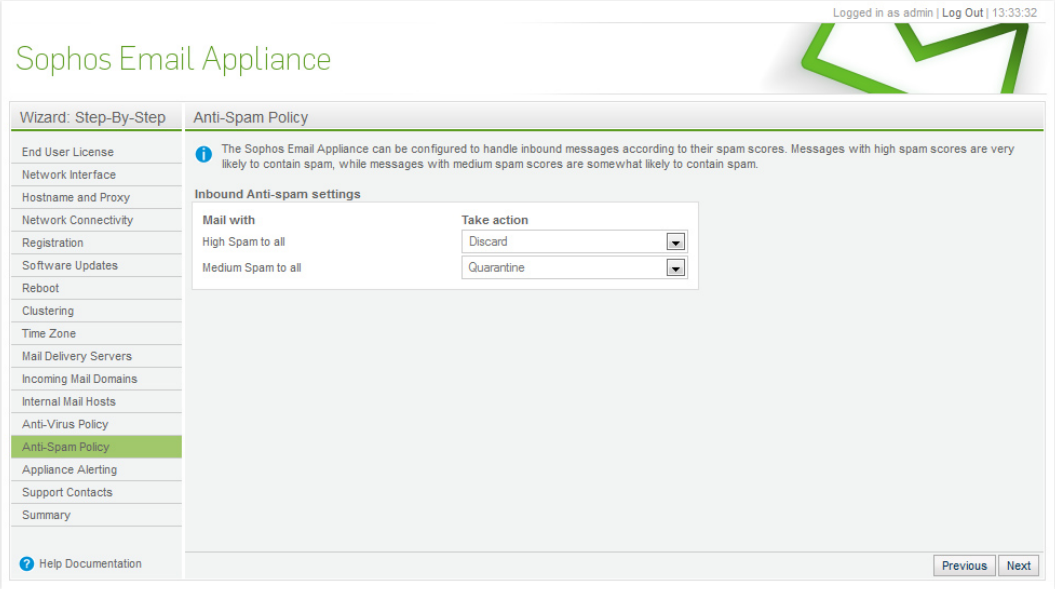
2. Choose one of the following basic anti-spam configuration options:

   - *To accept the default settings*: Leave **Enable default anti-spam settings** selected, and click **Next** to proceed directly to *Appliance Alerting* (page 180).

     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.

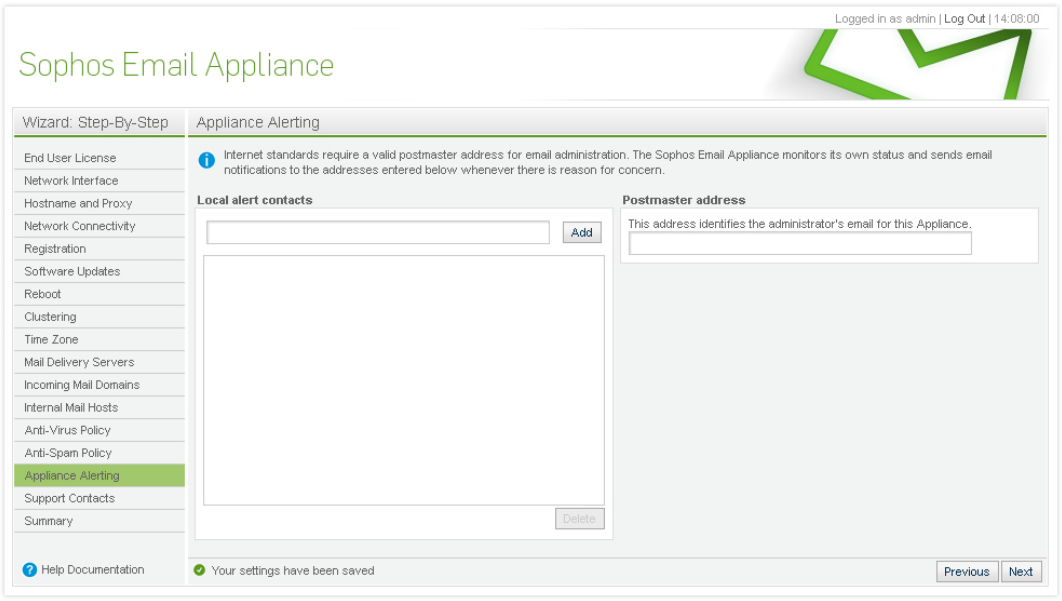
4. When you have finished configuring advanced anti-spam settings, click **Next** to proceed to *Appliance Alerting* (page 180).

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.



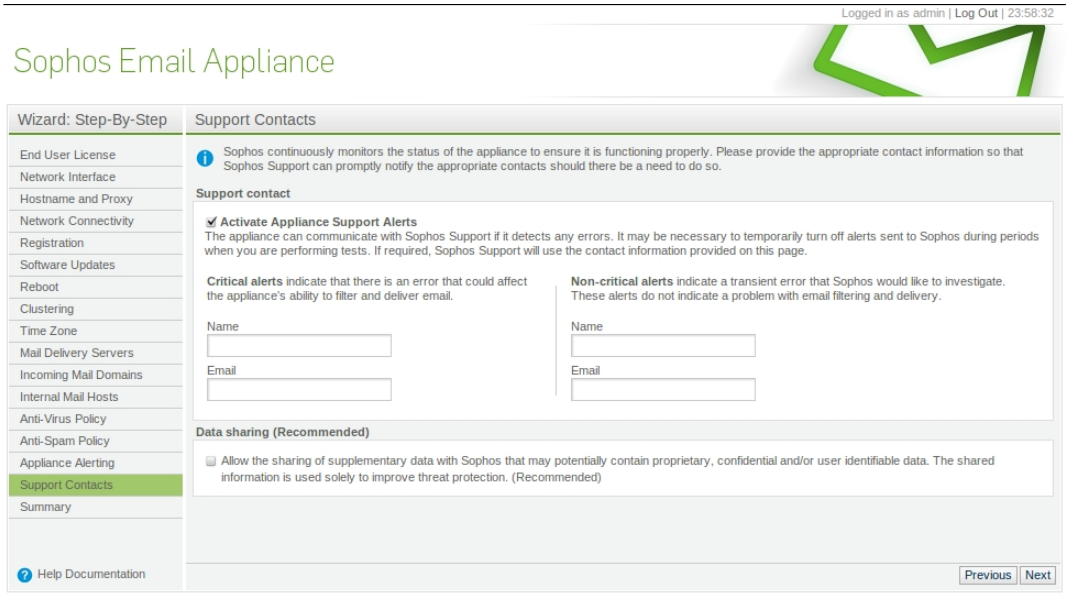
2. To configure alert recipients:
   a) In the **Local alert contacts** text box, enter the recipient email addresses.
   b) Click **Add** after each entry.
   Entries are displayed in the list of alert contacts.

   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 180) page.

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:

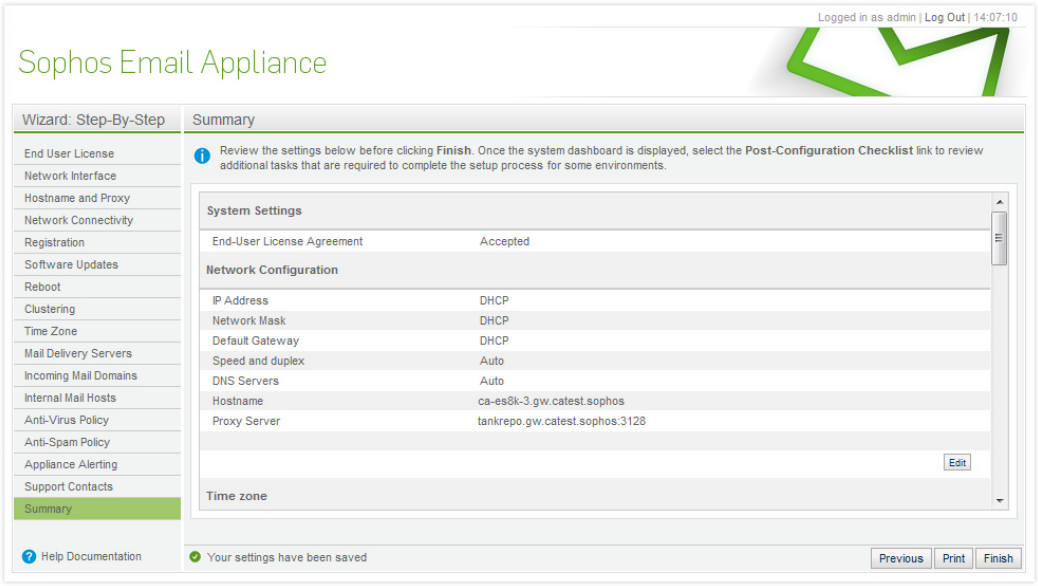
1. Select the **Activate Appliance Support Alerts** check box.
   The grayed out features below become available.
2. For **Critical alerts**, provide the **Name** and **Email** of the person who should receive these messages.
3. For **Non-critical alerts**, provide the **Name** and **Email** of the person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

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**.

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.

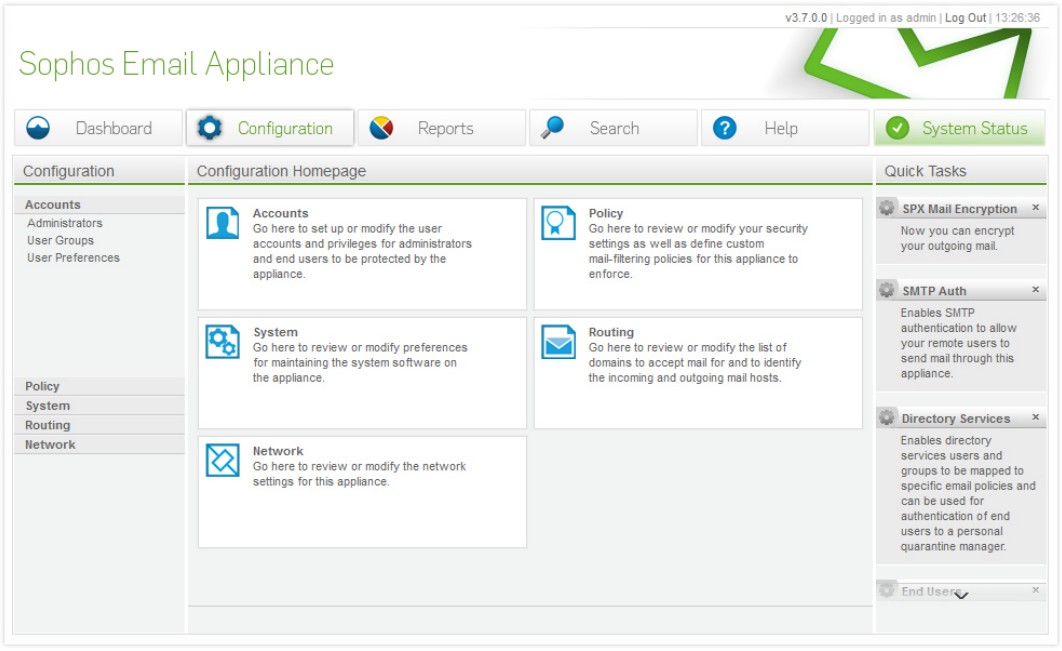
Immediately after you exit the setup wizard, the **Dashboard** tab of the appliance's administrative interface is displayed.

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.

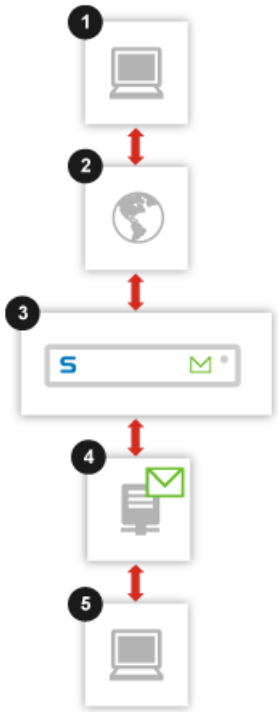
Testing Appliance Mail Flow

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.

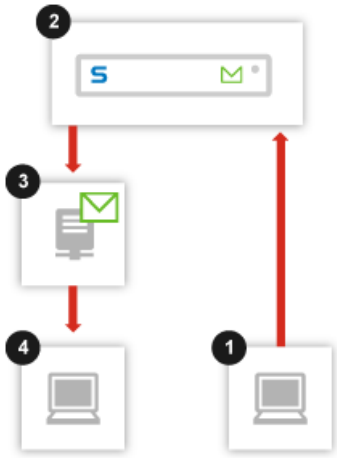
Testing a Fully Networked Appliance



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



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

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.

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:

   1. Check the internal email account to verify that the message was received.
   2. 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:

   1. Check the external account to verify that the message was received.
   2. 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.

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:

   1. Check the recipient account to verify that the message was delivered.
   2. 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.

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 integerated with other LDAP implementations. If you will not be using any form of LDAP, proceed to *Configuring User Preferences* (page 185).

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:

1. On the **Quick Tasks** sidebar of the **Configuration Homepage**, click **Directory Services**.
   The **System: Directory Services** page is displayed.
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 *Configuring User Preferences* (page 185).

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* (page 185)). 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 *Configuring Internal Mail Hosts/Outbound Mail Proxy* (page 186) task.

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 *Configuring Trusted Relays* (page 187) 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 *Configuring Trusted Relays* (page 187) task.

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**.

Configuration of Ports

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

These services are typically used for connections between your Email Appliance(s) and locations outside of your organization's network.

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

Internal Connections

These services are typically used for connections within your organization's network and your Email Appliance(s), or between appliances themselves, if you have multiple appliances.

Port	Function	Service	Protocol	Connection
20, 21	FTP backup	FTP	TCP	Outbound from appliance to FTP server
24	Clustering	SSH	TCP/UDP	Inbound/outbound between clustered appliances
25	Mail transfer	SMTP	TCP	[Required] Inbound/outbound between appliance and intranet
53	DNS services	DNS	UDP	Outbound from appliance to DNS server
161	SNMP monitoring	SNMP	TCP/UDP	Inbound from SNMP monitoring server(s) to appliance
162	SNMP traps	SNMP	TCP/UDP	Outbound from appliance to SNMP monitoring server(s)
389, 3268, (636, 3269)	Directory services synchronization	LDAP(S)	TCP	Outbound from appliance to directory server

Port	Function	Service	Protocol	Connection
443/10443 (redirect from 80)	End User Web Quarantine	HTTPS	TCP	Inbound from intranet to appliance (selectable)
5432	Database functions	Encrypted SQL	TCP/UDP	Inbound/outbound between clustered appliances
18080	Administration user interface and clustered UI functions	HTTPS	TCP	[Required] Inbound/outbound between appliance and intranet
8888	Delay Queue	DB Sync	TCP	Inbound/outbound Delay Queue database sync between clustered appliances

Supported Browsers

Browsers supported by the Email Appliance

- Internet Explorer 7.0 and later
- Firefox 4.x and later
- Google Chrome 37.x and later
- Safari 5 and later
- Opera 25.x and later
- Chromium 48 and later

Note: If you are using an earlier browser version and experience performance issues, consider upgrading to a newer version of the browser.

Creating a Custom Web Service for SPX

You can create a web service that integrates with your existing authentication system to issue SPX passwords. For information on how to create a custom web service, you should consult *the relevant knowledgebase article*.

Note: Sophos Technical Support does not officially support the development of custom web services. For additional assistance with customization, contact your account manager to receive guidance from Sophos Professional Services.

Template Variables

Certain predefined policy variables are available for use in banners and headers. Others can be used only with certain types of rules. In addition, there are variables that are designed specifically for use in the SPX Template wizard.

Global Policy Variables

The following variables can be used in banners and headers associated with any policy rule. To add banner or header text, use the **Additional Message Actions** dialog box, which is opened from the **Additional Actions** page of the wizard.

- **%%ESA_VERSION%%**: The version of the Sophos Email Appliance.
- **%%SUBJECT%%**: The subject of the message. If there are multiple Subject headers, only the last occurrence is used.
- **%%MESSAGE_SIZE%%**: The size of the message, in bytes.

- **%%QUEUE_ID%%**: The mail transfer agent's queue ID.
- **%%SENDER_IP%%**: The IP of the connecting MTA.
- **%%DATETIME_GMT%%**: A string containing the GMT date and time (for example, Sat Apr 24 12:49:28 2010).
- **%%ENVELOPE_TO%%**: A comma-separated list of the envelope recipients.
- **%%ENVELOPE_FROM%%**: The envelope sender.
- **%%HEADER_FROM%%**: The From field of the message header.
- **%%HEADER_TO%%**: The To field of the message header. All occurrences of the To field are returned in a comma-separated list.
- **%%HEADER_CC%%**: The Cc field of the message header. All occurrences of the Cc field are returned in a comma-separated list.
- **%%HEADER_DATE%%**: The Date field of the message header.
- **%%HOSTNAME%%**: The system's hostname as returned by the system hostname command. Useful in multi-system deployments for identifying which appliance processed a given message.

Other Policy Variables

The following variables can only be used after a spam probability test has been performed:

- **%%HITS%%**: A listing of all the rules that were found by the spam engine.
- **%%SPAM_REPORT%%**: A verbose listing of the antispam rules triggered by the message.

The following variables are available in keyword list rules and offensive language rules:

Note: If there are multiple matches in multiple files, only the last text match and the last scanned file that matched will be stored in these variables.

- **%%MATCHED_TEXT%%**: Provides the text that triggered the rule.
- **%%MATCHED_FILE%%**: Provides the file that triggered the rule.

The following variable is available after a message has been tested for a virus.

- **%%VIRUS_IDS%%**: IDs of viruses detected in the message (for example, 'W32/Klez.h@MM').

The following variable provides a comma-and-space delimited list of all attachments:

- **%%ATTACHMENT_NAMES%%**: Is available in the following rules that test for attachments:
  - "Message contains a virus" rule in **Config ➤ Policy ➤ Anti-Virus** .
  - "Encrypted attachment" rules in **Config ➤ Policy ➤ Anti-Virus** .
  - "Suspect attachment" rules in **Config ➤ Policy ➤ Anti-Virus** .
  - "Attachment name list" in **Config ➤ Policy ➤ Content** .
  - Any rule that specifies a message attribute for attachment size.

The following variable provides a list of all matches that caused a Content Control Rule (CCL) to trigger:

- **%%CCL_MATCHES%%**: Is available in data control rules that use CCLs. These can be configured in **Config ➤ Policy ➤ Data Control** .

Secure PDF Exchange (SPX) Variables

These variables are available for use on specific pages of the SPX Template wizard. As described the below, the available variables differ, depending on which text you are editing. The %%CHANGE_PASSWORD_URL%% and %%FORGOTTEN_PASSWORD_URL%% are automatically inserted in the instructional text if the associated end user password options are selecting when creating a new template.

SPX Instructional Text

Use any of the following variables on the **Recipient Instructions** page of the SPX Template wizard. The %%CHANGE_PASSWORD_URL%% and %%FORGOTTEN_PASSWORD_URL%% are automatically inserted in the instructional text, if the associated end user password options are selected when creating a new template.

- **%%SUBJECT%%**: The subject of the message. If there are multiple Subject headers, only the last occurrence is used.
- **%%DATETIME_GMT%%**: A string containing the GMT date and time (for example, Sat Apr 24 12:49:28 2010).
- **%%ENVELOPE_TO%%**: A comma-separated list of the envelope recipients.
- **%%ENVELOPE_FROM%%**: The envelope sender.
- **%%HEADER_TO%%**: The To field of the message header. All occurrences of the To field are returned in a comma-separated list.
- **%%HEADER_CC%%**: The Cc field of the message header. All occurrences of the Cc field are returned in a comma-separated list.
- **%%HEADER_FROM%%**: The From field of the message header.
- **%%HEADER_FROM_SANITIZED%%**: The From field of the message header, in a readable format similar to *User Name <name@example.com>*
- **%%ORGANIZATION_NAME%%**: The name of your company or institution as specifed in the **Organization name** text box on the **Template Name** page of the SPX Template wizard.
- **%%ATTACHMENT_COUNT%%**: The number of attachments included with the message.
- **%%ATTACHMENT_NAMES%%**: A comma-and-space delimited list of all attachments.
- **%%CHANGE_PASSWORD_URL%%**: The URL to the web portal where an SPX recipient can change their password.
- **%%FORGOTTEN_PASSWORD_URL%%**: The URL to the web portal where an SPX recipient can recover their forgotten password.

SPX Registration Message

Use any of the following variables on the **Password Settings** page of the SPX Template wizard if you have opted to let recipients choose their own passwords. When you select this password method, the wizard inserts the %%REGISTRATION_URL%%, %%ORGANIZATION_NAME%%, and %%HEADER_FROM_SANITIZED%% variables in the registration message text.

- **%%DATETIME_GMT%%**: A string containing the GMT date and time (for example, Sat Apr 24 12:49:28 2010).
- **%%ENVELOPE_TO%%**: A comma-separated list of the envelope recipients.
- **%%ENVELOPE_FROM%%**: The envelope sender.
- **%%HEADER_TO%%**: The To field of the message header. All occurrences of the To field are returned in a comma-separated list.
- **%%HEADER_CC%%**: The Cc field of the message header. All occurrences of the Cc field are returned in a comma-separated list.
- **%%HEADER_FROM%%**: The From field of the message header.
- **%%HEADER_FROM_SANITIZED%%**: The From field of the message header, in a readable format similar to *User Name <name@example.com>*
- **%%ORGANIZATION_NAME%%**: The name of your company or institution as specifed in the **Organization name** text box on the **Template Name** page of the SPX Template wizard.
- **%%REGISTRATION_URL%%**: The URL to the web portal where an SPX recipient can choose a password.

SPX Generated Password Message

Use any of the following variables on the **SPX password email** dialog if you have opted to generate passwords or use sender-specified passwords, and to have the sender communicate passwords to recipients. When you select this password method, the wizard inserts the %%GENERATED_PASSWORD%% variable for generated passwords, or the %%SPECIFIED_PASSWORD%% variable for sender-specified passwords in the instructional text. The %%ENVELOPE_TO%% variable will also be inserted in the instructional text.

- **%%SUBJECT%%**: The subject of the message. If there are multiple Subject headers, only the last occurrence is used.
- **%%DATETIME_GMT%%**: A string containing the GMT date and time (for example, Sat Apr 24 12:49:28 2010).
- **%%GENERATED_PASSWORD%%**: [Only when using generated passwords] The automatically generated password that must be securely communicated to the message recipient.

- **%%SPECIFIED_PASSWORD%%**: [Only when using sender-specified passwords] The sender-specified password that must be securely communicated to the message recipient.
- **%%ENVELOPE_TO%%**: A comma-separated list of the envelope recipients.
- **%%ENVELOPE_FROM%%**: The envelope sender.
- **%%HEADER_TO%%**: The To field of the message header. All occurrences of the To field are returned in a comma-separated list.
- **%%HEADER_CC%%**: The Cc field of the message header. All occurrences of the Cc field are returned in a comma-separated list.
- **%%HEADER_FROM%%**: The From field of the message header.
- **%%HEADER_FROM_SANITIZED%%**: The From field of the message header, in a readable format similar to *User Name <name@example.com>*
- **%%ORGANIZATION_NAME%%**: The name of your company or institution as specifed in the **Organization name** text box on the **Template Name** page of the SPX Template wizard.
- **%%ATTACHMENT_COUNT%%**: The number of attachments included with the message.
- **%%ATTACHMENT_NAMES%%**: A comma-and-space delimited list of all attachments.

Password Option/Template Variable Mismatches

A warning message was displayed because you have edited the text on the **Recipient Instructions** page of the SPX Template Wizard, and it no longer matches the end user password options selected on the **Password Options** page of the wizard.

The end user password options that you select must match the template variables included in the recipient instructions text. If there is a mismatch, an error message is displayed whenever you attempt to save changes to the template. See “Password Settings” and “Recipient Instructions” in the SPX Template Wizard documentation for more information.

Dialog Box Help

The following pages describe the various pop-up dialog boxes that are used throughout the Email Appliance administrator web interface. The documentation for each dialog box provides instructions for its use and includes descriptions of and links to the GUI pages from which the dialog box is launched.

Note: These entries are provided for reference only. See the appropriate procedure in the Configuration, Reports, Search, System Status, and Using Help section of the documentation for information about how each of these dialog boxes is used.

Directory Services Groups

The **Directory Services** dialog box is displayed if you click **Add** in the **Select groups from Directory Services** table on the **Configuration ➤ Accounts ➤ User Groups** page.

To manage which directory services groups are used in the Email Appliance:

1. From the **Directory Server** drop-down list, choose the server for which you want to select groups.
2. Choose the directory services groups that you want to add to the **Selected groups** list by doing the following:
   - Add groups to the **Selected groups** list by selecting one or more groups in the **Available groups** list box and clicking the "Add" (>) arrow.
   - Remove groups from the **Selected groups** list by selecting one or more groups in the **Selected groups** list box and clicking the "Remove" (<) arrow.
3. Click **OK**.

Add Certificate Authorities

The **Add Certificate Authorities** dialog box is displayed if you click **Add** in the **Locally managed** tab on the *Trusted Certificate Authorities* (page 206) dialog box.

To add a certificate authority:

1. Type a **Description**. This is the name that will be displayed in list of trusted certificate authorities.
2. In the **Paste certificate text** text box, paste the text of a valid certificate
3. Alternatively, upload a **valid certificate** by selecting **Import certificate file**, then clicking **Browse**.
4. Click **OK**.

Note: A certificate of any size can be used, provided it is in **PEM** or **PKCS#12** format, and is of a **cipher type** supported by the Email Appliance.

Complete CSR

To complete a CSR:

1. Upload the certificate and private key you have obtained from a certificate authority:
   - Select **Paste** if you wish to copy and paste the certificate.
   - Select **Import** if you wish to import the certificate from a file.
2. Click **OK**.

The certificate will now be available in the **Certificates** list.

Add User or Modify User

The **Add User** dialog box is displayed if you click **Add** in either the **Administrators** table or **Help desk users** table on the **Configuration ➤ Accounts ➤ Administrators** page.

The **Modify User** dialog box is displayed if you click a **Username** in either the **Administrators** or the **Help desk users** table on the **Configuration ➤ Accounts ➤ Administrators** page.

- To add a user account:
  a) Type the **Full name**. This is the name that will appear in email messages generated by this user from the Email Appliance system.
  b) Type the **Username**. The username must be more than two characters long, it must begin with a letter, and it may only contain lowercase letters, numbers, underscores, hyphens, or at (@) signs.
  c) Type the **Password**. The password must be between 6 and 20 characters, must contain letters, and must contain at least one number or punctuation symbol.
  d) Repeat the password in the **Confirm password** text box.
  e) Select the user's time zone. This is specific to each user.
  f) Click **OK**.
- To modify account information:
  a) Change any of the following:
     - **Full name**: The name that will appear in emails generated by this user from the Email Appliance system.
     - **Username**: The login name. It must be more than two characters long, it must begin with a letter, and it may only contain letters, numbers, underscores, hyphens, or at (@) signs .
     - **Password**: Must be between 6 and 20 characters, must include letters, and there must be at least one number or punctuation symbol.

- **Confirm password**: Re-enter the password that you typed in the previous text box.
- **Timezone**: Change the time zone to correspond to the user's timezone.

b) Click **OK**.
The viewable account information appears in either the **Administrators** or **Help desk users** table, depending on which user was modified.

Add Message Attribute

The **Add Message Attribute** dialog box is displayed if you click **Add** on the **Message Attributes** page of the Policy Wizard.

To use the Message Details dialog box:

1. From the drop-down list, select a message attribute. The configurable options vary, depending on which attribute you select.
   - **Header**: Verify that the header exists, or if a header contains a specific word or phrase. In the **Name** text box, enter the header to match, and then select one of the following:
     - **exists**: Match messages containing this header.
     - **does not exist**: Match messages that do not contain this header.
     - **is (exact match)**: Match instances of the named header with the exact text that you specify in the **Value** text box.
     - **contains (substring match)**: Match instances of the named header that contain the substring that you specify in the **Value** text box.
     - **matches regular expression**: Match instances of the named header according to the regular expression that you specify in the **Value** text box.
   - **Source IP**: Verify if a message was sent by a specified IP address. Note that the source IP is the first untrusted relay, according to the contents of the Trusted Relays list. In the **IP address** text box, enter a source IP or CIDR address. Then select **is** to trigger the rule whenever a match is found, or **is not** to trigger the rule whenever no match is found.
   - **Source Hostname**: Verify whether a message was sent by a specified host or domain by performing a reverse DNS lookup of the first untrusted relay (FUR). In the **Hostname or domain** text box, enter a source IP. Then select **is** to trigger the rule whenever a match is found, or **is not** to trigger the rule whenever no match is found.
   - **Message Size**: Verify that the size of the message is **greater than** or **less than** the specified threshold. Specify a message size in **MB**, **KB**, or **Bytes**.
   - **Attachment Size**: Verify that the attachment size is **greater than**, **less than**, or **equal to** the specified threshold. Specify an attachment size in **MB**, **KB**, or **Bytes**.
2. Click **Apply**.

Advanced System Updates

1. To specify your preferred software update window:

   Use the **Software engine update schedule** to set the time window in which automatic software updates are installed.

   Critical updates (for example, security-related patches) are applied automatically within 24 hours of availability during the update window. Maintenance updates are applied automatically during the update window, but only on the days of the week specified in the check boxes.

   1. In the **From** and **to** drop-down lists, specify the window of time in which to apply automatic updates.
   2. Select the day of the week check box(es) to specify the day(s) on which non-critical automatic updates are applied.
2. Click **OK**.

Alias Map Editor

The **Alias Map Editor** dialog box is displayed if you click the **Custom alias maps** link on the **Configuration ➤ Accounts ➤ User Groups** page. Use the Alias Map Editor dialog box to create, modify or delete alias maps.

Note: The **Alias Map Editor** dialog box is also displayed if you click **Directory services alias maps** on the **Configuration ➤ Accounts ➤ User Groups** page. However, directory services alias maps are retrieved from the directory services server, and can only be viewed, not edited.

- To add an alias map:
  a) Enter an email address that you want to substitute in the **Map from address** text box, then enter the substitute email address in the **Map to address** text box. Alternatively, click **Upload** to upload a list of addresses. The list should contain one pair of colon-separated email addresses per line, where the first address is the address you want to substitute, and the second is the substitute address itself.

     Note: You can map one domain to another by entering *@<from_domain>* as the **Map from address**, and *@<to_domain>* as the **Map to address**. For example, you could enter *@subdomain.example.com* for the **Map from address**, and *@example.com* for the **Map to address**. This would cause any mail addressed to users at *subdomain.example.com* to be mapped instead to *example.com* for policy purposes.

  b) Click **OK**.
- To remove an alias map:
  a) Select the check box beside the email map(s) that you want to remove.
  b) Click **Delete**.
  c) Click **OK**.
- To edit an alias map you must first delete the map you want to change, then add a new map that contains the changes you want to make.

  Use the **Find** text box to search a large list for email addresses that you want to delete, or use the page controls below the list to navigate through the list.

Alert Contacts

The **Alert Contacts** dialog box is displayed if you click **Edit** in the **Local alerts recipients** row on the **Configuration ➤ System ➤ Alerts** page.

- To add an alert contact:
  1. Type the email address of the person in your organization that you want to receive email alerts into the text field.
  2. Click **Add**.

     The email address appears in the **Alert Recipients** table.
- To remove an alert contact:
  1. Select the check box to the right of the email address that you want to remove from the list.
  2. Click **Delete**.

     The email address is removed from the list.
  3. Click **OK** to close the dialog box.

Appliance Support Contact

The **Appliance Support Contact** dialog box is displayed if you click **Edit** in the **Appliance support contact** row on the **Configuration ➤ System ➤ Alerts** page.

To set the information for your organization's appliance support contact:

1. From the **Business country** drop-down list, select the country in which your Email Appliance operates.
2. From the **Business time zone** drop-down list, select the time zone in which your Email Appliance operates.
3. From the **Business hours** drop-down lists, select the begin and end times of the normal business hours for your organization, or that part of your organization in which your Email Appliance operates.
4. In the **Business hours contact** section, set the appropriate information in each field or drop-down list:
    1. **Name**: Enter the full name of the person who is the Email Appliance support contact.
    2. **Method of contact**: Select the method by which your Email Appliance support contact person would prefer to be contacted.
    3. **Email**: Enter the email address of your organization's Email Appliance support contact person.
    4. **Alternate email**: Optionally, enter the alternate email address of your organization's Email Appliance support contact person.
    5. **Mobile Phone**: Enter the cell phone number of your organization's Email Appliance support contact person.
5. In the **Out of hours business contact** section, either select the **Same as business hours contact** check box or clear that check box and fill in the fields for your organization's off-hours Email Appliance support contact person.

    See step 4 for details for what to enter in each field.
6. Click **Submit**.

Additional Message Actions

The **Additional Message Actions** dialog box allows you to configure an additional action for a rule.

You can add a banner to the top or bottom of a message, add or replace the header of a message, or send a notification to the sender, recipient, or to a custom address.

To configure an additional action:

- Select **Add banner** if you want to add a banner to the top or bottom of a message.
    - Select **Top** or **Bottom** to configure the banner location.
    - Enter the banner text in the text box.
    - [Optional] Select the **Preserve the character encoding of the original message** check box to ensure that the message body's encoding is maintained during the processing of the message. When selected, the message body's encoding is also applied to the banner.

      You may want to select this option if the appliance processes messages with a character encoding that is not universal (for example, Shift_JIS).

      Note: If you are configuring multiple rules that will add a banner when triggered, you should be consistent in the use of this option. Otherwise, more than one character encoding may be applied to a message, causing the message or banner to be displayed incorrectly.

- Select **Add header** if you want to add or replace the header of a message.
    - Select **Add** or **Replace** to configure whether a header will be added or replaced.

      Note: If you select **Replace**, and multiple headers of the same name are present, all of them will be replaced.

  - In the **Header name** text box, enter the name of the header you want to replace.
  - In the **Header value** box, enter the header text.

- Select **Add a log entry** if you want events that trigger this policy rule to be logged to the message policy log. Events are displayed in the log as key/value pairs with the form *user_<key>=<value>*, where *user_* is added to beginning of the assigned key. The message policy log is accessible through either FTP backup or syslog.

  - Select **Add** or **Replace** to configure whether a log entry will be added or replaced.

    Note:

    If you select **Add**, there can be multiple entries of the same key, but with different values. For example, if multiple policies trigger, entries similar to the following will appear:

    ```
    user_policy=strip_suspect_attachment
    user_policy=quarantine_for_spam
    ```

    If you select **Replace**, and multiple log entries with the same key are present, all of them will be replaced.

  - In the **Key** text box, enter the key that you want to assign to this log entry.

    Note: Keys will be logged with the prefix *user_*. Keys may only contain alphanumeric characters, or the underscore ("_") character.

  - In the **Value** text box, enter the value that you want assigned as the key for this log entry.

  You can choose arbitrary key/value pairs.

  When selecting this option, you should also *Syslog* (page 118) for your appliance.

- Select **Notify** if you want to send a notification to the sender, recipient, or to a custom address.

  - In the **Notify users** section, select:

    - **Sender** to send a copy of the message to the sender.
    - **Recipient** to send a copy of the message to the recipient.
    - **Postmaster** to send a copy of the message to the system postmaster.
    - **Custom email address** to send a copy of the message to a different email address than the sender or recipient. Enter the custom address in the **Custom email address** text box.

  - In the **Subject** text box, enter the subject line of the notification.
  - In the **Notification message** text box, enter the text, if any, of any notification message you want to include.
  - Select the **Attach Original Message** check box if you want to include the original message with the notification.

- Use predefined variables called *Template Variables* (page 189), if you want to include additional information in a notification. For example, you can insert the template variable *%%MESSAGE_SIZE%%* in the **Subject** text box of a notification, and the appliance will replace the template variable with the message size.

Advanced Backup Schedule

The **Advanced Backup Schedule** dialog box is displayed if you click **Configure** on the **Configuration ➤ System ➤ Backup** page.

To use the Advanced Backup Schedule dialog box:

- Select **Allow Sophos to automatically manage this scheduled job (recommended)** so that Sophos manages backups.
- Select **Manually configure which appliances can run this scheduled job** if you want to manage backups yourself. Once you have elected to manage backups, use the check box next to the appliance name to select whether it will run this job. If the appliance is a member of a cluster, you will see a list of the other appliances in the cluster, which you can also manage.
- Select **OK** to save any changes, or **Close** to exit the **Advanced Backup Schedules** dialog box without saving any changes.

Calendar

The **Calendar** dialog box is displayed if you click in any date/time field on the **Search** tab.

To change the date and time for the selected field:

- To set the month, use the left and right arrow buttons beside the name of the month.
- To set the day of the month, click the day number.
- To set the time of day, use the up and down arrows beside the hour (hr), minute (min), and second (sec) fields to set the time, or type the time in the respective fields. Note that the hour field uses 24-hour time (00-23).
- Click **OK** to apply your changes and close the **Calendar** dialog box, or click **Cancel** to close the dialog box without saving any changes.

Certificate Details

The **Certificate Details** dialog box is displayed if you click a certificate description in the **Certificates** section on the **Configuration ➤ System ➤ Certificates** page. It shows detailed information about the certificate, and also allows you to download the certificate, or the certificate and its private key.

1. To download the certificate, click **Download**.

   Your browser will prompt you to save the certificate on your local computer.

2. To back up a certificate and its corresponding private key, click **Backup**. Your browser will prompt you to save the certificate/private key pair on your workstation.

   Caution: It is important to not share this file with anyone. It contains a private key that can be used to allow anyone to masquerade as your organization.

Upload Certificate

The **Upload Certificate** dialog box is displayed if you click **upload certificate** next to a pending CSR on the **Configuration ➤ System ➤ Certificates** page. You can upload a certificate provided by a certificate authority (CA), or view details of the pending CSR.

- To upload a certificate:
  - Select **Paste certificate text** and paste the provided certificate or,
  - Select **Import certificate file** to upload a certificate you have saved to a file.

  Note: The certificate must be in **PEM** or **PKCS#12** format, and it must match the selected CSR.

- To view details of the pending CSR, click on the **CSR Details**.
  - Click **Download** to save the CSR:
  - Cut and paste the displayed CSR and save it as a text file.

  Note: The CSR's exact formatting must be preserved. Because of this, it is recommended that you use a text editor such as Notepad, and not a word processor or similar program to save the CSR.

Edit notification email

Customize the **Subject** and **Body** of the message that accompanies the password service method that you have chosen.

A number of template variables are available to customize messages. The template variables available depend on which password service you have selected. Template variables specific to the *SPX registration message* (page 191) are available

if you have opted to let recipients choose their own passwords, and variables specific to *messages with SPX generated or sender-specified passwords* (page 191) are available if you have opted to either generate passwords or allow sender-specified passwords and have the sender communicate passwords to recipients.

Note: Certain template variables must be present in the subject or text of different kinds of notification emails, or you will not be able to save it:

Password service	Required template variable(s)
Allow the message recipient to choose their own password	%%REGISTRATION_URL%%
Encrypt the message with a generated password	%%ENVELOPE_TO%%, %%GENERATED_PASSWORD%%
Encrypt the message with a sender-specified password	%%ENVELOPE_TO%%, %%SPECIFIED_PASSWORD%%

Edit SPX Recipient Instructions

Use the **SPX recipient instructions** page to customize the text of the email that is sent with each SPX email message. This provides recipients with information about the SPX message that they have received, such as the required Adobe Reader software, and, if necessary, how to obtain the password needed to read the message.

Note: When using sender-specified passwords, the instructional email will have the same subject as the sender-specified password email, except that the associated tag, password, and brackets will be removed.

Add or edit email body:

1. In the **SPX recipient instructions** dialog, edit the text as necessary.

   Note: You can use basic HTML to help format the registration email. If the recipient's email client is configured to accept HTML messages, the formatted version is displayed; otherwise, their email client shows a text version of the registration email, with no special formatting. The registration email has a size limit of 4KB.

   You can customize messages with any of the template variables *available for the SPX instructional text* (page 190).

   Selecting any of the **End user password options** on the previous wizard page automatically inserts text on this page that contains an associated template variable. Included in the text is a URL that recipients can click to access the appropriate password page on the SPX Secure Email Portal.

   Customize the recipient instructions text as necessary, but for each end user password option check box selected on the previous page (**Password Settings**), ensure that the associated template variable is preserved. If the included template variables do not match the selected check boxes, a warning message is displayed. A match is required to create an active link to the appropriate SPX portal page.

2. In the **Text** text box, edit or update the instructions that will be sent to recipients of SPX messages. This should contain useful information, such as how to open SPX messages, how to obtain their password and so forth.

Email Password List

The **Email and Password List** dialog box is displayed if you click (**Define users**) beside the **Custom list** option on the **Configuration ➤ Accounts ➤ User Preferences** page.

To build the email addresses and password list:

1. In the **Addresses** text box, type or paste a comma-separated list of email address/password pairs, with only one email address and password per line. Each entry must not contain spaces.
2. Click **OK**.

Configure End User Web Quarantine Ports

Use the Configure End User Web Quarantine dialog box to select the port used by the Web Quarantine. By default, port 443 is used for the web quarantine, and port 10443 is used for the Secure PDF Exchange (SPX) portal. To change this:

1. Select the port for either the Web Quarantine.
   After you select the port for one service, the remaining port will automatically be assigned to the other service.
2. Click **OK** to save your changes.

Forward

The **Forward** dialog box is displayed if you click the **Forward** button beneath the **Search ➤ (Quarantine) search results** . This is done to send the selected email message to someone other than the originally intended recipient.

To forward the message:

1. Type the email address to which you want to forward the message.
2. Click **OK**.

Group Editor

The **Group Editor** dialog box is displayed if you click **Add** or click on the name of an existing group in the **Create groups manually** table on the **Configuration ➤ Accounts ➤ User Groups** page.

To create or change a group:

1. Enter or edit the **Group name**.
2. Create the list of email addresses that will belong to the group by doing the following:
   - In the **Email address** text box, enter an address and click **Add**. Repeat this step for each email address that you want to add. Alternatively, click **Upload**, which opens the *Upload* (page 203) dialog box, and add a list with only one email address per line.

     Note: Email addresses must be actual addresses, not alias addresses, unless alias map support is turned on.

   - Remove one or more email addresses from the list by selecting the check box beside the email addresses that you want to remove and clicking **Delete**.
   - Use the **Find** text box to search a large list for email addresses that you want to delete, or use the page controls below the list to page through the list.
3. Click **OK**.

Global Function History

The **Global Function History** dialog box is displayed if you click the **History** link for any function in the **Global functions** panel.

A list of events since the history was last cleared is displayed. Only changes of state are shown. If several identical events are logged, only the first will be shown in the list.

- To clear the history, click **Delete All**
- To close the **Global Function History** dialog box, click **OK**

Upload a Header/Footer Image for the SPX Portal

To add a custom header or footer image to the SPX Secure Email Portal:

- Enter the location of the image you want to use in the **File location** text box, or click **Browse** to use the file selection dialog to locate the image file.

Click **OK** to upload the file.

Note: Header and footer images must be JPG, GIF or PNG format. The portal is optimized to use images that are 752 pixels wide by 69 pixels high. Other image sizes may be used, though results may vary.

Additional Network Routes

The **Additional Network Routes** dialog box allows you to specify routing of requests to specified IP ranges via specified gateways. Additional routes can enable the Email Appliance to process requests from client machines whose IP addresses reside outside of the native subnet of the Email Appliance.

Important: Adding additional routes is an advanced option and should only be used if you have a thorough understanding of both routing and your network topology. Adding routes incorrectly can make the administrative user interface inaccessible.

- To add a route:
  - Enter a descriptive **Route Name**.
  - Enter the requested **Destination IP Range** in CIDR format.

    Important: This range must not include the static IP address of the Email Appliance and must be outside the subnet of the Email Appliance.

  - Enter the **Gateway IP Address** to which you want the requested IP addresses routed. This represents the next hop that can be used to reach the destination IP specified, and should be on the same subnet as the Email Appliance.
  - Click **Add**.

    To disable a route, you must delete it. To modify a route, you must delete it and re-add the modified route information.

- To delete a route:
  - Select the check box beside the route that you want to delete.
  - Click **Delete**.

    The route is de-activated and removed from the routing table.

    Note: If you change your network configuration or topology, it may be necessary to alter any additional routes you have created.

    Note: If a route is specified that makes the administrative user interface inaccessible, you must connect a laptop to the configuration port on the back of the appliance and access the Email Appliance via the IP address 172.24.24.172 to gain access to the appliance and delete the incorrect routes.

List Editor

The **List Editor** dialog box is displayed when you click **Suspect Attachments** in either the **Inbound anti-virus** or **Outbound anti-virus** tables on the **Configuration ➤ Policy ➤ Anti-Virus** page, when you click **Offensive Language**, **Inbound Keywords**, or **Outbound Keywords** links on the **Configuration ➤ Policy ➤ Content** page, or when you click either **Allowed hosts/senders** or **Blocked hosts/senders** on the **Configuration ➤ Policy ➤ Allow/Block Lists** page.

To modify a suspect attachments, offensive language, or keywords list:

1. Select a character-matching scheme (string or regular expression). There are separate lists for strings and regular expressions that combine to form a single filter. The default matching scheme is **String (wildcards supported)**.

   Note: When adding or editing strings using the **String (wildcards supported)** option, you must use wildcards to perform substring matches. For example, if you simply add *ReallyBadWord* to the list, that entry will not match sentences containing *ReallyBadWord*. However, the entry **ReallyBadWord** will match all sentences containing *ReallyBadWord*. Exclusions are also supported. For example, if you add an entry to block **foo**, you might want to exclude *!*foobar**.

2. Modify the list by doing any of the following:

   - Add an entry by typing it in the top text box and clicking **Add**. Repeat this step for each additional entry. Alternatively, click **Paste List**, which opens the *Paste List* (page 204) dialog box.
   - Import a list of entries from a text file by clicking **Upload**. In the **Upload** dialog box you may either:
     - Select **Merge with current list**. Only entries which do not already exist will be added to the list.
     - Select **Replace current list**. All list entries will be replaces with the new list.
   - Remove entries from the list by selecting the check box beside the entry that you want to remove and clicking **Delete**.
   - Use the **Find** text box to search for entries or use the page controls below the list to browse through the list.

3. Click **OK**.

List Selector

The **List Selector** dialog box is displayed when you click the item in the **To** or **Except** column of a message-filtering option on the **Configuration ➤ Policy ➤ Anti-Spam** , **Anti-Virus**, or **Additional Policy** pages.

To define the users for which this filtering option will apply:

1. On the **Select users** drop-down list, select one of the following options:

   - **All end users**: Includes or excludes all groups of users previously defined on the **Configuration ➤ Accounts ➤ User Groups** configuration page.
   - **No end users**: Includes or excludes none of the users.
   - **Custom users**: Allows you to select a subset of all the users by selecting from the groups previously defined on the **Configuration ➤ Accounts ➤ User Groups** page or to define a custom group of users.

2. If you selected **Custom users** in the previous step, select an option button (**Existing groups** or **Custom groups**).
3. Do one of the following:

   - If you selected **Existing groups**, select groups in the **Available** list and click the add button (>>) to add groups to the **Current** list; select groups in the **Current Users** list and click the remove button (<<) to remove groups from the **Current** list.
   - If you selected **Custom groups**, type the email addresses of individual users in the text box and separate the addresses with a comma (but no space).

   Note: Email addresses must be actual addresses and not alias addresses (unless *User Groups* (page 29) is turned off).

4. Click **OK** to save your changes and close the **List Selector** dialog box, click **Apply** to save without closing the **Group Editor** dialog box, or click **Cancel** to close the dialog box without saving the changes.

Upload

The **List Editor** dialog box lets you upload multiple entries from a text file. There should be one entry per line in the text file.

To upload a list of entries:

1. Click **Browse**, and select the file containing the list you want to upload.
2. Either:
   - Select **Merge with current list**. Only entries which do not already exist are added to the list.
   - Select **Replace current list**. All list entries are replaced with the new list.
3. Click **OK**.

Message Details

The **Message Details** dialog box is displayed if you click **View message details** in the expanded view of a selected message on the **Search ➤ (Quarantine) Search Results** page, or if you click **View log details** on the **Search ➤ (Mail Logs) Search Results** page.

To use the Message Details dialog box:

- For **Quarantine** search results, the **Message Details** dialog box shows the following information:
  - By default, the **Message Details** dialog box shows the content, or body, of the message.
  - Select the **Headers** tab to view the routing record and other information contained in the message header.
  - Select the **Info** tab to view the message's quarantine information.
  - Select the **Body** tab to return to the body of the message.
- For **Mail Logs** search results, the **Message Details** dialog box displays additional detail about each message.
- When you are finished, click **OK** to close the **Message Details** dialog box.

Modify User

The **Modify User** dialog box is displayed if you click a **Username** in either the **Administrators** or the **Help desk users** table on the **Configuration ➤ Accounts ➤ Administrators** page.

To modify account information:

1. Change any of the following:
   - **Full name**: The name that will appear in email messages generated by this user from the Email Appliance system.
   - **Username**: The login name. It must be more than two characters long, it must begin with a letter, and it may only contain letters, numbers, underscores, hyphens, or at (@) signs.
   - **Password**: Must be between 6 and 20 characters, must include letters, and there must be at least one number or punctuation symbol.
   - **Confirm password**: Re-enter the password that you typed in the previous text box.
2. Click **OK**.
   The viewable account information appears in either the **Administrators** or **Help desk users** table, depending on the user that was modified.

Rule Caution Indication

The caution indicator is displayed in the rules table to indicate that a rule will never be triggered. This can happen when you have two rules of the same type, but the rule listed first applies to all senders or recipients, and also discontinues processing after it has been triggered.

> **Example:**
>
> The first rule on the **Configuration ➤ Policy ➤ Anti-Spam** page has been configured to discard all messages containing unscannable attachments. The third rule on the **Configuration ➤ Policy ➤ Anti-Spam** has been configured to also discard unscannable attachments, but only for one specific group. In this case, the third rule will never trigger, because the first rule results in all messages of the same type being discarded. The caution indicator will be displayed next to the third rule.

Notify

The **Notify** dialog box is displayed if you click the item in the **Notify** column for a policy option in the **Configuration ➤ Policy ➤ Anti-Virus** or **Content** page. This dialog box allows you specify an email recipient, such as an Email Appliance system administrator, who will be notified when messages match this filtering option.

To specify a notification recipient:

1. In the **Email address** text box, type the email address of the person that you want to notify.
2. [Outbound Messages Only] Optionally, select the **Copy sender** check box if, additionally, you want a notification sent to the original sender of the message.
3. [Optional] Under **Notify Options**, specify how you want the specified recipient to be copied on this notification. Or, select **Redirect to** if you want the specified recipient to be notified instead of the recipient(s) named in "To" list.
4. [Optional] In the **Notification message** text box, type the message that you want included in the body of the notification email.

   This allows you to tell recipients why they are receiving a notification.
5. Click **OK**.

Paste List

The **Paste List** dialog box is displayed if you click **Paste List** in the **Group Editor**, **Alias Map Editor**, or **List Editor** dialog box.

To paste in an email address list:

1. Paste a list of email addresses that contains a single entry per line.
2. Click **OK** so save the list, or click **Cancel** to exit without saving the list.

Upload a PDF Cover Page

1. Click **Browse**, then select the PDF you want to use for the SPX email cover page(s).

   Note: There are requirements and restrictions for PDF cover pages. For more information, see the *SPX Best Practices* (page 104).

Postmaster Address

The **Postmaster Address** dialog box is displayed if you click **Edit** in the **Postmaster Address** section of the **Configuration ➤ System ➤ Alerts** page.

The postmaster is the person responsible for implementing and maintaining the email system for an organization. Email standards require that mail addressed to the "postmaster" virtual user will be accepted and sent to a real user.

To set or change the postmaster address:

1. In the text box, enter the email address of the person in your organization who will receive "postmaster" email.
2. Click **OK**.

CCL Configuration

Most SophosLabs Content Control Lists (CCLs) have a quantity assigned to them.

A quantity is the volume of the CCL key data type that must be found in a file before the CCL is matched. You can edit the quantity of a SophosLabs CCL by clicking on the CCL name on the "Rule Config" page of the Policy wizard. The quantity for custom CCLs must be edited in Sophos Enterprise Console.

Using quantity, you can fine-tune your data control rules and avoid blocking documents that do not contain sensitive information (for example, a document containing one postal address or one or two telephone numbers, possibly in the letterhead or signature).

If you search for a single postal address, thousands of documents may match the rule and trigger a data control event. However, if you want to prevent the loss of a customer list, you may want to only detect the transfer of documents containing, for example, more than 50 postal addresses. In other cases, however, it may be advisable to search for a single instance of content, for example, a credit card number.

Quantity is the volume of the CCL key data type that must be found in a file before the CCL is matched.

Custom rules use "trigger scores," which are created as part of an advanced CCL. See the Sophos Enterprise Console documentation for more information. A trigger score refers to the number of times a regular expression must be matched before a CCL is matched.

To set the quantity for a rule:

1. Click the green icon for the rule for which you want to set the quantity (the rule must be selected).
   The **CCL Configuration** dialog box is displayed.
2. In the details section, either:
   - accept the default quantity for the CCL
   - or specify a quantity.
3. Click **Apply**.

Setting Expiry Times and Passwords

Clicking **Configure** in the **Expiry and user password settings** section of the **Policy: Encryption** page opens the **SPX Expiry and Password Limits** dialog box. Here you can configure the periods for SPX option expiry, and notification times. All values must be entered as days. You can also specify the minimum number of characters required for passwords.

1. Set one or more of the following:
   - In the **Keep unused passwords** text box, enter the maximum number of days between password uses that passwords will remain valid.
   - In the **Allow secure reply** text box, enter the maximum number of days that the link sent for the secure reply portal remains valid for recipients of SPX email messages.

- In the **Keep delayed emails** text box, enter the number of days that an appliance will hold email while waiting for an SPX recipient to set a password.
- In the **Registration reminder** text box, enter the number of days before an SPX recipient will receive an email reminder to set a password.

  Note: The **Registration reminder** period should be shorter than the **Keep delayed emails** period.

- In the **Password strength** text box, enter the minimum number of characters an SPX user must type in order to create a valid password. The default is passwords that are at least 8 alphanumeric characters in length. The maximum length is 32.
- Select **Require special characters** to enforce inclusion of at least one special character in each password. Valid special characters are shown to recipients when they are setting a password.

2. Click **OK**.

Configuring the SPX Portal

Clicking **Settings** in the **Portal** section of the **Policy: Encryption** page opens the **Configure SPX Portal** dialog box. Here, you configure the URL used for the Secure PDF Exchange (SPX) email portal. By default, port 10443 is used for the (SPX) portal, and port 443 is used for the End User Web Quarantine.

Note: By activating the SPX portal you give recipients a means of registering for an SPX password. If you want recipients to have the option of securely responding to encrypted messages, you must enable secure reply using the SPX Template wizard. For more information, see “Portal Settings”.

To configure the portal URL:

1. Select either the **Use hostname from SSL certificate (Recommended)** if you want to use the hostname from the Email Appliance's SSL certificate, or select the **Specify a custom hostname** option and enter the hostname of the Email Appliance on which the SPX portal is located.
2. Under **Ports**, select the port used for the **SPX portal**.
   Whichever port you select for the SPX Portal, the remaining port will automatically be selected for the End User Web Quarantine (the reverse is also true).
3. Click **OK**.

Note: You may need to add or configure a certificate for use with the SPX portal. See the *Certificates* (page 129) documentation for more information.

System Alerts

The **System Alerts** dialog box is displayed if you click on an "exception" icon in the **Exceptions** column of the **System Status** page. The **System Alerts** dialog box shows all of the existing alerts for the selected monitored item.

To clear alerts:

1. Click **Delete All**.
2. Click **OK**.

Trusted Certificate Authorities

The **Trusted Certificate Authorities** dialog box is displayed if you click the **Certificates** page.

To add a new trusted certificate authority:

1. On the **Locally managed** tab, click **Add**. The *Add Certificate Authorities* (page 193) dialog box is displayed.

After you have added the trusted certificate authority, it will be displayed in the list of trusted certificate authorities on the **Locally Managed** tab.

Note: The **Sophos managed** tab displays a list of certificate authorities managed by Sophos. This list cannot be edited.

2. Optionally, to delete a certificate authority from the **Locally managed** list, select the CA, then click **Delete**.
3. Click **Close**.

Verify Settings

The **Verify Settings** dialog box is displayed if you click **Verify** on the **Server Settings** page of the Directory Services wizard.

The **Verify Settings** dialog box is a simple progress reporting dialog box that displays the success or failure of an FTP site or directory services server verification process.

To use the Verify Settings dialog box:

1. If a green check mark is displayed next to each of the listed settings, click **OK**. If any there are any failures, adjust the settings and run the verification again.

Note: The **Verify Settings** dialog box shows the server you are making a **Connection from** and the server you are **Connecting to**, to assist with directory services configuration.

Glossary

Active Directory

Microsoft's implementation of LDAP (Lightweight Directory Access Protocol) on Windows.

The Active Directory service provides management of identities and permissions of users throughout a network.

allow list

A list that identifies addresses, hosts or IP addresses from which email will always be allowed.

In Sophos email filtering products, this list is also referred to as an allowed hosts/senders list. This type of list was previously known as a "whitelist".

block list

A list used to block mail from specific hosts.

In Sophos email and URL filtering products, this list is also referred to as a blocked hosts/senders list. This type of list was previously known as a "blacklist".

bulk mail

Bulk-distributed email.

Bulk email consists of messages that are distributed to a large number of recipients. Unlike spam, users must first opt to receive that mail. This can include messages from mailing lists, advertisers, political parties, and others that users have opted to receive mail from.

Content Control List (CCL)

A Content Control List (CCL) is a set of conditions that describe structured file content.

A CCL may describe a single type of data (for example, a postal address or social security number), or a combination of data types (for example, a project name near the term "confidential").

You can use SophosLabs Content Control Lists that are provided by Sophos, or create custom CCLs from within Sophos Enterprise Console.

SophosLabs CCLs provide expert definitions for common financial and personally identifiable data types, for example, credit card numbers, social security numbers, postal addresses, or email addresses. Advanced techniques, such as checksums, are used in SophosLabs Content Control Lists to increase the accuracy of sensitive data detection.

denial of service (DOS) attack

An attack on a host or network that causes a loss of service to its users.

This is usually done by consuming the bandwidth of the target system or overloading its computational resources with multiple, distributed connections.

disk mirroring

Real-time duplication of all data between two hard disks. The Sophos ES4000, ES5000 and ES8000 use RAID disk mirroring.

DNS A Records

(Address record) maps a hostname to an IP address.

DNS MX Records

(Mail exchange record) maps a domain name to a list of mail exchange servers for that domain.

domain controller

An MS Windows server that responds to security authentication requests (logins, permissions, etc).

Sophos email-filtering products can connect to an *Active Directory* (page 207) domain controller to enable user authentication and map filtering policies to specific groups of users.

End User Web Quarantine

A web-based interface for end users that allows them to manage their Email Appliance user-specific options.

End users can manage messages that have been blocked (quarantined) for reason **Spam**, modify their Allowed Senders and Blocked Senders lists, and configure other user-specific options.

gateway

A node on a network that serves as an entrance to another network.

For example, a mail gateway handles all the mail coming into an organization.

groups

Lists of users to which differentiated policy settings can be applied.

The Sophos email-filtering products use these lists as a basis for the *policy* (page 209) settings that determine which filtering actions are performed for which users.

hub

A server that receives and stores email for clients to retrieve.

A mail hub is an alternative to a a mail *relay* (page 210), which transports email to the next server in the delivery chain). Also referred to as a mailbox server or mail store, a mail hub can be a "groupware" server such as MS Exchange or IBM Lotus Notes.

internal hosts

Hosts that reside within your network, behind the gateway or proxy server.

In setups where another device, such as another SMTP relay or a firewall, is positioned at the network boundary, "internal" refers to hosts that are further inside the network than the gateway or proxy server.

latency

The time delay added to a page load or file download.

More specifically, the delay between the moment something is initiated, such as a URL request made in a user's browser, and the moment its first effect begins, such as the moment when that URL first starts to load in the browser's content pane.

malware

Malware includes viruses, worms and Trojan horses.

Malware, or malicious software, refers to programs that are designed to damage or disrupt a computer. Malware is generally installed without the user's knowledge and describes various types of malicious code.

MTA

(Mail Transfer Agent) A service that transfers messages from the sender or another relay toward its destination. Often referred to as a mail relay or a mail hub.

network mask

Specifies which are the subnetwork and host parts of an IP address.

Also known as a subnet mask, netmask or address mask, the network mask is used to specify which parts of the dotted quad of an IP address identify the subnetwork the host is on and which parts identify the host itself. Network masks are usually represented in either dotted quad notation (for example, 255.255.255.0) or CIDR notation (for example, 192.168.1.0/24).

phishing

Acquisition of identity/passwords by false bank emails and websites.

(Also known as carding and spoofing) Attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term phishing arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords. Sophos email and URL filtering products are configured by default to detect phishing schemes.

policy

The Sophos email-filtering rules.

Policies consist of rules made up of tests and actions. As messages pass through the policy engine, they are tested against specified criteria. Messages that match have a specified action performed on them (for example, Mail With: Unscannable Attachments - Take Action: Quarantine). Rules can relate to the identification and handling of messages or URLs containing:

- spam
- viruses
- unscannable, encrypted, or suspect attachments
- offensive words
- keywords

proxy

A secure server through which internal clients connect to the internet.

A service that allows clients to make indirect network connections to other networks, for example, an HTTP proxy for use by hosts with no direct connection to the internet. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client's request or the server's response for various purposes. A proxy server can also serve as a firewall.

quarantine

The quarantine is a store of messages whose delivery has been blocked by policy rules.

Messages held in the quarantine can be reviewed, released, or deleted.

RAID

(redundant array of independent disks) A system of using multiple hard drives for sharing or replicating data among the drives.

The Sophos ES4000, ES5000 and ES8000 use RAID disk mirroring for data redundancy: if one disk fails, the other disk takes over, and the appliance continues to function normally.

RAID controller

A device that manages the disks in a RAID (redundant array of independent disks).

The computer that is accessing the RAID setup interacts with the disks as a logical unit via this controller.

relay

A mail relay is a server that transports email to the next server in the delivery chain.

A relay is an alternative to a mail *hub* (page 208), which stores email for clients to retrieve).

SMTP

(Simple Mail Transfer Protocol) The standard protocol for email transmission across the internet.

SophosLabs

A 24/7 global network of skilled analysts that responds to evolving security threats.

Focused on rapidly evolving threats like viruses, spam, phishing schemes, spyware and other malware, SophosLabs provides both proactive and rapid solutions for all Sophos customers.

spam

Unsolicited email, often sent to millions of recipients at a time.

"Spammers" harvest recipient addresses from Usenet postings and web pages, obtain them from databases, or simply guess them by using common names and domains.

Sending spam violates the Acceptable Use Policy (AUP) of most ISPs, and can lead to the termination of the sender's account. Many jurisdictions now consider spamming a crime, such as the US, which regulates via the CAN-SPAM Act of 2003.

spam score

A score assigned to a message by the anti-spam engine indicating the relative likelihood that the message is spam.

Anti-spam rules consist of a test definition and a "weight". If the test matches the message, the corresponding weight is added to the message's total spam score. Generally, multiple rules must be triggered by a message in order to result in a

spam score high enough for an action to be taken. SophosLabs constantly analyzes emerging spam techniques and updates the Email Appliance anti-spam rule sets accordingly.

spambot

A spambot is a computer program that spammers use to harvest email addresses from the internet.

spyware

Software that covertly gathers information on users' internet activities.

Most often, spyware gathers user information for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the internet. Once installed, the spyware monitors user activity on the internet and transmits that information in the background to someone else.

SSH

(Secure Shell) a program used for authentication and secure communication.

(Secure Shell) A suite of applications offering secure equivalents to telnet, rlogin, and FTP. The standard versions of these applications transmit unencrypted passwords across the network or internet, leaving systems that use these unsecured applications vulnerable to intrusion. The SSH equivalents - SSH, SCP, and SFTP - encrypt all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

Syslog Monitoring

Syslog is a standard for forwarding log messages in an IP network.

Syslog is a client/server protocol. Logging information is sent as text-based messages from a client system to a syslog receiver or server. Log messages from several clients can be consolidated and analyzed by a syslog server. Syslog messages can be sent via UDP and/or TCP.

TLS

(Transport Layer Security) is a communications protocol used to encrypt and secure communication.

(Transport Layer Security) can use a number of different algorithms to encrypt traffic transmitted across otherwise insecure networks. It can also verify the identity of the server by checking a certificate from trusted certificate authority.

virus

A malicious computer program that copies itself.

Often viruses will disrupt computer systems or damage the data they contain. A virus requires a host program and will not infect a computer until it has been run. Some viruses spread across networks by making copies of themselves or may forward themselves via email. The term 'virus' is often used generically to refer to both viruses and worms.

Submit a Spam Sample

How to submit a spam sample to SophosLabs.

If you received spam that was not detected by your Sophos software, you can submit a sample to SophosLabs.

By forwarding spam to SophosLabs, your users can help Sophos in its ongoing efforts to improve the accuracy of spam heuristics.

What to do

It is preferred that you send samples as RFC-2822 attachments. Submitting in any other format can cause the loss of key message content, which may prevent SophosLabs from effectively analyzing the samples. A similar procedure is required if you want to submit spam false positives to SophosLabs.

From Microsoft Outlook:

1. Create a new email message addressed to `is-spam@labs.sophos.com`.
2. Drag and drop the spam sample from the inbox onto the new email message.
3. Send the email message.

Note: Alternatively, you can deploy the Sophos Outlook Add-in, which allows email senders to report spam messages to Sophos with one click of a button on their Microsoft Outlook toolbar. For more information, see the "Sophos Outlook Add-In Deployment Guide."

From Mozilla Thunderbird:

1. Select the spam sample.
2. From the toolbar choose **Message ➤ Forward ➤ Attachment** .
3. Add `is-spam@labs.sophos.com` to the recipient list.
4. Send the email message.

From other email clients:

With other email clients, use the option 'Forward As Attachment'. You may want to discuss this with Sophos Technical Support before sending in a sample in this way.

Submitting spam false positives to SophosLabs:

Use the same method as described above for spam samples, except samples should be sent to `not-spam@labs.sophos.com`.

Further information

- Spam samples sent to 'is-spam' as RFC-2822 attachments will be automatically processed by systems within SophosLabs.
- You will not receive feedback for emails sent to 'is-spam'.
- Samples sent to 'is-spam' will not necessarily be considered to be, or detected as, spam.

If you need more information or guidance, contact Sophos Technical Support.

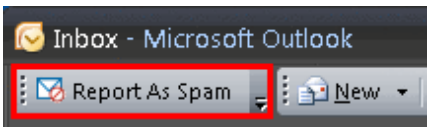
Sophos Outlook Add-in

The Sophos Outlook Add-in simplifies both the reporting of spam messages to Sophos and the encrypting of messages that contain sensitive or confidential information.

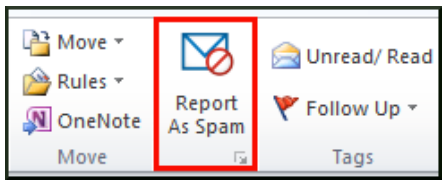
The add-in integrates seamlessly with your users' Microsoft Outlook software, making it easy for users to report spam, and encrypt messages through the Sophos Email Appliance.

Once installed, users can report spam by clicking a custom button in their Outlook window. By forwarding spam to SophosLabs, they help Sophos in its ongoing efforts to improve the accuracy of spam heuristics.

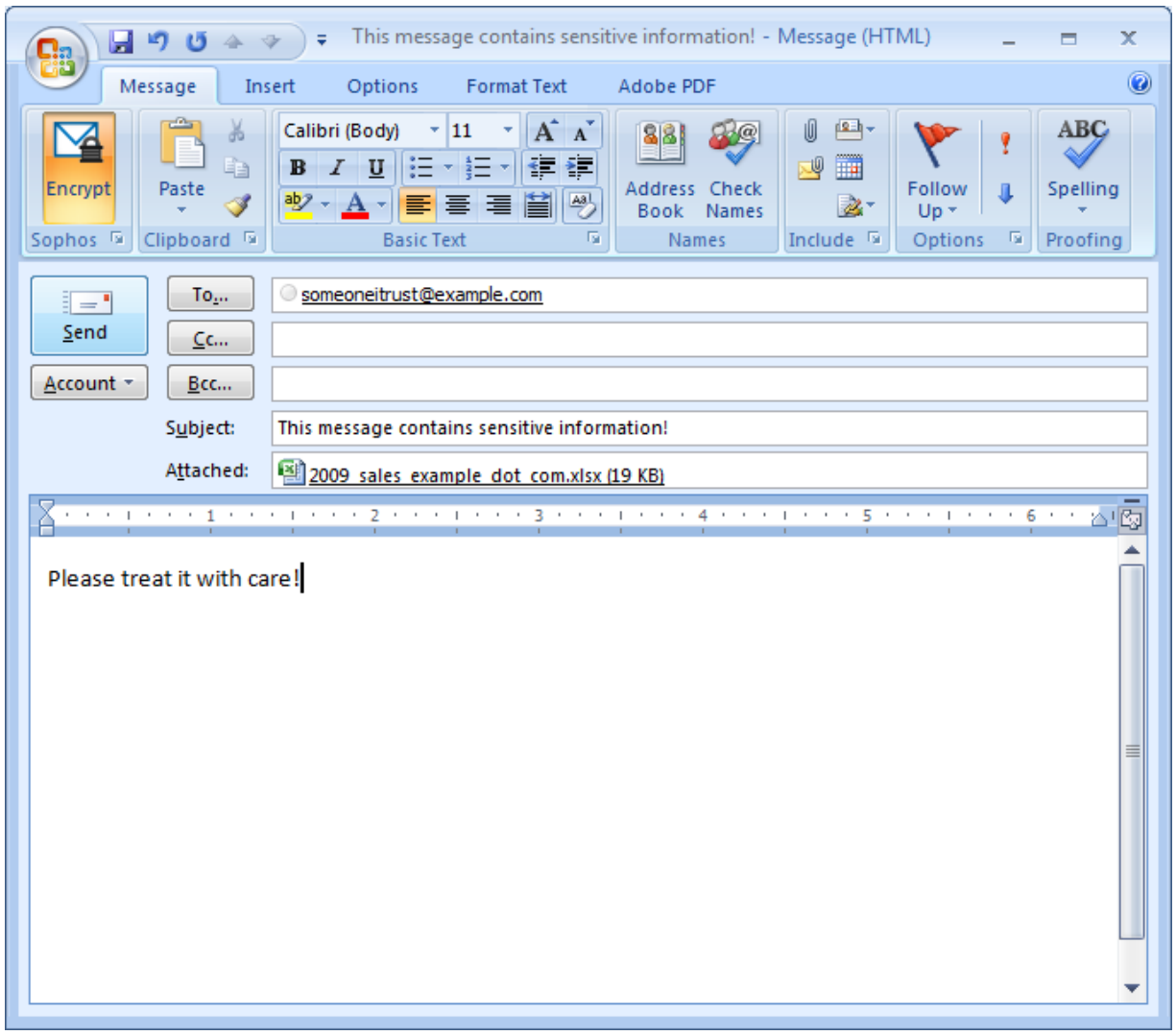
Outlook 2007: The button is in the top-left corner of the Outlook window.



Outlook 2010: The button is on the **Home** tab of the Outlook Ribbon.



If SPX encryption is enabled on the Email Appliance, users can also take advantage of one-click encryption, which allows them to send messages by way of the appliance using SPX encryption. With this feature, users can send content containing sensitive or confidential information as a secure PDF.



The **Encrypt** button at the far left of the toolbar (as shown in the image above) is highlighted in orange when clicked, indicating that the message will be encrypted.

Note: You must configure your Email Appliance policy to work with the clients' add-ins. For more about configuring an encryption rule, see the “SPX Deployment Guide” and the “Additional Policy” section.

As an administrator, you can control how the add-in is installed, and which features are available to your end users. For example, if you want the add-in to be solely a tool for reporting spam, you can disable the message encryption options, or hide them from your users.

The add-in works on the following versions of Microsoft Office and Windows:

- Microsoft Office 2007 or 2010 (32-bit)

  - To encrypt messages through the Sophos Email Appliance, Microsoft Outlook must be configured to send mail using either SMTP or Microsoft Exchange.

- Windows XP x86, Windows 7 x86, or Windows 7 x64

To download the add-in, and for documentation about installing and using the add-in, visit the Sophos website (you will be prompted to enter your MySophos credentials):

https://www.sophos.com/support/downloads/email/sophos-outlook-add-in.aspx

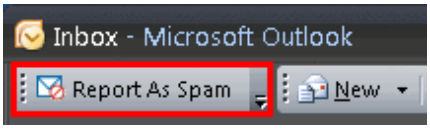
Using the Outlook Add-in

You can deploy the Sophos Outlook Add-in to give end users an easy way to report spam and encrypt messages. If you prefer to use it for only one of these tasks, you can disable or hide either spam reporting features or encryption features from your users.

Users can report spam and encrypt messages by following the steps below.

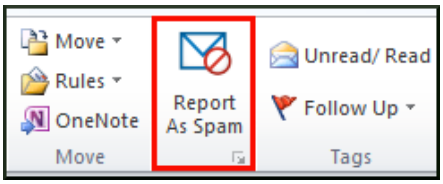
Reporting Spam

1. In the main Outlook window, select the folder (for example, **Inbox**) containing the spam message(s) you want to report.
2. Select the message(s) to report.
3. **Outlook 2007**: In the top-left corner, of the Outlook window, click **Report As Spam**.



or

Outlook 2010: On the **Home** tab of the Outlook Ribbon, click **Report As Spam**.

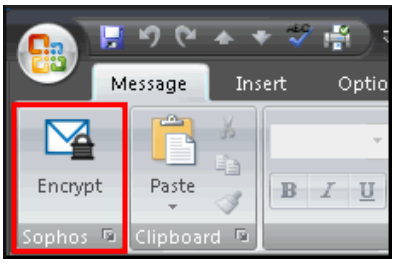


Note: You can also access the **Report As Spam** option from a context menu by right-clicking the message(s) that you want to report, or open any message in its own window, and click the **Report As Spam** button on the toolbar.

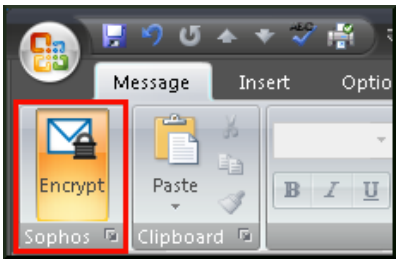
4. If the option to show a confirmation dialog box is selected, a message is displayed, asking if you want to move the message to the default folder, and report it as spam to SophosLabs. By default, the message is moved to the Junk E-mail folder. To specify a different folder, see “Setting Options”. Click **OK** to complete the report.

Encrypting Messages

1. In Outlook, compose an email message.
2. In the top-left corner of the Message window, click **Encrypt**.



The **Encrypt** button is highlighted in orange, indicating that the message will be encrypted.



3. Click **Send**.

   The message is sent to the Email Appliance for encryption.

Copyrights and Trademarks

The Sophos ES100 Email Appliance, the Sophos ES1000 Email Appliance, the Sophos ES1100 Email Appliance, the Sophos ES4000 Email Appliance, the Sophos ES5000 Email Appliance, the Sophos ES8000 Email Appliance, and the Sophos Virtual Email Appliance are all licensed in accordance with the terms of the Sophos Appliance License Agreement. A copy of this license agreement can be found at *http://www.sophos.com/legal*.

This Sophos appliance includes or may include:

- Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (*http://www.openssl.org/*).
- Cryptographic software written by Eric A. Young and software written by Tim J. Hudson.
- Software originally written by David Turner, Robert Wilhelm, and Werner Lemberg. Portions of this software are copyright © 2006 The FreeType Project *www.freetype.org*.
- Software originally written by Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group.
- Software written by Victor A. Abell. Portions of this software are copyright © 1994 Purdue Research Foundation.
- Software originally written by Jean-loup Gailly and Mark Adler.
- Software developed by the Apache Software Foundation (*http://www.apache.org/*). A copy of the license agreement for this software can be found at *www.apache.org/licenses/LICENSE-2.0.txt*.
- Software licensed under the IBM Public License Version 1.0 which permits the user to have access to the source code for such software. The source code of postfix is available free of charge at *http://www.postfix.org/*.
- Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses, which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the terms of the GPL, which is distributed in an executable binary format, that the source code for such software also be made available to the users of the binary form. For any such software covered under the GPL, the source code is available via mail order by submitting a request to Sophos; via email to *support@sophos.com* or via the web at *http://www.sophos.com/support/queries/enterprise.html*. A copy of the license agreement for any such included software can be found at *http://www.gnu.org/copyleft/gpl.html*.

- Some libraries that are licensed (or sublicensed) to the user under the GNU Lesser General Public License (LGPL) using a suitable shared library mechanism for linking with such libraries. A copy of the license agreement for any such included software can be found at *http://www.gnu.org/licenses/lgpl.html*.
- In this product `open-vm-tools` is used at *arms-length* from Sophos proprietary code.

IBM ICU License

ICU License - ICU 1.8.1 and later

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2009 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

All trademarks and registered trademarks mentioned herein are the property of their respective owners.

SEE License

The SEE library source is released under what is commonly called a "BSD-style" licence:

```
/*
* Copyright (c) 2003, 2004, 2005, 2006, 2007
* David Leonard. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. Neither the name of David Leonard nor the names of its contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS
* "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
* LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
* FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
* COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
```

```
* INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
* BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
* CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN
* ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
* POSSIBILITY OF SUCH DAMAGE.
*/
```

The separate 'dtoa.c' file is separately licenced, thus:

```
/****************************************************************
*
* The author of this software is David M. Gay.
*
* Copyright (c) 1991, 2000 by Lucent Technologies.
*
* Permission to use, copy, modify, and distribute this software for any
* purpose without fee is hereby granted, provided that this entire notice
* is included in all copies of any software which is or includes a copy
* or modification of this software and in all copies of the supporting
* documentation for such software.
*
* THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED
* WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR LUCENT MAKES ANY
* REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY
* OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.
*
***************************************************************/
```

UNICODE License

UNICODE, INC. LICENSE AGREEMENT - DATA FILES AND SOFTWARE

Unicode Data Files include all data files under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/ . Unicode Software includes any source code published in the Unicode Standard or under the directories http://www.unicode.org/Public/, http://www.unicode.org/reports/, and http://www.unicode.org/cldr/data/.

NOTICE TO USER: Carefully read the following legal agreement. BY DOWNLOADING, INSTALLING, COPYING OR OTHERWISE USING UNICODE INC.'S DATA FILES ("DATA FILES"), AND/OR SOFTWARE ("SOFTWARE"), YOU UNEQUIVOCALLY ACCEPT, AND AGREE TO BE BOUND BY, ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE, DO NOT DOWNLOAD, INSTALL, COPY, DISTRIBUTE OR USE THE DATA FILES OR SOFTWARE.

COPYRIGHT AND PERMISSION NOTICE

Copyright © 1991-2009 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

Permission is hereby granted, free of charge, to any person obtaining a copy of the Unicode data files and any associated documentation (the "Data Files") or Unicode software and any associated documentation (the "Software") to deal in the Data Files or Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Data Files or Software, and to permit persons to whom the Data Files or Software are furnished to do so, provided that (a) the above copyright notice(s) and this permission notice appear with all copies of the Data Files or Software, (b) both the above copyright notice(s) and this permission notice appear in associated documentation, and (c) there is clear notice in each modified Data File or in the Software as well as in the documentation associated with the Data File(s) or Software that the data or software has been modified.

THE DATA FILES AND SOFTWARE ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THE DATA FILES OR SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in these Data Files or Software without prior written authorization of the copyright holder.

Unicode and the Unicode logo are trademarks of Unicode, Inc., and may be registered in some jurisdictions. All other trademarks and registered trademarks mentioned herein are the property of their respective owners.

Malware, or malicious software, refers to programs that are designed to damage or disrupt a computer. Malware is generally installed without the user's knowledge and describes various types of malicious code.

NGINX License

NGIX LICENSE AGREEMENT

```
/*
 * Copyright (C) 2002-2012 Igor Sysoev
 * Copyright (C) 2011,2012 Nginx, Inc.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
 * THIS SOFTWARE IS PROVIDED BY AUTHOR AND CONTRIBUTORS ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
```

ipfilter License

ipfilter LICENSE AGREEMENT

```
/*
* Copyright (C) 1993-2001 by Darren Reed.
*
* The author accepts no responsibility for the use of this software and
* provides it on an ``as is'' basis without express or implied warranty.
*
* Redistribution and use, with or without modification, in source and binary
* forms, are permitted provided that this notice is preserved in its entirety
* and due credit is given to the original author and the contributors.
*
* The licence and distribution terms for any publically available version or
* derivative of this code cannot be changed. i.e. this code cannot simply be
```

```
* copied, in part or in whole, and put under another distribution licence
* [including the GNU Public Licence.]
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*
* I hate legalese, don't you ?
*/
```

Mootools License

Mootools LICENSE AGREEMENT

```
The MIT License

Copyright (c) 2006-2009 Valerio Proietti, <http://mad4milk.net/>

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.
```

SSDB License

SSDB LICENSE AGREEMENT

```
      Copyright (c) 2013 SSDB Authors All rights reserved.
        Redistribution and use in source and binary forms, with or without modification,
are
        permitted provided that the following conditions are met:

        1. Redistributions of source code must retain the above copyright
           notice, this list of conditions and the following disclaimer.

        2. Redistributions in binary form must reproduce the above copyright notice,
           this list of conditions and the following disclaimer in the documentation
           and/or other materials provided with the distribution.

        3. Neither the name of the SSDB nor the names of its contributors may be used
           to endorse or promote products derived from this software without specific
           prior written permission.

           THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
```

```
 ANY
          EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES

            OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT
            SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
            INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED
            TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
 OR
           BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN

            CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
 IN
            ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH
            DAMAGE.
```

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: *http://www.sophos.com/ companyinfo/contacting/*