IBM Lotus Protector for Mail Security

Administrator Guide

Version 2.8 Release 2.8.1

SC27-3829-01

Publication Date: October 2013

Contents

Tables

About this publication

This publication describes the features and capabilities of IBM® Lotus® Protector for Mail Security.

Audience

This publication is intended for network system administrators who are responsible for installing and configuring Lotus® Protector for Mail Security, applying mail security best practices, configuring SMTP services, and if needed, running applications on VMware.

Latest product documentation

For the latest product documentation, go to the IBM Lotus® Protector for Mail Security Documentation site at https://www.ibm.com/developerworks/lotus/documentation/protector/mailsecurity/.

License agreement

For licensing information about IBM Lotus® Protector for Mail Security, view the IBM Licensing Agreement site at http://www.ibm.com/software/sla/sladb.nsf/search.

What's new in Version 2.8

The following table lists features new to IBM Lotus® Protector for Mail Security V2.8, and tells you how to get started using those features.

Table 1. New features for Lotus Protector for Mail Security V2.8

New feature	How do I use it?
File Attachment Analysis	You can set up Lotus Protector for Mail Security to inspect the content (keywords, regular expressions, URLs) of files attached to incoming email messages. **LMI navigation:** SMTP > File Attachment Analysis **More info:** "Inspecting the contents of files attached to incoming email messages" on page 66
Global IP Access List	You can set up a list of IP addresses that are allowed or denied access at the start of an incoming SMTP connection. This feature is used by the Dynamic Host Reputation Filter and the DNSBL settings. **LMI navigation:** SMTP > SMTP Configuration > Receiving SMTP > Global IP Access List **More info:** "Configuring a global IP access list" on page 28
ICAP server	You can set up Lotus Protector for Mail Security to provide realtime virus scanning services to ICAP-compatible clients such as IBM® Connections, IBM Lotus Quickr®, or Squid 3.x. **LMI navigation:** System > ICAP Server **More info:** "Providing realtime virus scanning services to ICAP-compatible clients" on page 14

Table 1. New features for Lotus Protector for Mail Security V2.8 (continued)

New feature	How do I use it?
Rejection handling for IP addresses using the Silent Drop option	You can set up the SMTP service to reject an incoming email message, but not notify the sender of the email that the email message has been rejected. This method is used to prevent spammers from probing for valid email addresses. This feature is used by the Dynamic Host Reputation Filter, the Global IP Access List, Recipient Verification, and Zero Level Analysis (ZLA).
Configuring system routes manually	You can use the **Manage network routes using Management Interface** option to influence how system routes are handled by the Routing policy. When you enable the option, Lotus Protector for Mail Security uses the system routes that you have configured in the Local Management Interface (LMI). When you disable this option, all system routes are left as is so that you can implement special routing settings that are not currently available in the LMI. **LMI navigation:** System > Routes **More info:** "Configuring system routing manually" on page 17
Updated version of SUSE Linux Enterprise Server (V2.8.1.0)	The underlying operating system is updated from SUSE Linux Enterprise Server 10 to SUSE Linux Enterprise Server 11.
Intrusion Prevention signatures are no longer supported	This feature is no longer available.

Technical support

IBM provides technical support to customers who are entitled to receive support.

The IBM Support Portal

Before you contact IBM about a problem, see the IBM Support Portal at http://www.ibm.com/software/support.

The IBM Software Support Guide

If you need to contact technical support, use the methods described in the IBM Software Support Guide at http://www14.software.ibm.com/webapp/set2/sas/f/handbook/home.html.

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Customer support telephone numbers for the country in which you are located
- Information you must gather before you call

Using Lotus Protector for Mail Security with a command line

Using the command line for read-only access (such as to view settings, services, logs, processes, disk space, or to query the database) is supported. However, using the command line to perform configuration modifications of Lotus Protector for Mail Security voids your IBM Support agreement unless these procedures are followed.

Any changes made to Lotus Protector for Mail Security using the command line must be:

- Authorized in writing by IBM Support.
- Implemented by an IBM Partner, reseller, or internal employee.
- Summarized and documented in a text file in `/root/lib/customization` on the Lotus Protector for Mail Security management console.

Any changes that you have made to Lotus Protector for Mail Security from the command line might be incompatible with future product releases. For troubleshooting new issues with Lotus Protector for Mail Security, you might be required by IBM Support to revert any custom configurations of Lotus Protector for Mail Security back to a default state.

Chapter 1. Getting started with Lotus Protector Manager

This chapter describes how to start using Lotus Protector for Mail Security after you have configured initial network settings with the Setup Assistant.

Navigating the Lotus Protector Manager

The topic explains the navigation features of the Lotus Protector Manager.

Left navigation pane

In the left pane, select the category in the tree that you want to configure. Some categories have more than one component for you to configure. Expand the tree to display a list of configurable elements.

The following table describes each category of the navigation tree:

Table 2. Navigation tree categories

Category	Description
Home	This site provides information about the current health and system status of Lotus Protector for Mail Security, including statistics of email message and data flow.
Mail Security	The options in the Mail Security category explain how to configure a mail security policy that contains a set of rules that define how Lotus Protector for Mail Security should inspect and filter both incoming and outgoing mail traffic.
SMTP	The options in the SMTP category explain how to configure SMTP service settings for Lotus Protector for Mail Security and how to manage the queues for the SMTP server.
System	The options in the System category explain how to set up alert notifications, how to configure firewall settings, and how to make adjustments to configuration settings for Lotus Protector for Mail Security, such as network settings, passwords, and date or time settings.
Backup and Restore	The options in the Backup and Restore category explain how to manage snapshots of configuration settings, how to create complete system backups, and how to back up log files generated by Lotus Protector for Mail Security.
Updates	The options in the Updates category show the status of the licensed security modules and how to configure Lotus Protector for Mail Security to download and install updates for its security modules and firmware.
Support	The options in the Support category explain how to view contact information and how to create support data files for IBM Support.

Lotus Protector Manager icons

The following table describes icons that appear on pages in the Lotus Protector Manager:

Table 3. Lotus Protector Manager icons

Icon	Description
	Click this icon to add an item to the list.
	Click this icon to edit an item in the list.

Table 3. Lotus Protector Manager icons (continued)

Icon	Description
	Click this icon to remove an item from the list. **Note:** In some cases, when you click this icon, you might receive a warning that an item is already being used in another location (for example, in a policy rule or by another object). You should resolve this dependency first, before you remove the object.
	Select an item in the list and click this icon to move the item up the list.
	Select an item in the list and click this icon to move the item down the list.
	Select an item in the list and click this icon to copy the item to the clipboard. **Tip:** You can use the standard `SHIFT+click` or `CTRL+click` methods to select adjacent or non-adjacent items in the list.
	Click this icon to paste a copied item from the clipboard into a list. Items you paste appear at the end of the list.
	If this icon is displayed on a page or next to a field on a page, then you must enter required data in a field, or the data you have entered in a field is not valid.

Administrator session or Limited Access mode

Only one user at a time has full unrestricted access to the Lotus Protector Manager. Other users can use Limited Access mode, but they will only be able to view, but not modify, the current configuration of Lotus Protector for Mail Security. In Limited Access mode, users are limited to browsing and viewing email messages in the message stores, managing users, obtaining reports, and viewing log files.

If you want to log on to Lotus Protector for Mail Security in Administrator mode and another user is already logged on in that mode, you will be prompted to log on in Limited Access mode or to disconnect the other user in order to log on in Administrator mode.

Home page

This site provides information about the current health and system status of Lotus Protector for Mail Security, including statistics of email message and data flow.

Status indicator lights

The indicator lights on each status tab provide a brief status summary for Lotus Protector for Mail Security:

Table 4. Status indicator lights on the Home page

Indicator light	Color	Description
 [G] Good	Green	Indicates that Lotus Protector for Mail Security services are operating as expected.
 [W] Warning	Yellow	Indicates that one or more services for Lotus Protector for Mail Security has encountered a problem. Try to correct this problem as soon as possible.
 [E] Error	Red	Indicates that one or more services for Lotus Protector for Mail Security is experiencing a problem. Try to resolve this problem immediately. **Tip:** The screen might provide an explanation of the issue and suggested actions for resolving the error.

Protection status

The Protection status tab provides a general overview of the categories of email messages that Lotus Protector for Mail Security has analyzed over a given period of time. Additionally, this page informs you if the level of protection provided by Lotus Protector for Mail Security is not sufficient enough, (for example, disabled Firewall), and provides suggestions on how to remedy such problems.

Table 5. Protection status categories

Category	Description
Compliance	Email messages that might contain confidential data.
Ham	Email messages that do not contain advertising or inappropriate content.
IP Blocking	Email messages that were rejected by the SMTP service, because the sending host IP address is known to be a spamming host.
Other	Email messages that do not belong in one of the other predefined categories.
Phishing	Email messages in which a perpetrator sends legitimate-looking email in an attempt to gather personal and financial information from recipients.
Recipient Verification	Email messages that might have been sent to a user who does not exist in the organization.
Remote Malware Detection	Email messages that are detected by antivirus software as containing known malware files such as computer viruses, worms, Trojan horses, root kits, and spyware (programming that gathers information about a computer user without permission).
Signature Virus Detection	Email messages that are detected by antivirus software as containing signature-based viruses.
Spam	Email messages that contain unsolicited advertisements or offensive content.
ZLA NDR	Email messages that have been detected by the Zero Level Analysis module. These messages have failed transmission and did not reach the intended recipient of the message.
ZLA Spam	Email messages that have been detected by the Zero Level Analysis module. These messages are classified as unsolicited bulk email messages, such as phishing, advertisements, or malware.

Assessment status

The Assessment status tab provides an overview of the current health status of Lotus Protector for Mail Security.

Note: Lotus Protector for Mail Security might throttle processing of email traffic in order to alleviate the situation (for example, accept less incoming email messages from other hosts), if one of the following values is too high. However, if Lotus Protector for Mail Security remains in an unhealthy state for a long period of time, you might want to consider adjusting your setup.

Table 6. Assessment status settings

Setting	Description
Database Writer Queue	The number of records of analyzed email messages that have not been written to the database yet.
Analysis Queue Rating	The current fill level of the SMTP queue used to temporarily store email messages until they are analyzed by Lotus Protector for Mail Security (*unchecked queue*).
Resource Shortage	The current status of RAM and disk usage of Lotus Protector for Mail Security. Possible values include: • 0 = The amount of free memory and disk space is sufficient. • 1 = Lotus Protector for Mail Security has detected a shortage of memory or disk space, which may negatively impact its operation. You should monitor this situation and remedy it if necessary. • 2 = Lotus Protector for Mail Security has almost run out of available resources. You should try to solve this situation immediately. **Note:** If Lotus Protector for Mail Security has detected a shortage of available resources, it will generate the event(s) (`MSM_ResourceError`) on the Events page (**System** > **Events**). The event contains additional information about the issue.
Message Tracking Queue	The current fill level of the queue used to store the Message Tracking Data in the Lotus Protector for Mail Security database.
IPC Queue Rating	The current fill level of the communication channel between the SMTP service and the Mail Security.
Send Queue Rating	The current fill level of the SMTP service queue for outgoing email messages (*send queue*).

Traffic status

The Traffic status tab shows incoming and outgoing network traffic over a given period of time.

Table 7. Traffic status settings

Setting	Description
Incoming (Minute Average)	Total number of email messages received over a given period of time.
Outgoing (Minute Average)	Total number of email messages delivered over a given period of time.
Queued for Analysis	Shows the number of email messages waiting to be analyzed by Lotus Protector for Mail Security.
Queued for Delivery	Shows how many email messages have been analyzed and are waiting to be delivered by the SMTP module.
Queued for Re-Delivery	Shows the number of email messages that have already attempted to be delivered to the destination SMTP server, but the delivery failed with a temporary error, such as the host was not reachable. **Attention:** A large number of email messages in the redelivery queue can indicate a permanent problem with delivery (such as an issue with configuration).

Resources status

The Resources status tab shows information about the system resources in use for Lotus Protector for Mail Security. This information might be helpful if you must contact IBM Support about a problem.

Table 8. Resources status settings

Setting	Description
System	
CPU Usage (Percent)	Monitors processor resources used by user-level processes and the system kernel.
System Load	Monitors the amount of work that the system is doing.
Memory Usage (MB)	Monitors how much of the installed memory is free.
Hard disks	
System (MB)	Monitors the amount of disk space being used for the system running Lotus Protector for Mail Security.
Data Storage (MB)	Monitors the amount of data stored on the system running Lotus Protector for Mail Security.
Database (MB)	Monitors the amount of disk space being used for the Lotus Protector for Mail Security database.
Message Store (MB)	Monitors the amount of disk space being used for the email message storages.

Updates status

The Updates status tab shows the current status of the latest updates to Lotus Protector for Mail Security.

Table 9. Updates status settings

Component	Description
Appliance Firmware	The latest version of the firmware version of the Lotus Protector for Mail Security software.
Content Filter Database (Web)	The version of the Content Filter Database currently in use by Lotus Protector for Mail Security. This Web version of the Content Filter Database contains URLs and classification of web pages.
Content Filter Database (Mail)	The version of the Content Filter Database currently in use by Lotus Protector for Mail Security. The Mail version of the Content Filter Database contains spam signatures for all known spams (gathered by spam collectors and other sources).
Bayes Filter Database	The version of the Bayes Filter Database currently in use by Lotus Protector for Mail Security. The Bayes Filter Database is pre-trained by IBM to identify spam using words and other tokens that routinely appear in legitimate email streams.
Spam Heuristics	The version of the Spam Heuristics signatures currently in use by Lotus Protector for Mail Security. The Spam Heuristics signatures use rules describing the characteristics of spam in order to assess incoming email messages (headers and body text) and attachments.
Spam Keyword Analysis	The version of the Spam Keyword Analysis signatures currently in use by Lotus Protector for Mail Security. The Spam Keyword Analysis signatures include standard keywords and patterns (regular expressions) that are typically found in spam email messages.
Phishing	The version of the Phishing signatures currently in use by Lotus Protector for Mail Security. IBM uses a variety of methods to detect phishing email messges. The URL checker is able to detect links to banking and other commercial sites in all spam coming from the spam collectors. Phishing email messages also show typical heuristics compared to regular spam, and are categorized separately from regular spam in the filter database.
CAL Scripting	A module that contains highly specialized algorithms for detecting certain types of spam. **Note:** This module is maintained and updated by IBM.
Antivirus Signatures	The version of the Antivirus signatures currently in use by Lotus Protector for Mail Security. The Antivirus signatures contain an IBM defined list of virus definitions for well known viruses. Lotus Protector for Mail Security scans email traffic for these signatures and takes the appropriate action to quarantine any infected files.

System status

The System status tab shows the current status of Lotus Protector for Mail Security.

Table 10. System status settings

Setting	Description
Base Image Revision	The base or initial version of the Lotus Protector for Mail Security software. **Note:** The base version is the software version shipped with Lotus Protector for Mail Security, or the software version of the most recent system backup.
Firmware	The firmware version of the Lotus Protector for Mail Security software that is currently installed.
Uptime	The length of time that Lotus Protector for Mail Security has been online.
Last Restart	The date Lotus Protector for Mail Security has been turned on or was restarted, given in the `yyyy-mm-dd hh:mm:ss` format (for example, 2011-12-31 12:45:10).
System Time	The current system time of the machine running the Lotus Protector for Mail Security software.
Total Network Interfaces	The number of physically installed network interfaces on your Lotus Protector for Mail Security.
Bound IP Addresses	The IP addresses currently in use by Lotus Protector for Mail Security as configured by the Administrator.
Last System Backup	The date that the last system backup was created, given in `yyyy-mm-dd hh:mm:ss` format (for example, 2011-12-31 12:45:10).
Content Analysis Library	The list of modules currently installed for the Content Analysis Library (CAL), which are used to determine the categories of email messages passing through Lotus Protector for Mail Security.

Section A: Recommended tasks

This section provides procedures that you should follow after you have installed and configured initial settings for Lotus Protector for Mail Security.

Installing license keys

The Updates and Licensing page (**Updates** > **Updates and Licensing**) provides important information about the current status of your license keys, including expiration dates.

About this task

You can view information for each license you purchase for Lotus Protector for Mail Security:

Table 11. License key settings

Setting	Description
Serial Number	The serial number of the license key. **Note:** Each license key has its own serial number, unique to the Identity and the OCN.
OCN	The Order Confirmation Number (OCN) or your customer number with IBM.
Expiration	The date the license expires, given in the `yyyy-mm-dd` format: 2011–12–31.
Maintenance Expiration	The date the maintenance agreement expires, given in the `yyyy-mm-dd` format: 2011–12–31.

Procedure

1. Click **Updates** > **Updates and Licensing** in the navigation pane.
2. Click the **Licensing** tab.
3. Click **Install a new license key**.
4. Locate or provide the license key.
5. Click **Install Key**. Lotus Protector for Mail Security installs the license key file in the appropriate directory.

Backing up configuration settings

The process for updating Lotus Protector for Mail Security is designed to keep it up-to-date while taking the precautionary action of backing up your system before you install updates that alter original configuration settings.

About this task

Create a settings snapshot file of the original configuration settings for Lotus Protector for Mail Security before you apply firmware updates or change your configuration settings. You can also create additional settings snapshot files later if you want to use different configuration settings or test new policy settings.

The default settings snapshot file, `factoryDefault.settings`, contains the original Lotus Protector for Mail Security settings. You should create a settings snapshot file before you change your configuration settings.

Procedure

1. Click **Backup and Restore** > **System** in the navigation pane.
2. Click **Manage Configuration Backups**.
3. In the **Configuration Backups** section, choose an option:

Option	Description
Create a snapshot file	1. Click **New**. 2. Type a name for the snapshot file, and then click **Create**.
Restore a snapshot file	Select the snapshot file you want to restore, and then click **Restore**.
Delete a snapshot file	Select the snapshot file you want to delete, and then click **Delete**.
Upload a snapshot file	1. Click **New**. 2. Type the name of the snapshot file you want to upload, and then click **Upload**.
Download a snapshot file	Select the snapshot file you want to download, and then click **Download** to copy the file to your local computer.

Applying mail security updates

Before you begin to use Lotus Protector for Mail Security, you should apply the latest mail security updates to its database. You can configure Lotus Protector for Mail Security to automatically retrieve updates from the IBM Download Center.

About this task

The mail security updates provide daily updates of URLs and spam signatures for Lotus Protector for Mail Security.

Important: You should update your local mail security database at least once daily to keep it current.

Procedure

1. Click **Updates** > **Updates and Licensing** in the navigation pane.
2. Click **View versions online** at the bottom of the page to access a list of each update and its contents.
3. After you have downloaded and installed your license keys, click **Configure Automatic Updates**.
4. Make sure **Automatically Update Mail Security Database** is enabled in the **Mail Security Database Updates** section.
5. Click **Save Changes**.

Configuring the local firewall

You might need to configure the local firewall for Lotus Protector for Mail Security in order to control access to the provided services from any network attached to a specific network interface.

About this task

Use options on this page to control access to services provided by Lotus Protector for Mail Security. In order for Lotus Protector for Mail Security to function properly, you might need to change settings on your corporate firewall or any other firewall deployed between Lotus Protector for Mail Security and the service provider, such as a directory service.

Procedure

1. Click **System** > **Firewall** in the navigation pane.
2. Verify services for Lotus Protector for Mail Security are enabled correctly or are accessible:

Table 12. Required network services

Service	Port number	Description
SMTP	TCP 25	Enables access to the SMTP service through the specified network interfaces, to allow internal and external SMTP servers to relay email messages to Lotus Protector for Mail Security.
HTTPS	TCP 443	Enables access to Lotus Protector Manager from networks attached to the specified network interfaces.
SSH	TCP 22	Enables an SSH client (for example, PuTTY) to connect to the command line interface for Lotus Protector for Mail Security.
Access to End User Interface	TCP 4443	Enables access to the End User Interface where recipients of email messages can release quarantined email messages from message stores and manage their block lists and allow lists.
SNMP	UDP 161	Enables access to the SNMP agent of Lotus Protector for Mail Security in order to collect data about its current status using SNMP Get.

Table 12. Required network services (continued)

Service	Port number	Description
Database access	TCP 5432	Enables the clients of a Mail Security cluster to access the database of the central appliance **Attention:** Make sure this option is enabled before you create a Mail Security cluster or an appliance joins a Mail Security cluster.
Cluster communications	TCP 4990	Enables members of a Mail Security cluster to communicate with this host. **Attention:** Make sure this option is enabled before you create a Mail Security cluster or an appliance joins a Mail Security cluster.
ICMP ping		Enables Lotus Protector for Mail Security to answer ICMP echo requests (ping) on the specified network interfaces.

Defining Administrator email addresses and system notification accounts

You must set up the email addresses for the Administrator of your local mail environment and to define the email accounts used by Lotus Protector Manager to send status notification messages for undeliverable email messages or quarantine reports.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Global** tab.
3. Provide the following information:

Option	Description
Root Domain	The primary mail domain of the SMTP service. For example, this value is sent by the SMTP service in return of an HELO/EHLO command by an SMTP client.
Postmaster	The email address of the person responsible for the mail system in the organization.
Error Admin	The email address of an Administrator who should be notified of permanent delivery errors. **Note:** If you leave the field blank, only the original sender of the email message receives a notification if an attempt to deliver the email message was not successful.
Temporary Error Admin	The email address of an Administrator who should be notified of temporary delivery errors. **Note:** If you leave the field blank, only the original sender of the email message receives a notification if an attempt to deliver the email message was not successful.
Send New Email As	The email address used by Lotus Protector Manager as the sender for locally generated email messages.
Send Quarantine Report As	The email address used by Lotus Protector Manager as the sender of the quarantine report.

4. Click **Save Changes**.

Section B: Optional tasks

This section provides optional procedures that you can follow after you have installed and configured initial settings for Lotus Protector for Mail Security.

Changing passwords for Lotus Protector for Mail Security

This topic explains how to change the passwords for Lotus Protector for Mail Security accounts that you or another Administrator initially set up from the Setup Assistant.

Before you begin

To change a password, you must know the current password.

About this task

When you configure Lotus Protector for Mail Security, you must supply passwords for these accounts:

Table 13. Lotus Protector for Mail Security passwords

Account	Purpose
root	Enables you to access the operating system of Lotus Protector for Mail Security.
Admin	Enables you to access the Setup Assistant and Lotus Protector Manager for the Lotus Protector for Mail Security.

Procedure

1. Click **System** > **Admin Passwords** in the navigation pane.
2. Choose an option:

If you want to change the...	Then...
root password	1. In the **root** section, type the current password. 2. Click **Enter Password**. 3. Type and confirm the new password.
Admin password	1. In the **Admin** section, type the current password. 2. Click **Enter Password**. 3. Type and confirm the new password.

3. Click **Save Changes**.

Changing date and time settings

This topic explains how to change the date and the time of Lotus Protector for Mail Security, and to enable the network time protocol (NTP) to synchronize Lotus Protector for Mail Security time with a network time server.

About this task

The Time page always contains the last manually configured values for date and time options, not the actual date and time. When you save the settings, Lotus Protector for Mail Security is set to the currently configured values, whether you have changed them or not.

Important: To avoid resetting the time and date to the previously configured values, update the time and date before you save the settings.

Procedure

1. Click **System** > **Time** in the navigation pane.
2. Choose an option:

If you want to...	Then...
Change the date and time of Lotus Protector for Mail Security	1. Click the **Date and Time** arrow to see the calendar. 2. Select the correct month and date. **Tip:** Use the arrows at the top to change the month and year in the calendar. 3. Select the hour and minutes in the **Time** boxes. 4. Click outside the calendar to close it. 5. Click the **Time Zone** arrow and select the correct time zone for your region. 6. Click **Save Changes**.
Enable the network time protocol (NTP)	**Note:** NTP synchronizes the configuration time with a network time server. 1. Select the **Enable NTP** check box, and then type the name of the NTP server. 2. Click **Save Changes**.

Note: When you schedule a task, you use an absolute value to specify when it will run (for example, you schedule a task to run on 2011-10-10 at 10:10). Changing the time of the Lotus Protector for Mail Security system can affect when a scheduled task runs. If you set the time of your system forward, all tasks that are scheduled in the timeframe between the old value and the new value run immediately. Setting the time of your system backwards delays scheduled tasks. Recurring tasks will not run if you set the system time forward to a value beyond the configured time.

Providing realtime virus scanning services to ICAP-compatible clients

This topic explains how to enable Lotus Protector for Mail Security to provide realtime virus scanning services to ICAP-compatible clients such as IBM Connections, IBM Lotus Quickr®, or Squid 3.x.

About this task

For specific instructions on enabling virus scanner services for IBM Connections or IBM Lotus Quickr, visit the IBM Connections Wiki site at http://www.lotus.com/ldd/lcwiki.nsf or the IBM Lotus Quickr Wiki site at http://www.lotus.com/ldd/lqwiki.nsf.

Procedure

1. Click **System** > **ICAP Server** in the navigation pane.
2. Select the **Enable ICAP Server** check box.
3. Type the server port for the ICAP Server, typically port 1344.

Managing network interfaces

If needed, you can change the initial configuration of the management port, default gateway port, and DNS servers.

Why you would need to change network settings?

You might need to change the network configuration settings for the following reasons:

- Your company's network policy has changed
- Your company has relocated
- You have changed your Internet Service Provider
- You have changed addresses
- You want to specify DHCP settings
- You want to change DNS settings

Configuring external interfaces

You can use a DHCP server for the external interfaces, or manually set the IP address and DNS servers for each network interface.

Procedure

1. Click **System** > **Networking** in the navigation pane.
2. Click the **External Interface** tab.
3. Select the **Enabled** box.
4. Type the host name of Lotus Protector for Mail Security, using this format: `appliance.example.com`
5. Select an IP address type:

Option	Description
DHCP	1. Select **DHCP**. 2. If needed, select **Enable Mac Cloning**, and then type 6 hex pairs, separated by colons: `AA:BB:CC:11:22:33`
Static	1. Select **Static**. 2. Type the IP address for the external interface of Lotus Protector for Mail Security, and then press `ENTER`. 3. Type the subnet mask (network mask) value. 4. Type the gateway IP address.

6. Select a setting for your Domain Name Server (DNS):

Option	Description
Use Dynamic Settings (enabled)	Enables dynamic settings for your Domain Name Server. **Tip:** You can only use dynamic settings with DHCP or PPPoE; you cannot use it if your external interface uses a static IP address.
Use Dynamic Settings (disabled)	Uses static settings for your Domain Name Server: • Type the IP address for **Primary DNS Server**, **Secondary DNS Server**, **Tertiary DNS Server**, using the dotted decimal format: `127.0.0.1`

7. Click **Save Changes**.

Configuring internal interfaces

You can configure which network interface Lotus Protector for Mail Security uses.

Procedure

1. Click **System** > **Networking** in the navigation pane.
2. Click the **Internal Interface** tab.
3. Click **Add**.
4. Select an interface from the list.

   Tip: ETH0 is always the primary internal interface.
5. Select the **Enabled** box.
6. Type the following IP addresses or values:
   - Destination IP address
   - Subnet mask value
   - Gateway IP address
7. Click **Save Changes**.

Routing network traffic

Lotus Protector for Mail Security routes traffic on the networks and subnetworks connected to it. You must assign IP network settings to the interfaces, including IP addresses, subnetwork mask, and gateway router IP addresses.

How Lotus Protector for Mail Security routes traffic

Lotus Protector for Mail Security routes traffic on the networks and subnetworks connected to it. You must assign IP network settings to the interfaces, including IP addresses, subnetwork mask, and gateway router IP addresses.

In routing mode, one of the basic functions of Lotus Protector for Mail Security is to route network traffic from one physical network to another network. These networks are connected to the multiple interfaces of Lotus Protector for Mail Security.

For routing to occur, you must enable the interfaces and physically connect them to their corresponding networks. You must also assign network information to the interfaces such as IP addresses and subnet masks. The external and internal interfaces are enabled and configured during the initial setup. You can use additional internal interfaces as needed to connect Lotus Protector for Mail Security to other internal networks.

Route precedence in the Routing table

If there are two or more routes for identical destinations, the most specific route in the Routing table takes precedence.

In this example, a packet destined to the host 10.1.1.1 uses the 192.168.1.2 route.

Table 14. Example of a Routing table

Destination	Subnet mask	Gateway IP address
10.0.0.0	255.0.0.0	192.168.1.1
10.1.1.0	255.255.255.0	192.168.1.2
10.1.0.0	255.255.0.0	192.168.1.3

Adding a static route

You can add a static route to Lotus Protector for Mail Security.

Procedure

1. Click **System** > **Routes** in the navigation pane.
2. Click the **Add** icon.
3. Type the following IP addresses or values:
   - Destination IP address
   - Subnet mask value
   - Gateway IP address
4. If needed, type a value in the **Metric** field.

   Note: The Metric (or hop count) indicates the number of routes or segments between the source and destination.
5. Click **OK**, and then click **Save Changes**.

Configuring system routing manually

This topic explains how the Manage network routes using Management Interface option affects how system routes are handled by the Routing policy.

Procedure

1. Click **System** > **Routes** in the navigation pane.
2. For the **Manage network routes using Management Interface** option, choose one of the following:

Option	Description
Enable the check box	All system routes will be set up as you have the routes configured in the Local Management Interface (LMI). Any customization made from the command line is overwritten.
Clear the check box	All system route settings remain as is; no system routes are deleted or created. This scenario works well with network environments that require special routing settings that are not currently available in the LMI. **Example:** You want to use the console to add routing settings that are not available in the LMI (`/etc/sysconfig/network/routes`). Lotus Protector for Mail Security will detect the system routing settings that you have added, but will not change them.

3. Click **Save Changes**.

Chapter 2. SMTP configuration

This chapter describes how to set up Lotus Protector for Mail Security to process mail traffic.

Deploying Lotus Protector for Mail Security

The Administrator who sets up Lotus Protector for Mail Security must make sure all incoming SMTP traffic is routed through Lotus Protector for Mail Security before the traffic is delivered to internal mail servers.

This topic explains methods that are used for Internet mail exchange and how these methods affect or relate to setting up Lotus Protector for Mail Security. You should read this information if you are not familiar with Internet mail exchanger deployments and configuration.

Fast path: If you are only interested in how MX records affect your setup of Lotus Protector for Mail Security, go to the paragraphs labeled **Fast path** for a brief explanation of that section.

DNS MX records

When an email message is sent through the Internet, the sender of the email message must determine the receiving host name responsible for processing email messages for a domain, which is the domain part of an email address (for example, `ibm.com` in `joe@ibm.com`). In order to determine the receiving host name, the sender queries the recipient's DNS server for Mail eXchanger records (MX records) belonging to the domain found in the domain part of the recipient's email address. This record typically points to a fully qualified host name (for example, `server1.ibm.com`) that resolves to an actual IP address (known as an *A record*).

MX records contain an attribute known as an *MX preference*. An MX preference is used by the sender to determine the priority of a mail server, in case there are multiple hosts responsible for a single domain. By default, the host will choose the mail server with the lowest MX preference value (indicating the lowest cost like metric in IP routes) and will fail over to another referenced host with the lowest preference. If two or more MX records have an identical preference value, the sender might choose a mail server at random (depending on the implementation of the server). Identical preferences for several MX record entries is commonly used to distribute load among multiple servers.

Table 15. DNS MX record configuration with failover and load distribution example

Responsible mail exchangers	MX preference
server1.ibm.com	10
server2.ibm.com	20
server3.ibm.com	20

For example, assume the MX records for `ibm.com` are configured like the values shown in Table 15. An SMTP server will first try to deliver an email message for `joe@ibm.com` to `server1.ibm.com`. If the SMTP server is not able to connect to `server1.ibm.com`, it will choose to deliver the message, at random, to either `server2.ibm.com` or `server3.ibm.com`.

Fast path: SMTP servers must know where to deliver email messages for your domains. Make sure you have set up MX records for all of your domains. Depending on your deployment scenario (see the section on Inbound SMTP traffic), these MX records should point to a host name (*A record*) that in turn points to a public IP address owned by Lotus Protector for Mail Security.

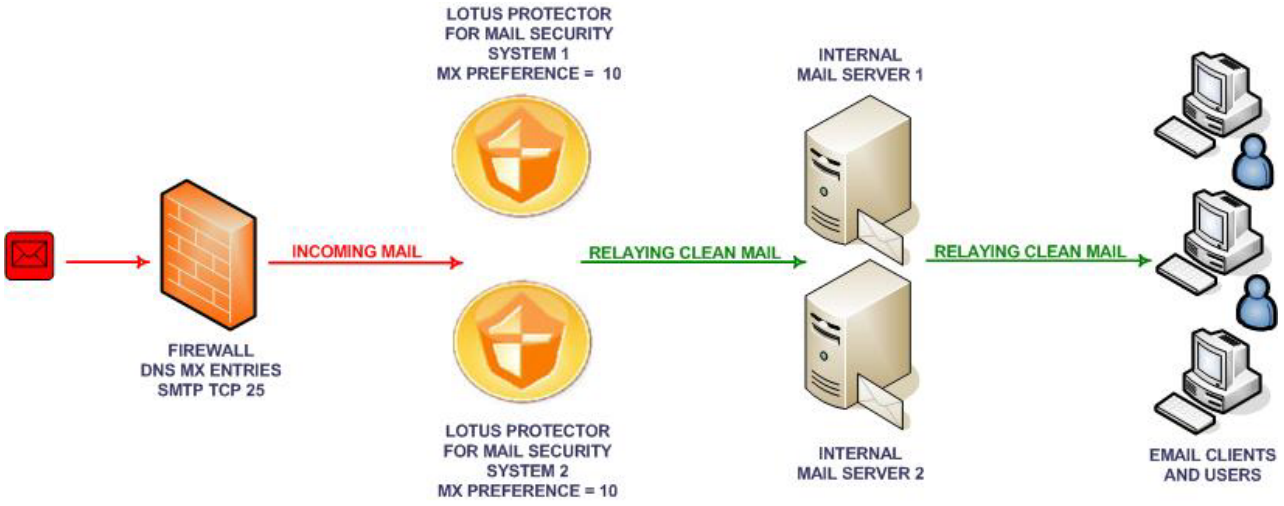
Note: DNS population can take up to three days on the Internet. If you must change DNS entries for your environment, make sure you can reroute SMTP traffic to obsolete IP addresses on Lotus Protector for Mail Security during this time.

Inbound SMTP traffic

When a host tries to deliver an email message to a destination SMTP server, as specified by DNS MX records, it tries to establish a connection with the destination host. By design, an email message is not always delivered directly to its destination by the server. The server might deliver the email message to another SMTP server instead, which is then responsible for delivering the email message. This method is known as *relaying*; an SMTP server that allows relaying is called an *SMTP relay*.

Lotus Protector for Mail Security acts as an SMTP relay when it allows hosts to relay email messages to your users. Unlike other SMTP relays, Lotus Protector for Mail Security does not store and forward email messages to internal mail servers. Instead, it stores incoming email messages locally until those messages have been analyzed and processed. When an email message has been analyzed, delivery of the email message is either allowed or declined, depending on your policy rules. If delivery of an email messages is allowed, Lotus Protector for Mail Security will relay the email message to internal SMTP servers where users connect to access their email accounts.

Most often, Lotus Protector for Mail Security is deployed to receive incoming email messages directly from the Internet, meaning SMTP traffic (on the IP layer) is routed to Lotus Protector for Mail Security by a gateway or firewall.



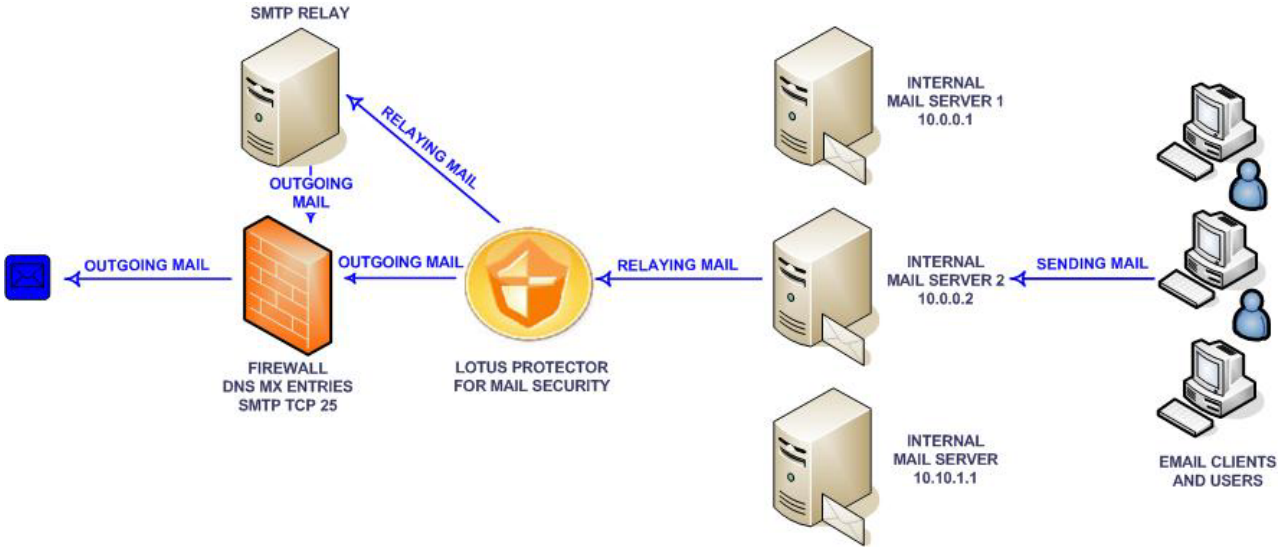
However, in some scenarios it might be useful or necessary for you to relay incoming email messages through other SMTP servers before passing the messages to Lotus Protector for Mail Security (for example, in cases where you must perform additional analysis or to compensate for strong peaks in email traffic or network constraints).

Fast path: From a deployment perspective, make sure that all email messages from the Internet can be relayed to Lotus Protector for Mail Security. You might need to adjust firewall rules for SMTP traffic (by default, TCP port 25), to add appropriate forwarding rules at your SMTP relays, or to reconfigure other preceding devices.

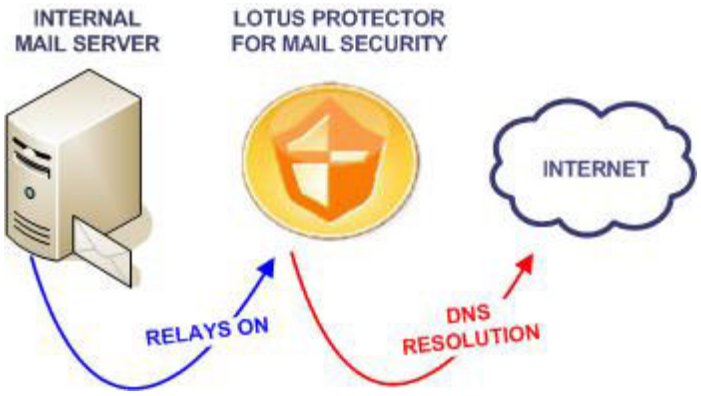
Important: Lotus Protector for Mail Security works as an SMTP relay. It does not analyze data streams on your network and cannot forward or route IP traffic because it is not a gateway. email messages must be relayed via Lotus Protector for Mail Security; inline deployment is not a deployment option for Lotus Protector for Mail Security.

Outbound SMTP traffic

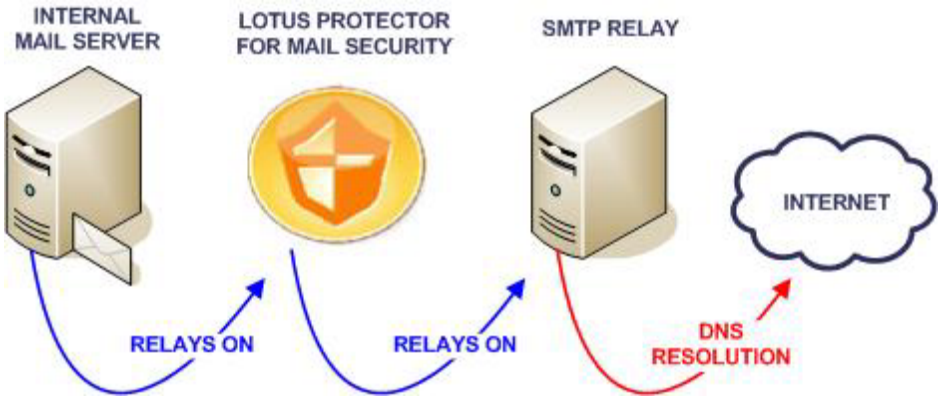
You can also use Lotus Protector for Mail Security to handle outbound SMTP traffic in which it analyzes and relays email messages that are leaving your environment. For example, you can use Lotus Protector for Mail Security to prevent confidential data from leaving your environment by email message, to enforce encrypted delivery of confidential data, to relay email messages to other SMTP servers in case of network constraints, or to generate statistics on outbound traffic.



As mentioned in the section on DNS MX Records, SMTP servers must determine where to deliver email messages to a specific domain. In general, SMTP servers try to deliver email messages using DNS resolution and by communicating directly to one of the specified servers.



You can also configure SMTP servers to relay all email messages (or only a subset of email messages to configured domains) to other SMTP relays, which in turn are responsible for delivering those email messages. You set up this behavior by adding forwarding rules to the configuration of the SMTP server.



Fast path: If you want to set up Lotus Protector for Mail Security to act as an outbound relay, you must add forwarding rules to your internal mail servers that allow them to relay outgoing email messages to Lotus Protector for Mail Security. Because of the built-in anti-relay check, you must add the internal mail servers as relay hosts for Lotus Protector for Mail Security, in order for Lotus Protector for Mail Security to accept email messages to any domain from these hosts. Choose whether Lotus Protector for Mail Security should deliver email messages directly using DNS resolution or if outgoing email messages should be forwarded to other SMTP relays that in turn will take care of delivery.

Note: Lotus Protector for Mail Security will automatically fall back to DNS resolution for domains that do not have a forwarding rule.

Configuring SMTP service settings

You can configure how the SMTP module of Lotus Protector for Mail Security will behave and where email messages received by local domains should be delivered. Additionally, you can set up some filtering options on the SMTP level.

Configuring general SMTP service settings

This topic explains how to configure the behavior of the SMTP service when it is receiving email messages from other SMTP servers.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Receiving SMTP** > **Settings** tab.
3. Provide the following information:

Option	Description
Enable Logging	Instructs the SMTP service to write information about email message deliveries to a log file. This log file is named `smtp-yyyymmdd0000`. **Note:** The SMTP service logs several lines to its log file for each delivery attempt. For successful delivery attempts, the SMTP service writes one log entry for each recipient of an email message and, additionally, one log entry if the transmission of the email message was successful.
Port	Specifies the port number on which the SMTP service is listening. **Default:** port 25 **Attention:** If you change this value, other SMTP servers might not be able to transmit email messages to Lotus Protector for Mail Security, because those servers are trying to open a connection to the default SMTP port (which is TCP port 25). If you must change the listening port of the SMTP service, consider adding a translation rule at the firewall.
Max Recipients per Message	SMTP server might try to transmit an email message to multiple recipients within a single transaction. This value regulates the maximum number of recipients allowed in a single message transaction. **Default:** 100 recipients
Max Messages per Session	An SMTP server might try to deliver several email messages to Lotus Protector for Mail Security using the same connection. This value defines how many email messages an SMTP server is allowed to transmit, before it is forced to establish a new connection to Lotus Protector for Mail Security.
Session Timeout	Specifies the amount of time before an SMTP session times out. A timeout can occur when the SMTP service does not receive any data from the SMTP server within the configured amount of time. In this case, the SMTP service closes the connection to the peer. **Default:** 60 seconds

Option	Description
Max Message Size (KB)	Defines the maximum size of an email message, in Kilobytes, that the SMTP service will accept from other SMTP servers. **Note:** If you set this value to zero, the SMTP service will allow any message size.
Allow NULL Sender	If enabled, the SMTP service accepts email messages even if the SMTP server did not specify an originator with the `MAIL FROM:` command. If disabled, the SMTP service rejects the transmission.
Max SMTP Errors per Session	Defines how many protocol errors, such as syntax errors, an SMTP server is allowed to cause before the SMTP service enforces the termination of the connection.
Check Mailer Domain	Select if you want the SMTP service to perform a DNS lookup on an MX record for the domain of the sender's email address, as provided by the `MAIL FROM` command, for validation. The SMTP service will only accept email messages from senders whose email address domain part has a valid MX record.
Max MTA Hops	Defines the maximum number of SMTP servers an email message is allowed to be relayed by so far, determined by the number of Received Fields in the Header of the message. If this number exceeds the defined limit, the SMTP service rejects the transmission. **Default:** 20
Enable Reverse DNS Lookup	Select if you want the SMTP service to determine if the IP address of an SMTP server resolves to an actual valid host name (meaning a DNS record exists that is pointing to the IP address of the peer). If the SMTP service cannot resolve the host name of the SMTP server, it will not accept any email messages from this SMTP server.
Return Path Domain Check	Select if you want the SMTP service to verify that the domain part of the sender's email address, provided by the `MAIL FROM` command, is compliant with RFC2821 Section 4.1.2. This means that the domain part only contains letters, numbers, hyphens, and dots in a specific format.
Helo Domain Check	Select if you want the SMTP service to verify that the argument, provided by the HELO/EHLO command, is compliant with RFC2821 Section 4.1.2. This means that the domain part only contains letters, numbers, hyphens, and dots in a specific format or an IP address enclosed in square brackets.

Option	Description
Forward Path Domain Check	Select if you want the SMTP service to verify that the domain part of the recipient's email address, provided by the `RCPT TO` command, is compliant with RFC2821 Section 4.1.2. This means that the domain part only contains letters, numbers, hyphens, and dots in a specific format.
SMTP Greeting	Specifies the welcome message (greeting) the SMTP service sends to an SMTP client when a connection is established, meaning that it is ready to process commands.
Received Header	The SMTP service adds information to the email message header (Received Field) such as when and by whom the email message was transmitted. You can regulate the amount of information in this header field using one of the following levels: • Standard (client IP shown, server IP not): The SMTP service adds the IP address of the SMTP server to the header field, but omits its own IP address. • Verbose (client IP shown, server IP shown): The SMTP service adds the IP address of the SMTP server, as well as its own IP address to the header field. • Strict (no IP shown): The SMTP service does not add any IP addresses at all (not its own or the IP address of the sender) to the header field. **Important:** If you set the Received Header Type to Strict (no IP shown), and then open ports on your corporate firewall to receive SMTP traffic, the analysis modules in the Sender Policy Framework will not work because these modules rely on information in the received header.

Configuring Transport Layer Security (TLS) settings

This topic explains how to configure options that influence the behavior of the SMTP service if TLS encryption is requested by an SMTP client.

Before you begin

To use the options described in the following procedure, you must install an SMTP TLS certificate. See *Uploading TLS certificates* for more information.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Encryption (TLS)** tab.
3. Enable these settings if you want to use TLS:

Option	Description
Require Certificates	Instructs the SMTP service to request a certificate from the SMTP server. If the SMTP server does not supply a certificate, delivery of email messages from this server is prohibited.
Verify Certificates	If enabled, the SMTP service tries to verify the certificate of the SMTP server (if it has sent one). If the verification process fails, the SMTP service will not accept any email messages from the SMTP server.
Allow Self-Signed Certificates	The SMTP service will accept a certificate from the SMTP servers that have not been signed by a certificate authority (for example, VeriSign, GlobalSign, CAcert).
Always Try TLS	If enabled, the SMTP service uses Transport Layer Security (TLS) in SMTP communications. Also known as opportunistic TLS, the server will always try to connect to the target server using the TLS protocol. If the target server supports TLS, SMTP traffic is encrypted. If TLS is not supported by the target server, the system will fall back to unencrypted communication, unless the delivery of specific email messages explicitly requires TLS (requested by a Response Object in the policy system). In this case, the SMTP service will not deliver the email message and sends a notification back to the originator.

Attention: TLS encryption support for receiving email messages is not enabled at the SMTP service unless you have uploaded a key file and a certificate on the TLS Certificates page (**SMTP** > **TLS Certificates**).

Defining IP addresses for local domains and relay hosts

This topic explains how to specify the domain and IP number range for your organization, and to set up relay hosts that relay all outbound email messages through a specific mail host.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Receiving SMTP** > **Settings** tab.
3. Provide the following information for local domains:

Option	Description
Domain	Defines the domain part of an email address (for example, `example.com` from `joe@example.com`) for which the SMTP service is accepting email messages. **Note:** The use of the entry `example.com` does not necessarily mean that the SMTP service will accept email messages from subdomains of `example.com` (for example, `department.example.com`). If you want the SMTP service to accept email messages for specific subdomains, you must add a separate entry for this subdomain. If you want the SMTP service to accept email messages for all subdomains, you must add an additional entry `.example.com`.
Mailserver(s)	Specifies the IP address or host name of an SMTP server for which email messages from a specific domain should be forwarded to after analysis. Use a single entry or a list of entries separated by semicolons (**;**). A list will cause the SMTP service to perform a failover if the first host in the list is not available. If the list is prefixed with an #, the SMTP service will load balance over all SMTP servers in the list.

4. Provide the following information for relay hosts:

Option	Description
IP Address	Specifies the IP address of a host or network that is allowed to relay email messages to Lotus Protector for Mail Security.
Subnet Mask	Defines a range of IP addresses within a network that are allowed to relay email messages.

Note: Do not delete the entry `127.0.0.1/255.255.255.255` because it allows Lotus Protector for Mail Security itself to generate and deliver email messages, such as quarantine reports or Non Delivery Reports (NDR), to other hosts.

Example: If you want a single host to relay email messages to Lotus Protector for Mail Security, add the IP address of this host (for example, 192.168.123.100) and use the Subnet Mask 255.255.255.255 with this entry.

If you want to allow an entire class C network to relay to Lotus Protector for Mail Security, use the IP address 192.168.123.0 with the Subnet Mask 255.255.255.0.

Configuring a global IP access list

This topic explains how to configure a list of IP addresses that are allowed or denied access at the start of an incoming SMTP connection.

About this task

The behavior of the Global IP Access List is also affected by whether you are using border IP addresses, which are IP addresses that specify the outer border of the trusted network around Lotus Protector for Mail Security. See the "Configuring DNSBL settings" on page 29 topic for more information about using border IP addresses.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Receiving SMTP** > **Global IP Access List** tab.
3. In the **Allow List** section, specify a list of hosts or networks that have been granted access to the SMTP server:

Option	Description
IP Address	Specifies the IP addresses that have been granted access to the SMTP server. Use CIDR notation to specify a block of IP addresses. For example: 123.123.123.123/14. The entry after the slash is the prefix length and is a number from 1 to 32.
Subnet Mask	Specifies a range of affected systems for the subnet mask of the IP address entered above.

When you add an IP address to the Allow List, every IP address from that sender is excluded from further IP-based checks (such as DNSBL checks at the SMTP level, Dynamic Host Reputation checks at the SMTP level, and RBL/DNSBL checks at the policy level). The IP addresses in the Allow List take precedence over the IP addresses in the Deny List.

Example:

Deny List uses 123.123.123.0/24 (123.123.123.1 - 123.123.123.255)
Allow List uses 123.123.123.123/32

Lotus Protector for Mail Security will deny access for 123.123.123.1 - 123.123.123.122, allow access for 123.123.123.123, and deny access for 123.123.123.124 - 123.123.123.254.

4. In the **Deny List** section, manually add hosts or networks to a list of systems that are not allowed access to the SMTP server:

Option	Description
IP Address	Specifies the IP addresses that are not authorized to access the SMTP server and will not be allowed to connect. Use CIDR notation to specify a block of IP addresses. For example: 123.123.123.123/14. The entry after the slash is the prefix length and is a number from 1 to 32.
Subnet Mask	Specifies the range of affected systems for the subnet mask of the IP addresses entered.

Rejection handling for IP addresses on the Deny List:

- Reject with Error: The SMTP service rejects deliveries of email messages from the sender and returns the given Error Code in combination with the defined Error Message.
- Silent Drop: The SMTP service rejects an incoming email message but does not notify the sender of the email that the email message has been rejected. This method is used to prevent spammers from probing for valid email addresses.

Configuring DNSBL settings

This topic explains how to configure a list of IP addresses that are blocked because these addresses allow spam to be sent from them, and to set scores for each available DNSBL (Domain Name Server Block List) server on your network.

About this task

DNSBL border IPs are IP addresses that specify the outer border of the trusted network around Lotus Protector for Mail Security. The following table lists the IP addresses that are considered DNSBL border IP addresses for Lotus Protector for Mail Security:

Table 16. DNSBL border IP addresses

DNSBL border IP address	Where to find
Servers that relay to local domains	**SMTP** > **Configuration** > **Receiving SMTP** > **Settings** > **Local Domains**
Servers that relay through Lotus Protector for Mail Security	**SMTP** > **Configuration** > **Receiving SMTP** > **Settings** > **Relay Hosts**
Servers that Lotus Protector for Mail Security forwards to	**SMTP** > **Configuration** > **Sending SMTP** > **Delivery** > **Forward**
A user-specified list of IP addresses separated by semicolons	`host_reputation.border_ips`

Important: You can use border IP addresses if Lotus Protector for Mail Security is receiving email messages directly from hosts on the Internet. However, you will not be able to use border IP addresses if Lotus Protector for Mail Security is behind an SMTP relay.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Receiving SMTP** > **DNSBL Settings** tab.
3. Select the **Enable** box.
4. Provide an error code and an error message.
5. Click the **DNSBL Settings** button.
6. In the **DNSBL Lists** area, set a threshold value. If the sum of all DNSBL server match scores exceeds this number, the analyzed email message is considered a match for the Spam DNSBL analysis module.
7. Click **Add**.
8. Select the **Enabled** box.
9. Type the name of the DNSBL server, and then enter the match score. The match score specifies the value that is added to the total score if this particular DNSBL server returns a positive result. This value can be used to fine tune the mechanism, if you use DNSBL servers with different reliabilities.
10. Click **OK**, and then click **Save Changes**.

Configuring Recipient Verification

Recipient Verification enables the SMTP service to immediately block email messages that are sent to a user who does not exist in your organization.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Receiving SMTP** > **Recipient Verification** tab.
3. Select the **Enable Recipient Verification** box.
4. Choose how Lotus Protector for Mail Security should handle recipients who are rejected:

Option	Description
Reject with Error	Lotus Protector for Mail Security returns the given error code and error message to the SMTP client. The sender knows which SMTP addresses are valid, and which can be acceptable or unacceptable behavior.
Silent Drop	The SMTP service rejects an incoming email message, but does not notify the sender of the email that the email message has been rejected. This method is used to prevent spammers from probing for valid email addresses.

5. Provide an SMTP error code and an SMTP error message.
6. Choose the access type for the recipients:

Option	Description
Denied	All recipients who are not on the list of recipients are rejected.
Allowed	All recipients who are not on the list of recipients are allowed. You can either build a list of allowed recipients and reject all others, or build a list of rejected recipients and allow all others.

Attention: You can also use user-generated SMTP domain lists and SMTP address lists with Recipient Verification. You must add the list of file names (comma-separated list including the full path) to the file `/etc/recipientverificationd.conf`.

Any files that are placed in the directory `/var/lib/recipientverificationd` are deleted when you save a configuration. You should use another directory, for example, `/var/lib/recipientverificationd/user`.

Configuring Zero Level Analysis (ZLA)

Zero Level Analysis (ZLA) is a classification method that Lotus Protector for Mail Security uses on incoming email messages.

About this task

Although many junk messages are rejected at an early stage of message delivery, ZLA analyzes email messages during transmission where they are either discarded or rejected by the SMTP service.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Choose which category ZLA uses to identify incoming email messages:

Category	Description
Spam	any type of unsolicited bulk email message, such as phishing, advertisements, or malware.
Non Delivery Reports (NDR)	Non Delivery Reports are sent back to the originator as a response to a failed transmission of an email message in order to indicate that the specified recipient did not receive the message. Spammers often use spoofed email addresses as originators of email messages. If a server rejects this type of message (for example, because the recipient of the message does not exist), it could cause the owner of a spoofed address to receive many Non Delivery Reports in error. **Attention:** Be careful when you select a response for this category. Many Non Delivery Reports could be legitimate, for example, in the case where an originator of an email message has misspelled the recipients email address.

3. Defines how the SMTP service should handle email messages from a specific category:

Response	Description
Block Message	If selected, the SMTP service responds with an error message at the SMTP level to the sender's attempt, which signals that the transmission of the email message has been rejected.
Silent Drop	If selected, the SMTP service rejects an incoming email message, but does not notify the sender of the email that the email message has been rejected. This method is used to prevent spammers from probing for valid email addresses.

Response	Description
Tag as Spam	If selected, the SMTP service adds a new header field `X-ZLA-Header` to the email message. Possible values for this field include: • Spam: Indicates that an email message has been classified as unsolicited bulk email (Spam). • NDR: Indicates that an email message has been classified as a Non Delivery Report (NDR). Each values uses a suffix **;** `xxxx` that provides information about the matching analysis module. **Tip:** Adding a header field to the email message might be useful in combination with the policy system. You can add a new rule containing the Message Field Check analysis module that detects email messages of a certain type, and how to handle those messages (for example, store the messages in a quarantine store). **Note:** This response might have a slight impact on the performance of Lotus Protector for Mail Security, because it involves modifying incoming email messages.
None	If selected, email messages are accepted by the SMTP service, but are not altered by ZLA.

4. From the Block settings, configure how the SMTP service should reject email messages that ZLA has determined belongs to one of the given categories assigned a BLOCK response. SMTP servers will either log an error message or send a Non Delivery Report to the originator of an email message. You should provide a good description as to why an email message was rejected by Lotus Protector for Mail Security. The error replies that are sent back to the sender include a numerical error code followed by a textual description or comment. For example, 550 Blocked by ZLA.

Option	Description
Error Code	Defines the numerical error code that ZLA should use when it detects an email message that should be rejected. **Attention:** The numerical error codes used in SMTP replies are predefined in RFC 2821 Section 4.2: SMTP Replies. Because SMTP servers use this code to maintain their current state, make sure you choose a value that is compatible with these definitions. For instance, a reply code starting with a value of 4*yz* indicates a temporary error, but a reply code starting with a value of 5*yz* signals a permanent error.
Error Message	Defines the textual description or comment about the error. **Note:** Because SMTP uses ASCII characters, make sure your description or comment only contains characters that are part of the ASCII character set.

Configuring the dynamic host reputation filter

This topic explains how to configure Lotus Protector for Mail Security to use a host reputation rating mechanism that determines if an incoming email message should be rejected based on whether the sender of the email message has sent spam in the past.

About this task

Because this mechanism is based on the IP addresses of connecting hosts, you must configure a list of border IP addresses if you are using additional SMTP relays that receive email messages from the Internet and forward those messages to Lotus Protector for Mail Security. Otherwise, your internal SMTP relays might be added to the list of rejected hosts, preventing them from forwarding email messages to Lotus Protector for Mail Security.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Receiving SMTP** > **Dynamic Host Reputation Filter** tab.
3. Select **Enable Dynamic Host Reputation**.
4. In the **Rejected Host Handling** section, choose what method the SMTP service should use to reject the email message:

Option	Description
Reject with Error	The SMTP service rejects deliveries of email messages from a listed SMTP client and returns the given Error Code in combination with the defined Error Message to the SMTP client. **Note:** SMTP clients might try to deliver an email message repeatedly if a previous delivery attempt was rejected. These clients can monopolize available concurrent connections to the SMTP service.
Silent Drop	The SMTP service rejects an incoming email message but does not notify the sender of the email that the email message has been rejected. This method is used to prevent spammers from probing for valid email addresses. **Example:** A sender is known as a spammer by the Dynamic Host Reputation Filter. If you select the Reject with Error option, the sender receives the error message: "550 You are listed as a spammer (123.123.213.123)" or whatever message you have configured as a reply. If you select the Silent Drop option, the sender receives the message: "220 Welcome to...." and communicates with Lotus Protector for Mail Security, even though the sender is known as a spammer. **Note:** The Reject with Error option is a more efficient way of handling connecting hosts because it drops the connection earlier if there is high volume of traffic or a heavy load.
Tag	If the IP address of the SMTP client is on the list of rejected hosts, the filter inserts the following header field on the email message: `X-MSHostReputation:<IP address of the sender>`

5. In the **Dynamic Host Reputation Configuration** section, configure the filter to quarantine the IP addresses of hosts who send a high percentage of spam:

Option	Description
Analysis Window (minutes)	Sets the amount of time Lotus Protector for Mail Security should keep the classifications of analyzed email messages in order to determine if an SMTP client should be quarantined or not, based on the criteria defined below.
Quarantine Duration (minutes)	Sets the amount of time a host is quarantined, meaning the host is not allowed to deliver any email messages during this time frame.
Minimum SPAM/Phishing Hits	Specifies the minimum number of spam or phishing email messages Lotus Protector for Mail Security requires to ensure proper ratings.
SPAM/Phishing Percentage	Sets the ratio of spam (or phishing) email messages to other email messages that are necessary to consider a host a spammer.

6. Click **Save Changes**.

Setting up outgoing email messages from your network

This topic explains how to set up the SMTP service to deliver email messages to internal and external SMTP servers and how the SMTP service should react if it encounters delivery problems.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Sending SMTP** > **Settings** tab.
3. Select the **Enable** box.
4. Provide the following information:

Option	Description
Enable Logging	Instructs the SMTP service to write a log entry to a log file for each successful delivery of an email message. This log file is named `smtp-yyyymmdd0000`. **Note:** You can access the SMTP log files using the Log File browser at **System** > **Log Files**.
HELO Domain	Defines how the SMTP service identifies itself to other SMTP servers using the HELO/EHLO SMTP command. This is typically the host name of Lotus Protector for Mail Security.
Remove Spool Errors	If enabled, email messages that could not be delivered after the maximum number of delivery attempts (as set in the **Maximum Number of Retries** option) are deleted. If disabled, these email message are moved to the *frozen* queue for the amount of days specified on the Maintenance tab.

Option	Description
Delivery Delay	Specifies the amount of time the SMTP service should wait between the first and the second delivery attempt. Each subsequent attempt is delayed by doubling the delivery delay of the previous attempt (for example, 240 seconds -> 480 seconds -> 960 seconds -> and so on). You can increase the delay between two attempts by changing the **Resend Increment Ratio** option.
Maximum Number of Retries	Sets the maximum number of retries per email message before a Non Delivery Report (NDR) is sent out to the sender of an email message and the email message is moved to the *frozen* queue.
Resend Increment Ratio	Influences the delay between two delivery attempts. You can set the following values: • 0 = Each delivery attempt is delayed by a fixed amount of time as specified in the **Delivery Delay** field. • 1 = Each delivery attempt is delayed by doubling the delay of the previous delivery attempt (default). • >1 (greater than 1) = Each delivery attempt is delayed by the sum of the previous delay attempt and the previous delay attempt divided by *n* (where *n* is the chosen value). The formula for delays in delivery attempts is `T(i) = T(i-1) + T(i-1) / n`, where *T(i)* is the delivery attempt delay of the *i* th attempt and a base case *T(1)* set to the value of **Delivery Delay** option. **Attention:** Changing this value can drastically impact the amount of time an email message sits in the *resend* queue. For example, using the default values for the **Delivery Delay** option (240 seconds) and the **Maximum Number of Retries** (8 retries) option, and then changing the **Resend Increment Ratio** value to 2, can cause an email message to sit about 197 minutes in the *resend* queue instead of 1020 minutes if you had used a value of 1. Make sure you adjust the values for the **Delivery Delay** option and the **Maximum Number of Retries** option appropriately.
Notify Sender on Retries	Defines the number of failed delivery attempts before the sender of an email message is informed about temporary delivery problems.
Number of Cited Lines in Bounces	Specifies the amount of lines of an undeliverable email message that should be included in a Non Delivery Report (NDR) that is sent back to the sender.

Option	Description
Delivery	Choose how the SMTP service should determine the next SMTP server an email message should be relayed to: • DNS Resolution: Determines the destination SMTP server by looking up DNS MX records. The service will use the default DNS servers as configured on the Networking page, unless specific DNS servers are added to the list. • Forward: Relays outgoing email messages to an SMTP server as configured in the list. You can either forward email messages to a specific domain by mapping the domain name to the IP address or host name of an SMTP relay (for example, `example.com` to `relay0.mycompany.com`), to a wildcard character `*` in conjunction with a specific domain (for example, `*.example.com` to `relay1.mycompany.com`) to relay subdomains to a specific relay, or to a wildcard character `*` to relay all outgoing traffic through a certain relay. The **Mailserver(s)** option can contain a list of SMTP servers separated by semicolons (;) for failover. If the list is prefixed by #, the SMTP service will distribute the email messages over all given SMTP servers. **Note:** If the SMTP service cannot find a configured relay for a specific domain, it will automatically fall back to DNS Resolution for this domain.

5. Click **Save Changes**.

Removing undeliverable email messages and SMTP log files from the file system

This topic explains how to set up the number of days you want Lotus Protector for Mail Security to store email messages that are not deliverable or to store SMTP log files in the file system.

Procedure

1. Click **SMTP** > **Configuration** in the navigation pane.
2. Click the **Maintenance** tab.
3. Provide the following information:

Option	Description
Days to Keep Undeliverable Message	Sets the number of days to wait until undeliverable email messages are deleted from the system. **Note:** Lotus Protector for Mail Security only stores undeliverable email messages if the **Remove Spool Errors** check box is not checked (disabled) on the **SMTP** > **Configuration** > **Sending SMTP** tab.
Days to Keep Log Files	Sets the number of days to wait until SMTP log files are deleted from the system.

4. Click **Save Changes**.

Installation of TLS certificates

To encrypt traffic between Lotus Protector for Mail Security and an SMTP server, you must install an SMTP TLS certificate. The certificate can be self-signed, issued by a third-party root authority, or signed by an intermediate certificate authority. Wildcard certificates are supported.

Uploading a server certificate

You can upload certificates for trusted SMTP servers that the SMTP service is communicating with (for example, your internal SMTP servers or SMTP servers in other subsidiaries).

You can also upload certificates for certification authorities that are used to verify the identity of the authority that has signed the certificate that has been sent by another SMTP server (Certificate Chains).

You upload both a private key file and the corresponding certificate that the SMTP service should use. The certificate is sent to the SMTP server that is requesting TLS encryption for delivery. The certificate contains the public key to be used to encrypt the data, while the private key file remains at Lotus Protector for Mail Security to decrypt the data. Typically, the certificate is signed by a trusted third-party in order to verify the identity of Lotus Protector for Mail Security, but you can also use a self-signed certificate.

If you do not have a key file and a certificate, you can follow the instructions at http://www.openssl.org/docs/HOWTO/keys.txt and http://www.openssl.org/docs/HOWTO/certificates.txt to create key/certificate pairs that can be used with the SMTP service of Lotus Protector for Mail Security.

Example: Creating a self-signed certificate

1. Create a private key using this command:

   ```
   $ openssl genrsa 2048 > server.key
   ```

2. After you create the private key, create your own copy of the self-signed certificate using this command:

   ```
   $ openssl req -new -x509 -key server.key -out server.cert
   ```

```
C:> openssl req -new -x509 -key server.key -out server.cert -config openssl.cnf
```

3. The Common Name (CN) that you specify for the OpenSSL binary is the fully qualified host name that answers to the IP address that your XMail server is listening on. If you want a certificate that is signed by an authority, generate a certificate request file using this command:

```
$ openssl req -new -key server.key -out cert.csr
```

```
C:> openssl req -new -key server.key -out cert.csr -config openssl.cnf
```

Uploading SMTP TLS certificates

Before you begin

You must have copies of both the certificate file and its private key file to complete the upload. The certificate must be encoded in Privacy-enhanced Electronic Mail (PEM) format. For more information about determining the file format, see *Verifying the file format of a certificate*.

About this task

You can install a certificate/key pair from the command line or by using the Lotus Protector Manager, also referred to as the Local Management Interface (LMI).

Note: You can upload a single private key and certificate pair at a time only. If you upload an additional pair, the existing pair is overwritten.

Procedure

- Install a certificate by using the Lotus Protector Manager
  1. In the navigation pane, expand **SMTP** and click **TLS Certificates**.
  2. Specify the locations of the certification file and the key file, and then click **Upload Certificate**.
  3. In the navigation pane, expand **SMTP**, click **Configuration**, and then click **Encryption (TLS)**.
  4. Select **Always Try TLS** and click **Save Changes** to enable opportunistic TLS.
- Install a certificate by using the command line
  1. Log in to the console with root privileges over SSH.
  2. Rename the files. The name of the private key file must be `server.key`. The name of the certificate must be `server.cert`.
  3. Use the **`sftp put`** command to upload the private key and certificate files to the following directory: `/etc/xmail/`
  4. From this same directory, use a text editor to open the file `server.tab` and set the value of **`EnableSMTP-TLS`** to *1*.
  5. Enable the change by restarting the XMail server. From the console, type `service xmail restart`.

What to do next

The SMTP connection is now secured by TLS. To verify the connection, as described in *Testing the TLS connection*.

Adding a certificate from an intermediate CA

You can use a certificate that is signed by an intermediate CA to secure the connection to the SMTP server. You must append the certificate of the intermediate CA to the existing server certificate.

Before you begin

An SMTP TLS certificate signed by a root authority must be installed before you can add a certificate from an intermediate CA.

About this task

If you do not have a copy of the intermediate certificate, you must retrieve details about its signer and download a local copy. If the certificate file is not in PEM format, you must convert it. For more information, see *Verifying the file format of a certificate*.

Procedure

1. Log in to the console with root privileges over SSH and from the `/etc/xmail/` directory, run following command: `openssl x509 -in server.cert -text -noout`

   The command returns detailed information about the certificate, including the URI from which you can download the certificate, for example:

   ```
   Authority Information Access
        CA Issuers - URI:https://ssl.trustedCA.com/ssl.crt
   ```

2. Use a browser to navigate to the address of the CA and download the certificate to a temporary directory.
3. Append the certificate to the existing server certificate.
   a. In a text editor, open both the existing server certificate and the certificate you downloaded from the intermediate CA.
   b. From the downloaded certificate, copy the portion of the file that begins with the line that reads `-----BEGIN CERTIFICATE-----` through the line `-----END CERTIFICATE-----`
   c. In the existing server certificate, find the line that reads `-----END CERTIFICATE-----`, and paste the information that you copied from the downloaded certificate immediately after that line.

Verifying the file format of a certificate

Certificate files must be in Privacy-enhanced Electronic Mail (PEM) format. You can run a command to check the file format and convert files to PEM format if necessary.

About this task

If the certificate file is in binary Distinguished Encoding Rules (DER) format, you can run a command to convert it to PEM format.

Procedure

1. To check the file format, from the command line, type :`openssl x509 -in` *`CERTIFICATE_NAME.crt`* `-text -noout`

   where *CERTIFICATE_NAME.crt* is the name of the CA file.

   If the file is in DER, rather than PEM format, the screen displays an error similar to the following one:

   ```
   Unable to load certificate
   13233:error:0906D06C:PEM routines:PEM_read_bio:no start
   line:pem_lib.c:644:Expecting: TRUSTED CERTIFICATE
   ```

2. To convert a file from DER format to PEM format, type the following command on a single line: `openssl x509 -inform der -in` *`CERTIFICATE_NAME.crt`* `-out` *`CERTIFICATE_NAME.cert`*

   where *CERTIFICATE_NAME.crt* is the name of the CA file in DER format.

Testing the TLS connection

After you install a certificate, test the connection to verify that it is secure.

About this task

You can test that the TLS setup is working correctly by using the following procedure.

Procedure

1. Log in to the console with root privileges over SSH.
2. Type the following command on a single line: `openssl s_client -starttls smtp -crlf -connect 127.0.0.1:25 -CAfile /etc/apache2/ssl.crt/ca-bundle.crt`

   If the connection is set up correctly, the command returns the following output: `Verify return code: 0 (ok)`

SMTP queues

The SMTP queues contain email messages that are waiting to be processed by Lotus Protector for Mail Security.

Unchecked queue

The *unchecked* queue contains email messages that are waiting to be analyzed by Lotus Protector for Mail Security.

Every incoming email message enters the *unchecked* queue first. The *unchecked/processing* status indicates email messages are being processed by Lotus Protector for Mail Security. After the email message has been analyzed by the policy in place, the email message is removed from the *unchecked* queue.

The email messages in the *unchecked* queue are considered temporary data; a large *unchecked* queue indicates that Lotus Protector for Mail Security is receiving more email messages than it can process.

The following messages might appear if there is bad mail or other issues (these messages are purely informational and do not require user intervention):

unchecked/processable
unchecked/processable.cal
unchecked/processable.smtp
unchecked/processable.timeout
unchecked/processable.processing
unchecked/processable.processing.db
unchecked/processable.processing.pgdb
unchecked/processable.processing.unk

Local queue

The *local* queue contains email messages that were in the *unchecked* queue, but have been analyzed and then moved from the *unchecked* queue to the *local* queue.

These email messages are also considered temporary data.

Sending queue

The *sending* queue contains new email messages in the mail queue that the SMTP service is trying to deliver.

Resend queue

The *resend* queue contains email messages that were sent to the target SMTP server but failed to be processed because of a temporary error. Temporary errors can include issues with:

- The SMTP server not being reachable.
- The receiving mail server (remote server) returning a permanent error.
- Lotus Protector for Mail Security not being able to send an email message within the configured resend interval.

A large *resend* queue indicates that there is an email delivery problem.

Frozen queue

The *frozen* queue contains email messages that were sent to the target SMTP server but failed to be processed because of a temporary error. Temporary errors can include issues with:

- The SMTP server not being reachable.
- The receiving mail server (remote server) returning a permanent error.
- Lotus Protector for Mail Security not being able to send an email message within the configured resend interval.

The email message is moved to the *resend* queue to be resent by Lotus Protector for Mail Security. A large *resend* queue indicates that there is an email delivery problem.

Optional: Use the Respool option if you have experienced a slowdown in email message processing that has caused a backlog in one of the spool directories.

Monitoring mail traffic flow in the delivery queues

The Queue Browser page (**SMTP** > **Queue Browser**) shows the delivery queues used by the SMTP service. Email messages are either waiting to be analyzed (*unchecked*), waiting for transmission (*local*, *send*, *resend*), or have experienced an error condition (*unprocessable*, *frozen*).

Counting email messages in a queue

Click on the **[Count]** link next to a queue to view the number of email messages waiting to be processed for that queue. Click on the number to refresh the message count for the queue without having to refresh data for the entire page.

Respooling email messages

If the SMTP service experiences problems during the delivery of an email message, the message is moved to the *resend* queue if a single delivery attempt fails, or moved to the *frozen* queue if delivery attempts fail altogether.

Delivery problems can occur if Lotus Protector for Mail Security has not been set up correctly or an external network component, such as a switch between Lotus Protector for Mail Security and the destination SMTP server, or the destination SMTP server itself is not available.

After you have resolved the issue, you can try another delivery attempt by respooling either all or specific email messages from a queue.

Exploring the queues

Click on the name of a queue to view a list of email messages residing in the queue, including the size of each email message and the date it was created. Each page contains a maximum of 1000 entries from the queue.

Use the **Show more** link to view additional files in the queue. For example, you can view a log file for email messages listed in the *resend* and *frozen* queue. This log file contains information about all the delivery attempts made by the SMTP service, and can provide you with valuable information for remedying delivery problems.

Viewing email messages

Click on the path of an item in the queue to view the contents of an email message.

An email message contains additional transport information at the start of its displayed data as it sits in one of the queues for the SMTP service. Depending on which queue you are viewing, this data can be separated by a single blank line or a line containing <<*MAIL-DATA*>> from the original email message.

This site only displays email messages as plain text; the parts of an email message written in HTML are not processed.

Note: Displayed data is truncated to 4096 bytes.

Solving delivery problems

If you have issues with a queue, try the following suggestions:

- Access log files for the email message, using the Log File Browser (**System** > **Log Files**), to determine why the email message was not delivered
- Immediately respool marked email messages in both the *resend* queue and in the *frozen* queue to the SMTP queue from the SMTP Queue Browser
- Delete email messages from the *frozen* queue using a cleanup job you can set from the Maintenance tab on the SMTP Configuration page (**SMTP** > **Configuration** > **Maintenance**)

Chapter 3. Policy configuration

This chapter describes how to configure a mail security policy that contains a set of rules defining how Lotus Protector for Mail Security should inspect and filter both incoming and outgoing mail traffic.

About policy rules

A policy rule defines how Lotus Protector for Mail Security should inspect and filter email messages that are relayed through the policy system.

Components of a policy rule

Each policy rule consists of various objects (Condition Objects, Who Objects, When Objects) and analysis modules that define how Lotus Protector for Mail Security should analyze an email message. A rule also consists of Response Objects that instruct the policy system on how it should handle an email message, including an Action that instructs the policy system on how to proceed with the message, when the rule becomes a matching rule.

Table 17. Components of a policy rule

Option	Description
Rule Name	Specifies the name of the policy rule.
Comment	Provides a meaningful description about the policy rule.
Pre Conditions	Specifies a list of Condition Objects that define the prerequisites for this policy rule to be evaluated.
Senders	Specifies the originator of an email message as specified by the `MAIL FROM` command during transmission.
Recipients	Specifies the recipient of an email message as specified by the `RCPT TO` command during transmission.
Whens	Specifies the When Objects that define the time periods when the policy rule is valid.
Analysis Modules	Provides a list of analysis modules that can inspect an email message to determine the category of its contents.
Responses	Provides a list of Response Objects (configured on the Policy Objects page) that define how the policy system should modify an email message that has matched the rule or where to store it.
Action	Defines how the policy system should continue processing an email message that has matched the rule. The following actions are available: • Allow: Allows delivery of the email message to its recipient. This ends the processing of the email message by the policy system. • Block: Blocked email messages are not delivered to their recipients. This ends the processing of the email message by the policy system. • Continue: The policy system continues processing the current email message by evaluating the next rule in the chain.

How the policy system uses rules

The policy system consists of a chain of rules. Each rule is evaluated from top to bottom, and from left to right. If a rule contains multiple objects of the same type, the result for a component of a rule (such as Recipient, Analysis Module) is considered *true* if at least one of the given objects has been evaluated successfully (logical OR).

The result of the evaluation of an object (except for a Response Object), however, can always be negated by choosing the **Toggle Not** option from the pop-up menu of an object. This causes the policy system to reverse the result of the evaluation of an object (considering the negated object is a match, if the object does not match).

The policy system processes the policy within the context of a single recipient. If an email message that is being analyzed has multiple recipients, the policy system evaluates the rules separately for each recipient of the email message.

When policy rules match

Lotus Protector for Mail Security keeps a copy of the original message, as it was received by the SMTP service, in memory while processing the active rules step-by-step. This copy is called the *current message* in the policy system, because it contains all the changes that were made to the message from prior rules. If the Action is set to *Allow*, Lotus Protector for Mail Security delivers the current message to a particular recipient. However, if the Action is set to *Block*, it drops the email message (if it was not previously stored in an email queue).

Lotus Protector for Mail Security follows these steps for every active policy rule from the first rule to the last rule (top to bottom) until a rule matches and the specified Action is either *Block* or *Allow*, or the end of the rule chain is reached (in which the default action is *Allow*).

Who Objects

Who Objects represent a single user or a group of users within the policy system. Who Objects can be defined by an SMTP address (`joe@mycompany.com`), SMTP address patterns (`*@mycompany.com`), or by a user or a group from a directory service as defined in a selected Directory Object.

Types of Who Objects

Table 18. Types of Who Objects

Type	Description
Email	Represents users or groups by their SMTP address. The defined pattern can contain the wildcard character `*` used to represent a sequence of arbitrary characters of any length. You can also populate the list of SMTP addresses using macros, such as `$(LOCAL_DOMAINS)`. **Example:** `*@.mycompany.com`
Directory	Represents any user known by the directory service in the Directory Object used by the Who Object.
Group	Represents a specific Directory Object type; it will only match if the user who uses a certain SMTP address is a member of the specified group in the directory used by the selected Directory Object. The name of the group in the Who Object is equal to its name in the directory.
User	Represents a single user by their name in a directory. This user's SMTP address is resolved by using the Name attribute configured for the Directory Object in use.
Compound Who	Combines different types of Who Objects (as mentioned above) into a single object. A Compound Who Object matches if one of the Who Objects contained in the Compound Who Object matches.

Who Object for Recipient Verification

Who Objects are not only used for rules in the policy, but are also used to verify the existence of a user within your environment during the delivery of an email message. The Recipient Verification mechanism, which is integrated into the SMTP service that rejects email messages to unknown recipients at the SMTP layer, also uses the same Who Objects that you use in policy rules.

Verifying Who Objects

You can use the Verify Who Objects page (**Mail Security** > **Verify Who Objects**) to check whether you have configured Who Objects (especially Directory-based Who Objects) correctly.

This page provides two different methods for verifying your Who Objects. Use the All Who Objects method if you want to verify that all your Who Objects (and underlying Directory Objects) are set up correctly. If you want to verify that a specific email address matches one ore more Who Objects, choose an SMTP Address from the list.

Table 19. Verifying Who Objects

Option	Description
Who	Specifies the name of the Who Object as configured on the Mail Security Policy Objects page.
Type	Specifies the type of Who Object: • Email Pattern: Represents users or groups by their SMTP address. • Directory: Represents any user known by the directory service in the Directory Object used by the Who Object. • Group: Represents a specific Directory Object type; it will only match if the user who uses a certain SMTP address is a member of the specified group in the directory used by the selected Directory Object. The name of the group in the Who Object is equal to its name in the directory. • User: Represents a single user by their name in a directory. This user's SMTP address is resolved using the Name attribute configured for the Directory Object in use. • Compound Who: Combines different types of Who Objects (as mentioned above) into a single object. A Compound Who Object matches if one of the Who Objects contained in the Compound Who Object matches.
Description	Provides an informal description of what the Who Object represents.
SMTP Match SMTP Address only	Indicates whether the given email address matches for the given Who Object.
Result	Indicates whether Lotus Protector for Mail Security was able to retrieve information from the given Who Object or the underlying Directory Object. If the specific Who Object uses a Directory Object, you can obtain detailed information about the retrieved data or find out why the lookup failed by clicking on the value in this column.

When Objects

When Objects define certain time frames, such as office hours. You use these objects within the policy system to define when a rule containing a When Object is valid.

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **When** tab, and then click **Add**.
3. Enable the **Active** box.
4. Type a name for the When object.
5. Click **Add** in the **Time range** area.
6. Set the following values:

Option	Description
Time	Specifies the starting time for the time frame defined by the When Object. **Note:** The date that is automatically entered for a new When Object uses the time of the system Lotus Protector Manager is running on, not the current system time of Lotus Protector for Mail Security. Additionally, the starting time might also use the time zone of your web browser or Greenwich Mean Time (GMT).
Duration	Specifies the size of the time frame defined by this When Object.
Repeats Every	Sets the amount of time between each repetition counted from the starting time.

Example: Set up a When Object to balance the amount of incoming email messages between two people using 5 minute time periods:

Start: 2009-06-15 00:00:00 GMT, Duration 5 minutes, repeats every 10 minutes

where the starting **Time** value for the new When Object is June 15, 2009 00:00:00 GMT, with a **Duration** value set at 5 minutes, and a **Repeats Every** value set at 10 minutes

7. Click **OK**, and then click **Save Changes**.

Condition Objects

Condition Objects are prerequisites that state under what circumstances a policy rule applies to an incoming email message. These conditions are evaluated and modified separately for each email message that is processed by Lotus Protector for Mail Security.

A condition stores the results of a policy rule (whether the policy rule matched or did not match) that you can then use as criteria for other policy rules. The initial value of a condition is always *false*.

You can optimize your set of policy rules by using conditions. You can set up a condition that avoids evaluating specific policy rules if an email message did not meet criteria defined in a previous policy rule or you can set up a condition that only evaluates the policy rule if an email message does not meet the defined criteria. You should use conditions if you have multiple policy rules that use a common set of criteria.

Table 20. Condition Objects

Option	Description
Name	Specifies the name of a Condition Object that is used in the policy system.
Comment	Provides a description about the Condition Object.

Using Condition Objects (example)

If you want to manage email traffic for a specific recipient (or group of recipients) by tracking an email message that contains a particular keyword in the subject, you can define a rule in the policy system that contains a Who Object representing the recipient(s) and an Analysis Module that tests if the subject contains the keyword. You must define a response to these types of email messages using a Response Object that sets the value of the condition to *true*.

In the subsequent rule, you can test if an email message meets the defined criteria by adding the Condition Object to the list of Pre Conditions. For example, the recipient(s) is not allowed to receive email messages containing executable files and all spam email messages should be stored in a specific message store for this recipient(s). You must create a rule that tests the value of the Condition Object, add a new Analysis Module Media Type (Type: application), and set its Action to *Block*. Additionally, you set up another rule that is also testing the value of the Condition Object and uses a set of spam detection Analysis Modules with an appropriate response that will store email messages in a specific message store.

Analysis Modules

Lotus Protector for Mail Security uses various spam analysis modules to inspect the content of an email message.

Attachment Check

This module analyzes the number of attachments, the size of single attachments, or the size of all attachments. You can use this feature, for example, if you have bandwidth problems and want to delay the delivery of email messages with big attachments.

Compound

This module is made up of a combination of analysis modules. You can assign different scores to the different modules and define a threshold.

Keyword Search

This module provides a regular expression search engine. This module allows you to generate your own categories that perform compliance checks.

Language Check

This module is used by Lotus Protector for Mail Security when you are training it to analyze email messages from countries other than the United States. Lotus Protector for Mail Security currently supports more than 40 different languages. It is possible to block or redirect email messages because they are written in a language the employee is not able to read.

Media Type

This module is able to detect more than 120 different file types. You can use this, for example, to extract dangerous file types such as executable programs.

Message Field Check

This module allows you to scan for expressions within the message fields of the email message using regular expressions. You can use this feature, for example, to check for a word in the subject or to identify HTML email messages (check for the content type header field).

Phishing Check

Phishing email messages are a type of spam intended to retrieve personal information from potential victims. Typically, phishing email messages look as if they are coming from an individual's bank or favorite shopping sites, but the intention is to steal that person's account information, including passwords. In many cases, it is very difficult for the average user to distinguish a real email message that was sent by their bank from a phishing email message.

For phishing detection, IBM combines a variety of methods. The URL checker is able to detect links to banking and other commercial sites in all spam coming from the spam collectors. Phishing email messages also show typical heuristics compared to regular spam, and are categorized separately from regular spam in the filter database.

Sender Policy Framework

Important: If you set the Received Header Type to **Strict (no IP shown)** when you open ports on the firewall to receive SMTP traffic, the analysis modules in the Sender Policy Framework will not work because these modules rely on information in the received header.

The Sender Policy Framework module evaluates an SPF record and produces one of the following results:

Table 21. Sender Policy Framework module results

Result	Description
None	The domain does not publish SPF data.
Neutral	The SPF client must proceed as if a domain did not publish SPF data. This result is given when the SPF record specifies the '?all' command.
Pass	The email message meets the definition of legitimacy for the publishing domain. MTAs proceed to apply local policy and can accept or reject the email message accordingly.
Fail	The email message does not meet a definition of legitimacy for a domain. MTAs might reject the email message using a permanent failure reply code, such as Code 550.
Softfail	The email message does not meet a strict definition of legitimacy for a domain, but the domain cannot confidently state that the email message is a forgery. MTAs should accept the email message but might subject it to a higher transaction cost, deeper scrutiny, or an unfavorable score. There are two error conditions, one temporary and one permanent.
Error	Indicates an error during lookup; an MTA should reject the email message using a transient failure code, such as 450.
Unknown	Indicates incomplete processing: an MTA must proceed as if a domain did not publish SPF data. When SPF-aware SMTP receivers accept an email message, they should add a prefix to a Received-SPF header. SPF clients must use the algorithm described in this section or its functional equivalent. If an SPF client encounters a syntax error in an SPF record, it must stop processing and return a result of unknown.

Spam Bayesian Classifier

The Bayesian classifier is a system that determines whether an email message is spam based on email statistics.

To train the classifier, thousands of examples of spam and regular email messages are presented to the system and relevant data is extracted and stored in a statistical model. Through this training, the classifier is able to learn the difference between spam and regular email messages.

IBM provides an updated, pre-trained Bayesian database that is trained using thousands of different spam types coming from the spam collectors and through user feedback. You can fine tune the filter or train a completely new one by providing additional spam and ham samples to the filter.

The advantage of the Bayesian classifier is the ability to recognize new types of spam, whereas the signature technology is better in detecting identical and nearly identical spam.

Spam DNSBL Check

This module uses DNSBL (Domain Name Server Block Lists) servers to determine if email messages have originated from possible spam sources. You can define multiple servers with relevant scores to generate more precise detection, which provides higher flexibility.

Spam Fingerprint

Every email message computes a unique 128-bit signature. You can use the signatures in the filter database to identify existing spams.

Lotus Protector for Mail Security computes spam signatures for all known spams (from spam collectors and other sources) and stores the signatures in the filter database.

Spam Flow Check

This module analyzes mail flow within a specific time frame. If the same email message (based on a number of similarity measures) is received more than a threshold number of times within the time frame and has different sender domains, then the email message is a classified as spam. This technology can detect completely unknown types of spam based on the way spam is typically created and sent.

Spam Heuristics

This module employs an internal scoring system with each heuristic receiving either positive or negative points, depending on whether the heuristic is designed to match spam or ham (normal email message). If the point count reaches a predetermined threshold, the email message is classified as spam.

For example, the following information is used for heuristic analysis:

- Message-ID field characteristics
- Received field not valid or missing
- Checks for "Apparently-To:" or "X-Apparently-To" fields
- Checks for mailing list fields
- Checks for multiple recipients and alphabetic recipient patterns, such as a@, b@, c@
- Checks for missing fields such as "From" and "To"

Spam Keyword

This module covers standard keywords and patterns (regular expressions) that are typically found in spam email messages.

IBM has extracted relevant keywords and patterns from known spam and weighted individual relevancy for additional spam protection.

Spam Signature Database

This module allows Lotus Protector for Mail Security to break down every email message into several logical parts (sentences, paragraphs), and computes a unique 128-bit signature for each part. These signatures are subject to minor modifications in the email message, but are still accurate enough to uniquely identify a known spam with a couple of matching signatures in the filter database.

Spam Structure Check

This module examines the HTML structure of the email message and computes two signatures based on the structure.

For example, some spam typically has a bold headline followed by one or more paragraphs in a different color, and then some random text at the bottom. Such layout structures are close to the actual text in the email message and are therefore an excellent addition to the textual spam signatures mentioned earlier in this section.

The module computes structure signatures are for all known spam (coming from spam collectors and other sources) and stores the spam signatures and URLs in the filter database.

Spam URL Check

This module compares data with URL entries found from the Internet. All relevant URLs that appear in spam email messages are stored in the filter database together with the stored spam signatures. A single Spam URL is enough to identify a spam email message.

URL Check

This module analyzes URLs in email messages using content from the filter database. Lotus Protector for Mail Security provides more than 61 categories that allow you to block email messages with unwanted or dangerous links.

User Sender Allow List

Each user is able to maintain their own Sender allow list. You can specify in detail which user is allowed to use this feature and in which position of the rule chain this check is performed.

User Sender Block List

Each user is able to maintain their own Sender block list. You can specify in detail which user is allowed to use this feature and in which position of the rule chain this check is performed.

Virus Check

This module provides two modules that use antivirus software to detect viruses and handle infected email messages:

- Signature Pattern Detection
- Remote Malware Detection

You can choose between a pattern-based scanner such as Sophos (if you have installed a valid license) or the Remote Malware Detection scanner.

Using spam analysis modules

This topic explains how you can enable the spam analysis modules that the appliance uses to inspect the content of an email message.

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **Analysis Modules** tab, and then click **Add**.
3. Select the **Enabled** box to enable the rule.
4. Type a name and a comment for the rule.
5. Select a spam analysis module. See "Analysis Modules" on page 50 for detailed descriptions of each module.
6. Click **OK**, and then click **Save Changes**.

Response Objects

Response Objects define how an email message should be handled after it has been analyzed by Lotus Protector for Mail Security.

Table 22. Types of Response Objects

Option	Description
Add Attachment	Provides a response that modifies the content or nature of an original using an added attachment that contains the current email message, the original email message, or a file.
Add Disclaimer	Provides a response that modifies the content or nature of an original email message by adding a standard company disclaimer for every outgoing email message.
BCC	Sends a copy of the email message as BCC to the given recipient. You can modify the email message sent as the BCC with other Action Objects. The BCC action applies to all email messages, allowed or blocked. • $(SENDER): The sender address used for the original email message. • $(RECIPIENTS): A list of all the recipients of the original email message. • $(ALLOWEDRCPTS): A list of all the recipients that were allowed. • $(BLOCKEDRCPTS): A list of all the recipients that were blocked. • $(NEWMSGSENDER): The sender address used for newly created email messages. • $(POSTMASTER): Sends the detected email message to the original sender as `postmaster@mycompany.com` and informs the sender that the original email message has been quarantined.
Log	Writes to a plain text file (with replaced macros), but does not write to the Lotus Protector for Mail Security database.
Modify Field	Modifies or adds a field to the email message header. **Important:** Be careful when you modify the message field. Do not modify fields that might eventually corrupt or damage your email message, causing it to be discarded instead of reaching its recipient.
Redirect	Sends the email message to the given recipient. • $(SENDER): The sender address used for the original email message. • $(RECIPIENTS): A list of all the recipients of the original email message. • $(ALLOWEDRCPTS): A list of all the recipients that were allowed. • $(BLOCKEDRCPTS): A list of all the recipients that were blocked. • $(NEWMSGSENDER): The sender address used for newly created email messages. • $(POSTMASTER): Sends the detected email message to the original sender as `postmaster@mycompany.com` and informs the sender that the original email message has been quarantined.

Table 22. Types of Response Objects (continued)

Option	Description
Relay Message	Relays a specific email message to a specific host.
Remove Attachment	Analyzes attachments found in email messages. If the attachment matches the defined Who/When/What condition, Lotus Protector for Mail Security will remove the attachment (or all attachments) from the original email message. **Note:** If you use this action to remove an uu-encoded text block and select the Matching attachments option, other uu-encoded parts of the email message are recorded as attachments in the resulting email message.
Require Encryption	Allows an Administrator to configure a response in which an email message that matches a specific rule must be delivered using Transport Layer Security (TLS). • If you want to send email messages to a specific domain using encryption, then create a policy rule from `My domains` to `this.specific.domain` with a Require Encryption response. • If you want to send email messages that require that all email messages using a Company Confidential disclaimer should be sent using encryption, then create a policy rule from `My domains` if the email message contains 'Company Confidential' with a Require Encryption response **Note:** If an email message is flagged for TLS delivery, but the SMTP counterpart does not support TLS, the system will try to resend the email message as configured for "normal" SMTP traffic by sending Non Delivery Reports (NDR) to the sender. However, if the email message cannot be delivered by TLS, the system will not deliver the email message.
Send To	Request the application to reply to the sender of the analyzed email message or to somebody else (such as the Administrator) with different options for manipulating the content of an email message. You can perform the following actions with this Object: • Create a new email message to the sender • Add an attachment • Attach the original email message as an attachment • Send a predefined warning email message to the original sender
Set/Clear Condition	Sets the state of a condition (or switch) used to dynamically enable or disable specific rules in the policy.
Store	Sends the email message to a storage folder. You can also choose whether to save the original or the current email message (an email message that has been modified by another policy rule).

Directory Objects

This topic provides information about integrating Lotus Protector for Mail Security with a Directory Object, such as an LDAP (Lightweight Directory Access Protocol) directory service, where you can obtain your directory service user database and use it with Who Objects and policy rules.

About LDAP directory servers

An LDAP server is a directory service, such as Active Directory, IBM Lotus Domino® Directory, OpenLDAP, Novell eDirectory, Oracle Internet Directory, Sun ONE, that stores information about people, organizations, and other resources and that is accessed using the LDAP protocol. The entries in the directory are organized into a hierarchical structure, and in some cases the hierarchical structure reflects the structure or geography of an organization.

LDAP directory servers provide user and user/group information to Lotus Protector for Mail Security. You can simplify Who Object configuration by mapping user names and groups provided by the LDAP server to the Who Object(s) you are defining for a policy.

Tip: If you are not sure about the structure of your directory service, you can use a directory service browser (for example, LDAP Browser/Editor by Jarek Gawor) to browse or edit your directory.

Directory Object settings

Specify the settings for the connection to a directory service that define the Directory Object:

Option	Description
Name	The name of the Directory Object that represents the directory service in the policy system.
Comment	An optional comment for the directory service.
Cache Expiration	The length of time Lotus Protector for Mail Security caches user and group information locally. Lotus Protector for Mail Security does not query the directory service if information found in its directory cache increases its performance. However, because cached data might not include the latest changes for the directory, make sure you set an appropriate expiration value. **Default:** Use the default value of 1440 minutes (1 day) as a trade-off between performance and actuality.

LDAP Server settings

Option	Description
Host	The host name or the IP address of the directory service provider.
Port	The port on which the directory service is listening for incoming connections. **Default:** Port 389 for unencrypted requests; port 636 for SSL requests
User name	The user name of a directory user who is allowed to enumerate the directory service. **Note:** The format for this account name depends on which directory service you are using. For example, an Active Directory uses `mycorp\administrator`. Other software might use user names such as `cn=Directory Manager,o=mycorp`.
Password	The password for the user entered in the User name field above.
OU (Directory Entry Point)	The directory entry point (BaseDN) for the directory search. Format: `DC=domain,DC=com`

Option	Description
Mode	• Base: Uses the entry configured at the OU (Directory Entry Point). • One Level: Only uses the entries located directly within the BaseDN configured at the OU (Directory Entry Point). • Sub Tree: Uses the BaseDN configured at the OU (Directory Entry Point) and all entries located somewhere below this entry in the Directory Information Tree.
Use ObjectClass or ObjectCategory	• ObjectClass: Uses the ObjectClass attributes to determine the type of directory entry. • ObjectCategory: Uses specific directory entries within an Active Directory. This attribute is used in determining the type of entry just as the ObjectClass attribute, but with the following differences: – There is only one attribute named ObjectCategory per directory entry. – This attribute is typically indexed in the underlying database of the server. **Tip:** Use ObjectCategory instead of ObjectClass to improve performance on large domains or on slow servers if you are using an Active Directory.

Users settings

Option	Description
Object Class	Defines the value of the ObjectClass attribute that is identifying a directory entry as a user. In most cases, set this to entry to *person*.
Name Attribute	Specifies the name of the attribute of a directory user that contains the user's login or short name. **Note:** Depending on the way you set up Who Objects for policy rules and for authentication with the End User Interface, you can use either the login name or the actual name of the user.

Groups settings

Option	Description
Object Class	Defines the value of the ObjectClass attribute that is identifying a directory entry as a group. This value can vary depending on what type of group you choose and the structure of your directory service. Common values are group, organization, or country.
Name Attribute	Specifies the name of the attribute of a directory group that contains the name of the group.

Membership settings

Option	Description
Membership defined in	Select the method used for detecting all groups that a particular user or group belongs to: • Member Object: The Object itself, either a user or a group, containing a list of membership attributes that defines the groups it belongs to. • Group Object: A list of member attributes that list all the Objects, either users or groups, belonging to the group.
Membership Attribute	Depending on what option you selected in the **Membership defined in** setting, this can be either the name of the attribute in a Member Object defining the groups the Object belongs to (for example, *memberof*), or the name of the attribute in a Group Object used to list all Objects belonging to a group (for example, *member*).

SMTP Addresses settings

Option	Description
SMTP Attributes	The name of the attribute of a directory user or group containing the email address of the entry. If your directory uses multiple attribute names to store email addresses, you can enter a list of attribute names separated by semicolons (;). **Example:** `address1@mycompany.com;address2@mycompany.com` **Note:** Lotus Protector for Mail Security uses the "mail" and the "uid" attributes.

SMTP Domains settings

Lotus Protector for Mail Security uses a list of SMTP domains for each Directory Object during message processing and for user login/authentication in order to determine whether a certain directory contains information about a specific domain. The SMTP Domains list acts a filter for directory lookups.

Option	Description
SMTP Domains list is empty	Lotus Protector for Mail Security tries to obtain information from this directory for all domain parts found in email addresses.
SMTP Domains list is not empty	Lotus Protector for Mail Security searches the list for the domain part of an email address. • If the domain part is in the list, Lotus Protector for Mail Security tries to obtain information about the user or group from this directory. • If the domain part is not in the list, this particular directory will not be queried for information about the user or group.

Schedule Objects

Schedule Objects are used to trigger certain tasks for Lotus Protector for Mail Security at a given point in time, such as backing up log files and generating quarantine reports.

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **Schedules** tab, and then click **Add**.
3. Provide the following information:

Option	Description
Name	Indicates the name of the Schedule Object.
Time	Specifies when tasks configured to use this Schedule Object should be run. **Note:** The date that is automatically entered for a new Schedule Object uses the time of the system that Lotus Protector Manager is running on, not the current system time of Lotus Protector for Mail Security. Additionally, the starting time might also use the time zone of your web browser or Greenwich Mean Time (GMT).
Repeats Every	Sets the amount of time between each repetition of tasks triggered by this Schedule Object.

4. Click **OK**.

   Note: When you schedule a task, you use an absolute value to specify when it will run (for example, you schedule a task to run on 2011-10-10 at 10:10). Changing the time of the Lotus Protector for Mail Security system can affect when a scheduled task runs. See the Time setting for more information about this issue.

FTP Servers

FTP servers store log files that you must back up.

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **FTP Servers** tab, and then click **Add**.
3. Specify a name for the file, and then click **Create**.
4. Provide the following information:

Option	Description
Name	Specifies the name of the FTP Server Object as it should be displayed in Lotus Protector Manager.
Host	Specifies the host name or IP address of the FTP server where you want to back up log files.
Port	Specifies the port on which the FTP servers are accepting connections from FTP clients.
Root Directory	Specifies the base directory for this FTP Server Object. The FTP client, as configured by this object, changes to the specified directory after you log in. You can configure multiple FTP Server Objects using the same FTP Server with different base directories. If you leave this field blank, the object uses the root directory of the FTP server.
User	Specifies the name of the user who is allowed to log in to the FTP server.
Password	Specifies the password for the user defined in the User field.

5. Confirm the password.
6. Click **OK**, and then click **Save Changes**.

Message storages

Message storages store email messages that you want to archive or quarantine.

About this task

Lotus Protector for Mail Security provides two types of message storages that you can use to store email messages:

Table 23. Types of message storages

Store	Storage Type
Message store	Stores blocked or delayed email messages, including email messages that are considered bad or problematic. You can create as many different message stores as needed.
Quarantine store	Stores email messages that meet certain criteria defined by an Administrator, such as email messages that are infected by viruses or contain confidential data.

Attention: If you change an existing storage type from message to quarantine or vice versa, Lotus Protector for Mail Security deletes the existing storage type and creates a new storage type, which can result in data loss and false message counts. You might see the storage type that you deleted listed in the Email Browser until it is removed from the system.

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **Email Storages** tab.
3. Choose an option:

If you want to...	Then...
Create a message storage	1. Click **Add**. 2. Select the type of message repository from the **Store Type** list. 3. Type a name for the message repository. 4. Click the **General** tab. 5. Set the number of days to store the email messages in the message repository. 6. Choose when and how the email messages will be delivered to their intended recipient. 7. Select a schedule to define when the appliance will deliver quarantine reports to the intended recipient. 8. Click the **MetaData** tab. 9. Use macros that represent parts of the email message that you want sent to the recipient of the quarantine report.
Schedule the number of days to keep email messages in the message storages	1. Select the **Enable** box in the **Message Log Cleanup** area. 2. Set the number of days to keep email messages. **Tip:** Seven days is the recommended amount of time to keep the logs at a manageable size in the database.

Searching for messages in a message storage

This topic explains how to use the Email Browser page (**Mail Security** > **Email Browser**) in order to search for blocked, delayed, or quarantined email messages that are being stored in a message storage.

Specify whether to search for emails messages in a folder, to search for a specific email message in a message storage, or to run queries on email messages in the message storages.

Folders

Option	Description
Trigger Quarantine Report	Generates a daily quarantine report of quarantined email messages.
Delete	Removes an email message from the message storage.
Send to spam@kassel.ibm.com	Send the email message to the recipient email address for spam mail.
Send to notspam@kassel.ibm.com	Sends the email message to the recipient email address for mail that is not spam.
Deliver	Allows you to mark the quarantined email messages you want to work with and then delivers the blocked email message to your personal email address.
Copy	Copies an email message from one message storage to another message storage.
Move	Moves an email message from one message storage to another message storage.

Mails

Option	Description
Message ID	Specifies the message identifier. You can also search for email messages that are not stored by Message ID if you have activated message tracking in the mail security policy (**Mail Security** > **Policy** > **Message Tracking/Reporting**).
Sender	Specifies the sender of the email message.
Recipient	Specifies the recipient of the email message.
Subject	Specifies the subject of the email message.
Metadata	Shows information about the sender, recipient(s), creation date, and attachments. **Note:** The types of metadata are dependent on how you have configured the MetaData field for the individual message store or quarantine store.
Size	Specifies the size of the email message.
Folder	Shows the location of the email message in the message storage.
In time range	Sets the range of time in which to search for the email message. Use the `yyyy-mm-dd hh:mm:ss` format: 2011-12-31 12:45:10.

Note: If you copy or move email messages from one message storage to another message storage, you will not be able to view metadata for the email messages in the message storage that you copied or moved the messages to.

Disabling a quarantine report

This topic explains how to disable a quarantine report for a given user. Quarantine reports are enabled by default to send an email to users informing them that their email has been quarantined for various reasons.

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **Email Storages** tab.
3. Select the Quarantine Store and double-click on the **Edit** icon.
4. From the **General** tab, clear the **Enable** check box.
5. Click **OK** and then save your changes.

Quarantine Reports Template

This topic provides information about the templates you can use as a basis for the quarantine report.

Email template

The Email template must contain at least the `$(DAILYLIST)` macro, which is replaced with a list of blocked email messages. The Line template text file defines each line of that list.

In the Email template, you can only use a few macros that are not specific to a current email message, for example, `$(RECIPIENTNAME)`. If Lotus Protector for Mail Security contains information about the domain or LDAP user name, it will be replaced with the respective user name. Otherwise, Lotus Protector for Mail Security displays the email address of the user.

Important: Do not use special characters such as umlauts when defining folder names.

You can use the following macros for the Email template:

Option	Description
$(TAB)	The tabulator macro or \t.
$(CR)	The new line macro or \n.
$(DATE)	The current date.
$(DATE.DAY)	The current day.
$(DATE.MONTH)	The current month.
$(DATE.YEAR)	The current year.
$(DATE.HOUR)	The current hour.
$(DATE.MINUTE)	The current minute.
$(ADMINSERVERPORT)	The port of the Administrator's server or port 4990.
$(ENDUSERSERVERPORT)	The port of the end user server or port 4991.
$(MSGSTORE)	The message storage (message store) root directory.
$(LOGDIR)	The Log file directory.
$(CONFIGDIR)	The configuration directory.
$(ENV.<env>)	The value of the environment variable <env>.
$(OPTION.<option>)	The value of the tuning parameter <option>.
$(FILE.<filename>)	The content of the file <filename>.
$(ENCODEHTML)	Encodes the HTML tags in the macro text.

Option	Description
$(NEWMSGSENDER)	The value of the **Send New Email As** setting located at **SMTP** > **Configuration** > **Global**.
$(POSTMASTER)	Sends the detected email message to the original sender as `postmaster@mycompany.com` and informs the sender that the original email message has been quarantined.
$(DAILYLIST)	This macro is replaced with a list of blocked email messages.
$(RECIPIENTNAME)	The SMTP address or directory user name of the recipient (if available).
$(RECIPIENT)	The SMTP address of the recipient.
$(ENDUSERLINK)	The value of the End User Interface configuration item.

Line template

The Line template defines the display of blocked email messages and relevant information including the link to allow delivery. You can add customized email messages or notifications to the template to provide information that is needed by email users.

The following text provides an example of a Line template:

```
<tr>

<td width="20%">$(ENCODEHTML $(MSG.FROM))</td>

  $(ENCODEHTML $(MSG.urn:schemas:httpmail:from))</td>

<td width="60%">

    $(ENCODEHTML $(ORIGMSG.SUBJECT))</td>

<td width="20%">

<a href="http://$(HTTPADDRESS):4990/$(CMD.HTTP_DELIVER)">

    Deliver</a><br>

a href="mailto:$(SMTPADDRESS)?subject=$(CMD.DELIVER)">

    Deliver by email</a></td>

</tr>
```

The example above is a mixture of HTML code and the template macros. This example displays a row in a table, and includes information such as Sender, Original Message Subject, and the respective delivery links. You can customize the formatting and use of macros. You can also make a test email message to trigger the rule to test the output of the quarantine report.

Defining recipients of a quarantine report

This topic specifies which email addresses, listed in the message storage that is storing quarantined email messages (the quarantine store), should be included in the quarantine report.

About this task

A recipient's email address is automatically added to the quarantine store if:

- The domain part of the SMTP address is found in one of the SMTP local domains.
- The domain part of the SMTP address is found in the semicolon separated list of additional domains defined in the tuning parameter `msgstore.quarantine_domains`. (A semicolon separated list of SMTP domains for which a quarantine is allowed, in addition to SMTP local domains.)

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **Quarantine Report Templates** tab, and then click **Add**.
3. Type a name for the report.
4. Click the **Email Template** tab.

   Reference: See "Quarantine Reports Template" on page 63 for an explanation about this template and the macros it uses.
5. Enter the macro that you want to use for the template.
6. Click the **Line Template** tab.

   Reference: See "Quarantine Reports Template" on page 63 for an explanation about this template and the macros it uses.
7. Enter the macros you want to use for each line.
8. Click **OK**, and then click **Save Changes**.

Inspecting the contents of files attached to incoming email messages

This topic explains how to enable Lotus Protector for Mail Security to examine the contents (keywords, regular expressions, URLs) of files that are attached to incoming email messages.

About this task

The following types of files are examined by Lotus Protector for Mail Security:

- Microsoft documents including Excel, PowerPoint, Word 95, Word 2003, Word 2007, XML
- Oracle Open Office documents
- Oracle StarOffice documents
- Lotus 1-2-3® workbook files
- PDF files
- RTF files
- Plaintext files including TXT, HTML, XML, and other files
- Archive files including 7z, bz2, gz, tar, rar, zip

Lotus Protector for Mail Security inspects the content of files attached to incoming email messages by using the analysis modules that have been enabled in the current policy rule. For example, if the policy rule specifies using the Keyword Search module and the URL Check module, then Lotus Protector for Mail Security uses these methods to examine the contents of the attached file before it relays the email message through the system. After the file attachment has been examined and considered safe (by matching the policy rule), the policy system continues to process the email message according to what response or actions (Allow, Block, Continue) have been defined when the email message matches the policy rule.

Procedure

1. Click **Mail Security** > **Policy** in the navigation pane.
2. Click the **File Attachment Analysis** tab.
3. Select the **Enable File Attachment Analysis** check box.

   Important: Enabling this feature might cause a decrease in the throughput average of email messages because Lotus Protector for Mail Security is examining large amounts of data.

Configuring the DNSBL/Spam Flow setting

This topic explains how to configure the Spam Flow Control setting and manage the list of DNSBL (Domain Name Server Block List) servers used by Lotus Protector for Mail Security.

Spam Flow settings

The Spam Flow Control module consists of a number of different email similarity measures. For a given email message, each similarity measure produces a unique signature. Each signature has an associated list of unique domains extracted from the sender's SMTP address (for example, `mycompany.com` from `joe@mycompany.com`) and a hit count of occurrences over a given time frame. If a domain list for a signature contains a predefined number of entries, the hit counter for this signature is incremented by the Spam Flow Control analysis module each time this signature is found in an email message.

If, over a given time frame, the signature count exceeds a predetermined threshold, every subsequent email message that is analyzed by the Spam Flow Control module matches.

Table 24. Spam flow settings

Option	Description
Analysis Window	Sets the number of seconds the analysis module keeps and maintains a certain signature. This setting also affects the amount of time the analysis module matches on a certain signature.
Minimum Hits	Specifies the necessary amount of occurrences for a certain signature in the flow of analyzed email messages before any subsequent occurrence of the signature is considered a match.

DNSBL Lists

A DNSBL server contains a list of IP addresses for hosts that are known to send or relay unsolicited email messages. The quality of a DNSBL list depends on the methods used by the DNSBL servers to establish its list of known spammers.

Table 25. DNSBL list settings

Option	Description
Threshold	If the sum of all DNSBL server match scores exceeds this number, the analyzed email message is considered a match for the Spam DNSBL analysis module.
Spam DNSBL Server	The host name of the DNSBL server you want to use (for example, `dnsbl.cobion.com`).
Match Score	Specifies the value that is added to the total score if this particular DNSBL server returns a positive result. This value can be used to fine tune the mechanism, if you use DNSBL servers with different reliabilities.

Note: When DNSBL lookups are performed as DNS requests, DNSBL matching can be fast. However, because DNS requests are used on demand from the network, analysis of an email message can be delayed until Lotus Protector for Mail Security receives an answer from available DNSBL servers. Using a large number of DNSBL servers can have a negative impact on the performance of Lotus Protector for Mail Security.

Setting up access privileges for the End User Interface

This topic explains how to set up access privileges for the End User Interface to allow users to browse and view their quarantined email messages, to manage personal block lists and allow lists, or to generate and deliver their daily quarantine report.

You can either allow full access to the End User Interface by setting the **Default Access Mode** to *Granted* or use a more granular setup by adding Who Objects to the list. The Default Access Mode always applies to users who are not represented by any of the Who Objects in the list.

Attention: If you plan on using the End User Interface, make sure you have opened the Lotus Protector for Mail Security firewall for access to the End User Interface on the Firewall page.

Table 26. End User Interface settings

Option	Description
Default Access Mode	Specifies the access mode for users who are not represented by a Who Object in the access list: • Granted: Users, not represented by any of the Who Objects, are allowed access to the End User Interface. • Denied: Access is denied to users who are not represented by any of the Who Objects in the list.
End User Interface URL	Provides the URL address of a website that a user can access in order to use the End User Interface. This URL is also used in the quarantine reports.
Who	Specifies that a particular user or group, represented by the Who Object, has a specific access mode.
Access Type	Specifies the access mode for a specific Who Object: • Granted: Users, as represented by the Who Object, are allowed access to the End User Interface. • Denied: Access is denied to users represented by the Who Object.

Tracking email messages

This topic explains how to track email messages passing through Lotus Protector for Mail Security, until the email messages are delivered or dropped.

Message Tracking

Option	Description
Tracking Level	Sets the level at which Lotus Protector for Mail Security should track the flow of email messages through the system: • Disabled: Lotus Protector for Mail Security will not track email messages. • Standard: Lotus Protector for Mail Security tracks the following information about an email message: – When the email message entered the system at the SMTP layer – When the email message was processed by the mail security policy – When the email message was delivered at the SMTP layer This option is useful when you use Recipient Verification at the SMTP layer to track the following information about an email message: – When and why the email message was rejected or dropped at the SMTP layer – The flow of an email message through the system (such as which sending server accepted the email message) – The delay between when the email message was accepted at the SMTP layer and analyzed – Which SMTP server delivered the email message • Verbose (more details): Lotus Protector for Mail Security uses the information it has gathered from the following sources: – The Standard mode (see above) – Logging information – Analysis details This option is useful if you must contact IBM Support about an issue you are having with email messages passing through Lotus Protector for Mail Security.

Chapter 4. Alerts, system events, and logs

This chapter describes how to configure notifications that alert you or others when specified events occur, how to view and manage system events, and how to view and generate log files.

Using email and SNMP alerts

The topic explains how to set up alert messages that notify you of system events.

Procedure

1. Click **System** > **Email and SNMP Alerts** in the navigation pane.
2. Click the **Alert Configuration** tab.
3. Select any of the following alert logging check boxes:

Option	Description
Send Alerts for Mail Security Events	Notifies you when a mail security event has occurred.
Send Alerts for System Error Events	Notifies you when a system error has occurred. An error has a description and might have additional information describing the reason for the error.
Send Alerts for System Warning Events	Notifies you when a problem has occurred on Lotus Protector for Mail Security itself.
Send Alerts for System Information Events	Notifies you about what actions users might have performed on Lotus Protector for Mail Security, such as changing passwords, downloading logs, or editing a parameter. **Note:** If you enable the **Send Alerts for System Information Events** setting, and then reboot Lotus Protector for Mail Security, you might receive the following message in the Message.log or as an SMTP or SNMP notification message: `Critical entry point(ResponsesdkGetClassObject) of library...` This is expected behavior for the system notification and does not require user intervention.

Option	Description
Notification Delivery methods	Specifies how event notification and message delivery are enabled: • Send to Email address/Email Name: Sends a notification to the email address specified in the default email name when the alert occurs. • Send to SNMP trap: Triggers an SNMP trap when the alert occurs. • Configure SNMP: – SSH: Provides secure log on for Windows and Unix clients and servers. – SNMP Get: Queries SNMP information about a network server - System Name: Specifies the target of the SNMP get request. - System Location: Specifies the location of the server on the network. - Contact Information: Sets the system contact using the SNMP community name. - Get Community: Specifies the SNMP community name (public or private) used in the SNMP get request. SNMP Trap: - Trap Receiver Address: Specifies the server IP address where the SNMP Manager is running. The SNMP host must be accessible to Lotus Protector for Mail Security to send email notifications. - Trap Community: Specifies the appropriate community name (public or private). - Trap Version: • V1: Simple Network Management Protocol version 1 • V2c: Community-Based Simple Network Management Protocol version 2

4. Click **Save Changes**.

Defining recipients of alert messages

This topic explains how to send alert messages to a designated email address or email group.

Procedure

1. Click **System** > **Email and SNMP Alerts** in the navigation pane.
2. Click the **Alert Configuration** tab.
3. In the **Email Configuration** section, click **Add**.
4. Provide the following information:

Option	Description
Name	Identifies the email alert configuration
SMTP Host	Identifies the mail server (as a fully qualified domain name or IP address)
To	Identifies the email address of the intended recipient (individual or group)
Subject Format	Lets you enter text and select from a list of message subject fields. You can insert multiple fields.
Body Format	Lets you enter text and select from a list of body subject fields. You can insert multiple fields.

Configuring advanced parameters for event notification

This topic explains how to use advanced parameters that provide greater control over the event notification behavior of Lotus Protector for Mail Security.

Procedure

1. Click **System** > **Email and SNMP Alerts** in the navigation pane.
2. Click the **Advanced Parameters** tab.
3. If the parameter you want to tune is not displayed in the Advanced Parameters tab, follow these steps:
   a. Click the **Add** icon.
   b. Type the name of the parameter.
   c. Type a description of the parameter.
   d. Specify the value type and value of the parameter.
4. If the parameter you want to tune is already displayed in the Advanced Parameters tab, click the value or description field and change the setting.

   Attention: In most cases, you should not have to change advanced parameters. However, do not change these parameters unless you are instructed by IBM Support.

Parameter name	Description	Default value
Trace.csf.filename	Identifies the name of the CSF trace file	`/var/spool/crm/CrmTrace.txt`

Parameter name	Description	Default value
Trace.csf.level	Identifies the level of trace information to display in the CSF trace file. Trace level settings are as follows: • 0 = No trace • 1 = Only errors • 2 = Only errors and warnings • 3 = Only errors, warnings, and anything worth noticing • 4 = Only errors, warnings, anything worth noticing, and informational messages • 5 = Errors, warnings, anything worth noticing, informational messages, and debug messages • 6 = All of levels 1 through 5	0
Trace.other.filename	Identifies the communications trace file	`/var/spool/crm/CrmCommTrace.txt`
Trace.other.level	Identifies the level of trace information to display in the communications trace file. Trace level settings are as follows: • 0 = No trace • 1 = Only errors • 2 = Only errors and warnings • 3 = Only errors, warnings, and anything worth noticing • 4 = Only errors, warnings, anything worth noticing, and informational messages • 5 = Errors, warnings, anything worth noticing, informational messages, and debug messages • 6 = All of levels 1 through 5	0

5. Click **OK**.

Managing system-related events

This topic explains how to view and manage mail security events, system messages, or update issues generated by the appliance over a specified period of time.

Procedure

1. Click **System** > **Events** in the navigation pane.
2. In the **Filter** field, select **On**.
3. Provide the following information:

Option	Description
Start Date	Instructs the filter to start filtering on this date, using the format: `yyyy-mm-dd hh:mm:ss` (for example, 2011-12-31 12:45:10)
End Date	Instructs the filter to stop filtering by this date, using the format: `yyyy-mm-dd hh:mm:ss` (for example, 2011-12-31 12:45:10)
Severity	Indicates the security level of the event: • High: Security issues that allow immediate remote or local access, or immediate execution of code or commands, with unauthorized privileges. **Example:** Most buffer overflows, back doors, default or no password, and bypassing security on firewalls or other network components. • Medium: Security issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components. **Example:** Cross-site scripting, man-in-the-middle attacks, SQL injection, denial of service of major applications, and denial of service resulting in system information disclosure (such as core files). • Low: Security issues that deny service or provide non-system information that might be used to formulate structured attacks on a target, but not directly gain unauthorized access. **Example:** Brute force attacks, non-system information disclosure (configurations, paths), and denial of service attacks.
Event Type	Specifies the type of event that you want to filter from the list.
Event Name	Indicates a unique, descriptive name for the event.

4. Click **Filter Results**.

Viewing log files

This topic explains how to view or download a log file to assist you when troubleshooting issues with Lotus Protector for Mail Security.

Procedure

1. Click **System** > **Log Files** in the navigation pane.
2. Choose a directory in the **Browse Directories** area.
3. Select the log file that you want to view.
4. Optional: Click the **Download** button to download the log file to a directory of your choice.

Generating a diagnostic file

This topic explains how to capture information that IBM Support can use to help you troubleshoot issues with Lotus Protector for Mail Security.

Procedure

1. Click **Support** > **Diagnostics File** in the navigation pane.
2. Set the number of days that you want to capture information for in the support data file.
3. Click **Generate Now**.

Note: The support data file uses the TGZ file name extension.

Viewing log files to determine why an email message was blocked

File	Description
/var/log/messages	Shows whether an email message was blocked because of a policy rule.
/etc/xmail/logs/	Shows whether an email message was blocked because of an SMTP-related issue.

Chapter 5. Predefined reports

This chapter describes how to use predefined reports to understand your mail security status.

Types of predefined reports

Lotus Protector for Mail Security includes predefined reports that provide details about the current status of the system, such as traffic flow, the top senders and internal recipients of spam-based email messages, and the current mail security policy in place.

Types of predefined reports

Lotus Protector for Mail Security provides the following predefined reports:

Table 27. Predefined reports

Report	Description
Executive Summary	Displays the overall throughput of Lotus Protector for Mail Security versus the email messages that where taken action on, and quarantined versus email messages released from quarantine.
Traffic Monitoring	Provides information about network traffic over a given period of time.
Matched Rules	Provides information about which policy rules matched over a given period of time.
Policy Configuration	Provides information about the mail security policy currently in place.
Top 10 Responses	Provides information about the top 10 responses that were executed by the mail security policy over a given period of time.
Top 10 Analysis Modules	Provides information about the top 10 analysis modules that have matched Analysis modules enabled in the mail security policy.
Top 10 Recipients	Provides information about the top 10 recipients by number of received email messages.
Top 10 Senders	Provides information about the top 10 senders by number of email messages sent.
Top 10 Viruses	Provides information about the top 10 viruses by number of infected email messages.

Generating a predefined report

This topic explains how to generate a predefined report.

Before you begin

Make sure you have selected **Reporting Enabled** in the Message Tracking/Reporting tab on the Mail Security Policy page.

Procedure

1. Click **Mail Security** > **Reporting** in the navigation pane.
2. If applicable, choose a data source, a starting time for the report, and an ending time for the report.
3. Select a report, and then click **Generate**.

Scheduling when to run predefined reports

This topic explains how schedule a predefined report from Lotus Protector for Mail Security at specified intervals.

Procedure

1. Click **Mail Security** > **Policy** in the navigation pane.
2. Click the **Message Tracking/Reporting** tab.
3. Select the **Reporting Enabled** box.
4. Provide the following information:

Option	Description
Days to Keep	Sets the number of days to keep the report on the file system.
General Reporting	• SNMP Trap Enabled: Sends an SNMP trap to an SNMP server. The trap includes event source IP addresses, requested URLs, and violated email categories. • System Log Enabled: Writes to a log file every time a report is run. • Database Enabled: Saves the report to the Lotus Protector for Mail Security database.

Option	Description
Configure Scheduled Reports	• Cluster: Specifies whether Lotus Protector for Mail Security belongs to a cluster. (All reports will report over all computers in a cluster scenario.) • Report: Select which report you want to schedule to run. • To: Specifies the email addresses for the recipients of the report. • Schedule: Specifies at what time a report should run, as set from **Mail Security** > **Policy Objects** > **Schedules**. **Example:** Type `Daily 7:00` to schedule the report to run every day at 7 a.m. • Time range: Specifies whether to run the report from a relative time range (time span relative to the current time) or an absolute time (has a fixed start and stop time).

5. Click **OK**, and then click **Apply Settings**.

Chapter 6. Backup and restore

This chapter describes how to manage snapshots of configuration settings for Lotus Protector for Mail Security and to create complete system backups of Lotus Protector for Mail Security settings.

Types of backups

You can generate snapshot files of configuration settings or perform a full system backup of the Lotus Protector for Mail Security operating system and current configuration settings.

Configuration backup

A configuration backup is a snapshot file that stores all of your Lotus Protector for Mail Security configuration settings. You can have many settings snapshot files of different configurations.

You also can create additional settings snapshot files if you want to test new policy settings for Lotus Protector for Mail Security. The default settings snapshot file, `factoryDefault.settings`, contains the original Lotus Protector for Mail Security settings. You should create a settings snapshot file before you change your configuration settings.

System backup

A system backup stores a complete image of the operating system and current configuration settings of Lotus Protector for Mail Security. You can have only one system backup file. When you restore from a system backup, you restore Lotus Protector for Mail Security to a previous state.

Backing up configuration settings

The process for updating Lotus Protector for Mail Security is designed to keep it up-to-date while taking the precautionary action of backing up your system before you install updates that alter original configuration settings.

About this task

Create a settings snapshot file of the original configuration settings for Lotus Protector for Mail Security before you apply firmware updates or change your configuration settings. You can also create additional settings snapshot files later if you want to use different configuration settings or test new policy settings.

The default settings snapshot file, `factoryDefault.settings`, contains the original Lotus Protector for Mail Security settings. You should create a settings snapshot file before you change your configuration settings.

Procedure

1. Click **Backup and Restore** > **System** in the navigation pane.
2. Click **Manage Configuration Backups**.
3. In the **Configuration Backups** section, choose an option:

Option	Description
Create a snapshot file	1. Click **New**. 2. Type a name for the snapshot file, and then click **Create**.
Restore a snapshot file	Select the snapshot file you want to restore, and then click **Restore**.
Delete a snapshot file	Select the snapshot file you want to delete, and then click **Delete**.
Upload a snapshot file	1. Click **New**. 2. Type the name of the snapshot file you want to upload, and then click **Upload**.
Download a snapshot file	Select the snapshot file you want to download, and then click **Download** to copy the file to your local computer.

Making full system backups

This topic explains how to create a complete image of the Lotus Protector for Mail Security operating system and current configuration settings before you apply firmware updates or apply snapshot files that change the original configuration settings.

Procedure

1. Click **Backup and Restore** > **System** in the navigation pane.
2. Click **Manage System Backup**.
3. Choose an option:

If you want to...	Then...
Create a full system backup	Click **Create System Backup**.
Restore a system backup	Click **Restore System Backup**.

Important: The IP address for Lotus Protector for Mail Security is unavailable during the backup process, and you cannot access Lotus Protector Manager in the browser window.

Chapter 7. Updates

This chapter describes how you can download and install firmware, database, and security content updates for Lotus Protector for Mail Security.

Important: You should update Lotus Protector for Mail Security as soon as possible after the initial setup to make sure you have the latest protection capabilities. Updates ensure that Lotus Protector for Mail Security has the latest fixes, features, security content, and database updates.

Viewing the current status and licenses for spam protection

This topic explains where to view the current status of the Lotus Protector for Mail Security spam protection databases and licenses.

The mail security updates provide daily updates of URLs and spam signatures for Lotus Protector for Mail Security.

Important: You should update your local mail security database at least once daily to keep it current.

Table 28. Component and license status

Option	Description
Components	Shows the current status of these components: • Content Filter Database: The Content Filter Database includes URLs and classification of web pages, including spam signatures for all known spams (gathered by spam collectors and other sources). • System Packages: The System Packages contain the latest hotfixes and patches for core system components. • Appliance Firmware: The firmware version of the Lotus Protector for Mail Security software. • Antivirus Signatures: The Antivirus signatures contain an list of virus definitions defined by IBM for well known viruses.
Licenses	Shows the current license status for these modules: • Mail Security: Enables you to install antispam updates for Lotus Protector for Mail Security. • Antivirus: Enables you to install antivirus updates for Lotus Protector for Mail Security.

Automating the update process

This topic explains how you can automate the process for checking, downloading, and installing updates to Lotus Protector for Mail Security.

About this task

IBM issues frequent updates for Lotus Protector for Mail Security; these updates can be either security content updates or product updates. You can schedule how frequently Lotus Protector for Mail Security checks for updates. How frequently Lotus Protector for Mail Security checks for updates can be defined separately for security content updates and product updates.

Procedure

1. Click **Updates** > **Automatic Updates** in the navigation pane.
2. Click the **Update Settings** tab.
3. Provide the following information:

Option	Description
Configure HTTPS Proxy	Specifies proxy server information if Lotus Protector for Mail Security uses a proxy server to access the update server: • Address: Specifies the address of the proxy server. **Note:** The following authentication exceptions must be added if there is no static proxy user available: – `*.ibm.com` – `license.cobion.com` – IP addresses that resolve to `filterdb.ibm.com` (currently 85.25.143.136, 85.25.252.124, 87.106.3.48, 87.106.21.125, 206.253.225.12) • Port: Specifies the port of the proxy server. • Enable Authentication: Enable this option if you want Lotus Protector for Mail Security to authenticate to the proxy server, and then type the user ID and password. • User ID/Password: Specifies the user ID and password used for authentication.
Automatically Check for Updates	Specifies how often Lotus Protector for Mail Security should connect to the update server and check for updates: • Check for updates daily or weekly: Specifies the day of week and time of day **Note:** Make sure that Lotus Protector for Mail Security checks for updates at least one hour before automatic installations to ensure sufficient time for downloading updates. • Check for updates at given intervals: Specifies an interval (in minutes) **Note:** The range is 60 minutes to 1440 minutes (24 hours).

Option	Description
Security Updates	Specifies how Lotus Protector for Mail Security should process available security updates: • Automatically Download: Enables Lotus Protector for Mail Security to download any applicable updates it finds • Automatically Install: Enables Lotus Protector for Mail Security to automatically install any downloaded updates
Mail Security Database Updates	Contains the latest spam signatures and heuristics for the Lotus Protector for Mail Security database.
Firmware Updates	Contains an update from the Download Center that includes: • New program files • Fixes or patches • Enhancements • Online Help **Note:** Some firmware updates require that you reboot Lotus Protector for Mail Security after installation.
Install Options: Perform Full System Backup Before Installation	This option is enabled by default. You should perform a full system backup before you install a firmware update. Lotus Protector for Mail Security stores only one system backup, therefore this option overwrites the previous system backup. • Do Not Install: Requires you to do all installations manually. This option gives you the most control over how an installation impacts your operation. • Automatically Install Updates: Installs updates automatically based on the When To Install choice you selected: – Delayed: Designates the day of week and time of day the installations occur – Immediate: Starts the installation as soon as the update is downloaded. This option gives you the least control and predictability of when an installation occurs. **Attention:** Installing an update can take the system offline while the installation is in progress.

Configuring event notification for updates

This topic explains how to configure Lotus Protector for Mail Security to notify you about updates.

Procedure

1. Click **Updates** > **Automatic Updates** in the navigation pane.
2. Click the **Event Notification** tab.
3. Provide the following information:

Option	Description
Alert Logging for Available Updates	Notifies you when there are updates available to download and install.
Alert Logging for Update Installation	Notifies you when updates have been installed.
Alert Logging for Update Errors	Notifies you of errors that have occurred during the installation of an update.
Notification Delivery	Specifies how event notification and message delivery are enabled: • Email Enabled: Determines whether email is enabled for the selected message level. • Email Name: Specifies the default email name for the selected message level. • Configure Email: Allows you to configure email settings for the selected message level. • SNMP Trap Enabled: Determines whether SNMP trap is enabled for the selected message level. • Configure SNMP: Allows you to configure SNMP settings for the selected message level.

Configuring advanced parameters for automatic updates

This topic explains how to configure advanced parameters that help diagnose, correct, or improve performance issues you might be experiencing while applying updates to Lotus Protector for Mail Security.

Procedure

1. Click **Updates** > **Automatic Updates** in the navigation pane.
2. Click the **Advanced Parameters** tab.
3. If the parameter you want to tune is not displayed in the Advanced Parameters tab, follow these steps:
   a. Click the **Add** icon.
   b. Type the name of the parameter.
   c. Type a description of the parameter.
   d. Specify the value type and value of the parameter.
4. If the parameter you want to tune is already displayed in the Advanced Parameters tab, click the value or description field and change the setting.

   Attention: In most cases, you should not have to change advanced parameters. However, do not change these parameters unless you are instructed by IBM Support.

Name and description	Default value
update.disable.remote.discovery Flag for turning off remote discovery of update files from the configured download server.	False
update.preserve.update.files Flag to indicate not to delete update package files after they have been successfully installed.	False

5. Click **OK**, and then click **Save Changes**.

Appendix A. End User Interface

This appendix describes how an Administrator can set up user accounts and access privileges for the End User Interface.

Setting up access privileges for the End User Interface

This topic explains how to set up access privileges to the End User Interface that allow users to browse and view their quarantined email messages, to manage personal block lists and allow lists, and to generate and deliver their daily quarantine report.

About this task

You can either allow full access to the End User Interface by setting the **Default Access Mode** to *Granted* or use a more granular setup by adding Who Objects to the list. The Default Access Mode always applies to users who are not represented by any of the Who Objects in the list.

Attention: If you plan on using the End User Interface, make sure you have opened the Lotus Protector for Mail Security firewall for access to the End User Interface on the Firewall page.

Procedure

1. Click **Mail Security** > **Policy** in the navigation pane.
2. Click the **End User Interface** tab.
3. Provide the following information:

Option	Description
Default Access Mode	Specifies the access mode for users who are not represented by a Who Object in the access list: • Granted: Users, not represented by any of the Who Objects, are allowed to access the End User Interface. • Denied: Access is denied to users who are not represented by any of the Who Objects in the list.
End User Interface URL	Provides the URL address of a website that a user can access in order to use the End User Interface. This URL is also used in the quarantine reports. You can enter a host name or an IP address, but the entry must start with `https://`. **Example:** `https://<host name>:4443` **Note:** Changing the port for this URL does not change the listening port of the internal web server. You might need to change this port if you are translating a custom port for the default port on a firewall. **Attention:** Make sure the specified host name, either set through a macro or set manually, can be resolved within your network environment.
Who	Specifies that a particular user or group, represented by the Who Object, has a specific access mode.

Option	Description
Access Type	Specifies the access mode for a specific Who Object: • Granted: Users, as represented by the Who Object, are allowed to access the End User Interface. • Denied: Access is denied to users represented by the Who Object.

4. Click **OK**, and then click **Save Changes**. The entry is displayed in the list.

Managing user accounts for the End User Interface

This topic explains how to search for user names on the End User Interface, to delete a block list or an allow list for a user from the End User Interface, to delete a user from managing a block or allow list on the End User Interface, or to reset a user's password for accessing the End User Interface.

Table 29. End User Interface tasks

Button	Description
Filter	Searches for a user on the End User Interface.
Delete Block List/Delete Allow List	Deletes a block list or allow list for a user on the End User Interface.
Delete User	Deletes a user from managing a block list or an allow list on the End User Interface.
Reset Password	Resets a user's password for accessing the End User Interface. The new password is automatically sent by email message to that user.

Configuring advanced parameters for the End User Interface

This topic explains how to configure advanced parameters that help diagnose, correct, or improve performance issues you might be experiencing with the End User Interface.

Procedure

1. Click **Mail Security** > **Policy** in the navigation pane.
2. Click the **Advanced Parameters** tab.
3. If the parameter you want to tune is not displayed in the Advanced Parameters tab, follow these steps:
   a. Click the **Add** icon.
   b. Type the name of the parameter.
   c. Type a description of the parameter.
   d. Specify the value type and value of the parameter.
4. If the parameter you want to tune is already displayed in the Advanced Parameters tab, click the value or description field and change the setting.

   Attention: In most cases, you should not have to change advanced parameters. However, do not change these parameters unless you are instructed by IBM Support.

Name and description	Default value
clientconnections.count The default amount of client connections that can be used at the same time for users to access theEnd User Interface.	4

5. Click **OK**.

Appendix B. Mail Security clusters

This appendix describes how to manage a cluster of Mail Security appliances that distributes policy management over multiple systems.

About Mail Security clusters

A Mail Security cluster consists of a number of Lotus Protector for Mail Security appliances (or virtual appliances running on a VMware ESX Server) in which one appliance acts as the central appliance (*Cluster Central*), and the other appliances become clients of the central appliance (*Cluster Clients*).

About Mail Security clusters

A Mail Security cluster consists of a number of appliances (or virtual appliances running on a VMware ESX Server) in which one appliance acts as the central appliance (*Cluster Central*), and the other appliances become clients of the central appliance (*Cluster Clients*).

How is data processed in the Mail Security cluster

All members of the Mail Security cluster share the policy configuration settings of the central appliance. The policy configuration settings for the central appliance are defined on the Mail Security Policy page (Mail Security > Policy) and the Mail Security Policy Objects page (Mail Security > Policy Objects).

The central appliance acts as the central database server for the Mail Security cluster. Each appliance in the Mail Security cluster has a local database that stores all the information for the email messages processed on that specific appliance. All appliances in the Mail Security cluster replicate database changes (such as new data, changed data, or deleted data) from their local database to the database for the central appliance. The database used by the central appliance collects that data to allow users to browse their quarantine stores, and to also generate and send quarantine reports to users.

Settings that are managed and replicated by the cluster

- Mail Security > Policy
- Mail Security > Policy Objects

  Some SMTP settings refer to the Policy Objects defined under Mail Security. Policy Objects are replicated between cluster members, but SMTP settings are not replicated. Remove all references to Policy Objects from SMTP > Configuration > Receiving SMTP > Recipient Verification. After the cluster is established, make sure you reactivate Recipient Verification.
- Mail Security > Reporting
- End Users registered with the appliance
- Block and Allow list entries (regardless of whether there is an LDAP Directory user or a "local" user that only exists on the appliances)
- All Cluster Clients replicate their quarantine report data to the Cluster Central. The Cluster Central then generates the quarantine reports. Users will only receive one quarantine report containing all quarantined email messages, regardless of which appliance processed the email messages.
- Mail Security > Email Browser (Message store data is no longer replicated.) When searching the Message Store, the search query is distributed to all the hosts in the cluster and the results are combined into a single view (like peer-to-peer searching).

Settings that are managed locally by members of the cluster (Cluster Clients)

- SMTP Settings
- TLS Certificates
- Firewall Settings
- IPS Settings
- Network Settings
- Routing
- Update Settings
- License Keys
- Backups

Creating a new Mail Security cluster

Use the Clustering page to create a cluster of Mail Security appliances that distributes policy management over multiple appliances.

About this task

When a Mail Security cluster is created:

- The appliance loses all of its current data, including email messages.
- All references to Schedule Objects (Mail Security > Policy Objects > Schedules) and FTP Server Objects (Mail Security > Policy Objects > FTP Servers) must be removed.

Procedure

1. Click **Mail Security** > **Clustering** in the navigation pane.
2. Click **Create a New Cluster** and click **Next**.

   Attention: The following configuration settings are automatically applied to the appliance during the process of creating the cluster:

   - Firewall ports 5432 (database) and 4990 (cluster communication) are opened to allow communication between the central appliance and an appliance that is joining the cluster.
   - The network time server is enabled to synchronize the time settings on all members of the Mail Security cluster.
3. In the **New Cluster Settings** section:
   a. Type and then confirm the passphrase for the Mail Security cluster.

      Attention: Choose a passphrase you can remember. IBM will not be able to reset or recover your passphrase after you have created it.

   b. Select an IP address from the **Communications IP** list and click **Next**.
4. Once all details have been collected, click **Next** to start the process for creating the cluster.

   Important: The appliance loses all of its current data, including email messages during the cluster creation process. You will not be able to access services on the appliance until the process for creating the cluster has been completed.

Joining an existing Mail Security cluster

Use the Clustering page to add the appliance to an existing Mail Security cluster if you want to share the load across multiple machines.

About this task

When an appliance joins an existing Mail Security cluster:

- The appliance loses all of its current data, including email messages.
- All references to Schedule Objects (Mail Security > Policy Objects > Schedules) and FTP Server Objects (Mail Security > Policy Objects > FTP Servers) must be removed.

Procedure

1. Click **Mail Security** > **Clustering** in the navigation pane.
2. Click **Join an Existing Cluster** and click **Next**.

   Attention: The following configuration settings are automatically applied to an appliance joining the cluster:

   - Firewall ports 5432 (database) and 4990 (cluster communication) are opened to allow communication between the central appliance and an appliance that is joining the cluster.
   - The network time server is enabled to synchronize the time settings on all members of the Mail Security cluster.
   - All Who objects are removed from SMTP Recipient Verification.
   - The FTP log file backup is disabled.
3. In the **Cluster Connection Details** section:
   a. Type the IP address of the central appliance for the Mail Security cluster.
   b. Type and then confirm the passphrase for the Mail Security cluster.
   c. Select an IP address for the appliance that is joining from the **Communications IP** list and click **Next**.
4. Click **Next** to start the process of joining the cluster.

   An appliance performs the following steps in order to receive the connection parameters to the database of the central appliance:

   a. Stops processing email messages, including the SMTP server.
   b. Connects to the database of the central appliance.
   c. Deletes all data from its own database.
   d. Replicates all configuration data from the central appliance (*Cluster Central*) to its own database.
   e. Applies the policy previously read from the database of the central appliance.
   f. Starts processing email messages.

Changing a passphrase or an IP address for the Mail Security cluster

This topic explains how to change the passphrase for the central appliance in the Mail Security cluster, or to change an IP address for any appliance in the Mail Security cluster.

Procedure

1. Click **Mail Security** > **Clustering** in the navigation pane.
2. Click **Manage this Cluster**.
3. Choose an option:

If you want to...	Then...
Change the passphrase for the primary central appliance in the cluster	1. Go to the *Cluster Central* appliance, and then click **Change Cluster Passphrase**. 2. Type the current passphrase for the Mail Security cluster, and then type the new passphrase twice to confirm it. 3. Click **Change Passphrase**.
Change the IP address of an appliance in the cluster	1. Choose an appliance, and then click **Update IP Address**. 2. Type the passphrase for the Mail Security cluster, and then provide a new IP address. 3. Click **Change IP Address**.

Removing a client from the Mail Security cluster

This topic explains how to remove a client from a Mail Security cluster.

Procedure

1. Click **Mail Security** > **Clustering** in the navigation pane.
2. Click **Manage this Cluster**.
3. Choose the client you want to remove from the Mail Security cluster.
4. Type the passphrase for the Mail Security cluster.

   Note: This is the passphrase that was set when you or another Administrator created the Mail Security cluster.
5. Click **Remove this client**. The client stops processing SMTP traffic and leaves the Mail Security cluster.
6. Restart the processing of SMTP traffic.

Erasing a cluster of Mail Security appliances

This topic explains how to return a cluster of Mail Security appliances back into a single appliance.

Procedure

1. Click **Mail Security** > **Clustering** in the navigation pane.
2. On the Cluster Central Mode page, click **Erase this Cluster**.
3. Type the passphrase for the Mail Security cluster, and then choose to erase the cluster.

Appendix C. Lotus Domino integration

This appendix describes how to integrate Lotus Protector for Mail Security (version 2.5 or later) with your existing Lotus Domino and Notes® (version 8.5.1 or later) infrastructure.

Lotus Domino Server configuration

You must specify settings in the Domino Administrator desktop policy that enable Lotus Protector for Mail Security to incorporate its spam protection features with Lotus Notes® clients. All protection features are available when the Lotus Notes client receives the Lotus Domino policy.

Configuring the Domino Administrator desktop policy to enable integration

Use the `NOTES.INI` setting `$PROTECTOR_LOCATION` to specify the location of the address that you should use to access Lotus Protector for Mail Security.

Procedure

1. From the Domino Administrator desktop policy settings document, click the **Custom Settings - Notes.ini** tab.
2. Click **Edit list**.
3. Complete these fields:

Option	Description
Item	Specify `$PROTECTOR_LOCATION`
Value	Provide the address for Lotus Protector for Mail Security using any of the following formats: • address:port (for example: `protector1.mycompany.com:4443`) • ip:port (for example: `192.168.2.42:4443`) **Note:** Lotus Protector for Mail Security typically uses port 4443. The connection port might be different if you use NAT as part of your network setup.
Enforce	Click this check box if you are enforcing the policy setting. If you enforce the policy, it will override settings that have precedence over this setting including those assigned through an Explicit policy.

4. Save and close the policy settings document.

What to do next

Configure settings on Lotus Protector for Mail Security to enable integration with the Lotus Domino server.

Lotus Protector for Mail Security configuration

This topic explains how to enable access privileges and user authentication on Lotus Protector for Mail Security that are needed for integration with the Lotus Domino server.

Before you begin: You must have a Lotus Protector for Mail Security system that is already online and filtering mail traffic. The Administrator for Lotus Protector for Mail Security must be logged in the Lotus Protector Manager.

Enabling access privileges for Lotus Notes users

This topic explains how to set up access privileges that allow Lotus Notes users to browse and view their blocked email messages, to manage personal block lists and allow lists, or to generate and deliver their daily quarantine report.

Opening ports on the local firewall

You must make sure Lotus Protector for Mail Security can connect to TCP port 4443 so that Lotus Notes users can access the End User Interface.

Procedure

1. Click **System** > **Firewall** in the navigation pane.
2. In the Enduser Access (4443) section, enable the interface connected to your internal network (typically eth1).
3. Save your changes.

Setting up access privileges to the End User Interface

You must set up access privileges to the End User Interface that allow Lotus Notes users to browse and view their blocked email messages, to manage personal block lists and allow lists, and to generate and deliver their daily quarantine report.

Procedure

1. Click **Mail Security** > **Policy** in the navigation pane.
2. Click the **End User Interface** tab.
3. Set the **Default Access Mode** to *Granted*.
4. Save your changes.

Enabling user authentication through your Lotus Domino server

You must register your Lotus Domino server with Lotus Protector for Mail Security in order for your users to authenticate using your Domino server. Lotus Protector for Mail Security communicates with the Domino server using LDAP. If LDAP access to your Domino server requires authentication, you must provide the necessary login credentials.

Setting up a connection to the Lotus Domino server

Procedure

1. Click **Mail Security** > **Policy Objects** in the navigation pane.
2. Click the **Directories** tab.
3. Locate the entry for `Domino example domain` in the list of directories.
4. Enable the **Active** check box next to this entry.
5. Click the **Edit** icon.
6. Click the **LDAP Server** tab.
7. In the **Host** field, type the host name or IP address of your Domino server.
8. In the **Username** field, type the user name of the user who has the appropriate access rights to read from the Domino LDAP.
9. Click **Enter Password**, and then type the password for the LDAP user you specified in the **Username** field.
10. Click **OK**, and then save your changes.

    Note: Although a Domino server is the preferred directory server for user authentication, you can use most LDAP-compatible directory servers. This can be useful, for example, if you use Microsoft Active Directory for user authentication.

Troubleshooting the LDAP connection to your Lotus Domino server

Most LDAP directory integration problems occur because of an incorrect LDAP user name or password. You can check the Event Log in Lotus Protector Manager to determine if Lotus Protector for Mail Security has connected with the LDAP server for Lotus Domino. However, you might not see any LDAP-related events until a user has tried to authenticate via Lotus Domino.

Procedure

1. Click **System** > **Event** in the navigation pane.
2. Search the Event Log for errors that might indicate that there were problems connecting to the LDAP server for Lotus Domino.

Appendix D. Advanced parameters

This appendix describes the advanced parameters for Lotus Protector for Mail Security that you use to diagnose, correct, or improve performance issues you might be experiencing with your network or environment.

Important: You should not change these parameters unless you are instructed by IBM Support.

General advanced parameters

This topic defines some of the more common advanced parameters that apply to Lotus Protector for Mail Security.

Table 30. General advanced parameters

Name and description	Default value
log_level Enables or disables the output of email messages. The possible values range from 0 (no log output) to 4 (detailed log output).	0
recipient.nospam_learn Specifies the recipient email address for the collector of emails that are not spam.	notspam@kassel.ibm.com
recipient.spam_learn Specifies the recipient email address for the collector of emails that are spam.	spam@kassel.ibm.com
sendmail.includetrackingdata If set to *true*, message tracking data is attached to email messages sent to nospam_learn and spam_learn.	True
display_mailbody.disable If set to *true*, the message store browser will not display the body of an email message.	False
Resource monitoring	
operational.behaviour Adjusts the thresholds for entering the memory and disk space warning levels at 1 and 2. 0 = The software can use less memory or disk space than normal until the warning levels are reached. 1 = Normal behavior 2 = The software can use more memory or disk space than normal until the warning levels are reached. 3 = A special value for disabling resource monitoring. It is not recommended that you use this value.	1
Filter database	

Table 30. General advanced parameters (continued)

Name and description	Default value
dbupdates.maxbandwidth Limits the amount of bandwidth used during database updates to the given value in KB per second. A value of 0 will not limit the amount of bandwidth used.	0 (KB per second)
dbupdates.weblearn Enables the upload of unknown URLs to the Download Server.	False

Advanced parameters for LDAP servers

This topic defines the advanced parameters that apply to LDAP directory servers used by Lotus Protector for Mail Security.

Table 31. LDAP server advanced parameters

Name and description	Default value
dirservice.connection.timeout Specifies the timeout value for the socket connection used for all LDAP server and NTLM client queries. If the connection is not successful (after the timeout has expired), the server is marked as unreachable.	3000 (in milliseconds)
dirservice.reconnect.interval Sets the amount of time that an unreachable NTLM client or LDAP server remains in an unreachable state until reconnecting.	180 (in seconds)

Advanced parameters for message storages

This topic defines the advanced parameters that apply to the message storages used by Lotus Protector for Mail Security.

Table 32. Message storages advanced parameters

Name and description	Default value
msgstore.release.tag.subject.disable If set to *false*, email messages are tagged when they are released from a quarantine store. See **msgstore.release.tag.subject.string** parameter below.	False
msgstore.release.tag.subject.string Adds this string at the beginning of the subject of an email message when the email message is released from a quarantine store. See **msgstore.release.tag.subject.disable** parameter above.	[Release from quarantine]
nospam.send.to.recipients If set to *true*, an email message that has been sent to notspam@kassel.ibm.com will be sent to the original recipient(s) as well.	False
quarantinereport.maxlines Sets the maximum number of email messages reported in one quarantine report.	100
msgstore.quarantine_domains Indicates a semicolon separated list of SMTP domains for which a quarantine is allowed (in addition to SMTP local domains).	

Advanced parameters for SMTP settings

This topic defines the advanced parameters that apply to the SMTP settings used by Lotus Protector for Mail Security.

Table 33. SMTP settings advanced parameters

Name and description	Default value
smtp.command_delay Sets the delay on each SMTP command.	0 (in milliseconds)
smtp.passthrough If set to *true*, email messages are not analyzed, but forwarded to the next SMTP relay.	False
xmail.smtp.threads Specifies the number of threads used for receiving email messages.	256
smtp.check_helo_domain Enables the HELO domain check according to RFC2821 4.1.2.	0
smtp.check_return_path Enables the return path (MAIL FROM) check according to RFC2821 4.1.2.	0
smtp.check_forward_path Enables the forward path (MAIL FROM) check according to RFC2821 4.1.2.	0
smtp.throttle.unchecked_max_count Sets the maximum calculated value of the fill level for the unchecked queue. **Important:** You should not change this value unless it is absolutely necessary.	10000/5000
smtp.ipc.send_timeout Specifies the timeout value of IPC sends to the mailsec daemon.	50000 (in milliseconds)

Advanced parameters for the DNS Block List (DNSBL) settings

This topic defines the advanced parameters that apply to the DNS Block List (DNSBL) settings.

Table 34. DNS Block List settings advanced parameters

Name and description	Default value
dnsblthreads.count The minimum amount of DNSBL threads used for the DNSBL check. If needed, the check dynamically allocates threads up to the value of the maximum amount.	20 (hardware) 10 (VMware)
host_reputation.border_ips A semicolon separated list of DNSBL border IP addresses.	

Advanced parameters for a replication of clusters

This topic defines the advanced parameters that apply to a replication of a cluster of appliances.

Table 35. Cluster replication advanced parameters

Name and description	Default value
replication.alerting.warn.perc A warning alert is generated if the replication rating exceeds this value.	90
replication.alerting.warn.duration A warning state is applied if the fill level exceeds the **warn.perc** value for more than a given period of time.	30*60 (30 minutes)
replication.alerting.error.perc An error alert is generated if the replication rating exceeds this value.	200
replication.alerting.error.duration An error state is applied if the fill level exceeds the **error.perc** value for more than a given period of time.	60*60 (1 hour)
replication.alerting.critical.perc If the replication rating exceeds this value, the cluster host is forcibly removed from the cluster to avoid overflowing the size of the database.	400
replication.alerting.critical.duration A critical state is applied if the fill level exceeds the **critical.perc** value for more than a given period of time.	24*60*60 (1 day)

Advanced parameters for the End User Interface

This topic defines the advanced parameters that apply to accessing the End User Interface.

Table 36. End User Interface advanced parameters

Name and description	Default value
clientconnections.count Specifies the default amount of client connections that can be used at the same time in order for users to access the End User Interface.	4

Appendix E. Accessibility features for Lotus Protector for Mail Security

Accessibility features help users who have a physical disability, such as restricted mobility or limited vision, to use information technology products successfully.

IBM and accessibility

See the *IBM Accessibility Center* at http://www.ibm.com/able for more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
P.O. Box 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709-2195
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

IBM, the IBM logo, and ibm.com, and Lotus are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Index

Special characters

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z

Printed in USA

SC27-3829-01