GFI MailSecurity

ADMINISTRATOR GUIDE

Find out how to configure GFI MailSecurity in different environments, and learn how to set up advanced features.

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranties of any kind, either express or implied, including without limitation any warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software disclaims and in no event shall be liable for any losses or damages of any kind, including any consequential or incidental damages in connection with the furnishing, performance or use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no warranty, promise or guarantee about the completeness, accuracy, recency or adequacy of information contained in this document and is not responsible for misprints, out-of-date information, or errors. GFI reserves the right to revise or update its products, software or documentation without notice. You must take full responsibility for your use and application of any GFI product or service. No part of this documentation may be reproduced in any form by any means without prior written authorization of GFI Software.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

Document Version: 1.0

Last updated (month/day/year): 12/16/2019

Contents

1 Getting Started

Want to try out GFI MailSecurity? This topic provides a quick list of actions to help you set up a GFI MailSecurity account.

1 **Sign up to GFI MailSecurity**
Go to https://gfimailsecurity.com and sign up for GFI MailSecurity.

2 **Log in to the GFI MailSecurity Admin Console**
Go to https://eu.gfimailsecurity.com for EU datacenter or https://us.gfimailsecurity.com for US datacenters. Use the credentials specified when registering to GFI MailSecurity (Root Account) to log in to the Admin Console.

3 **Create a domain on GFI MailSecurity**
Creating a domain is very simple, in GFI MailSecurity after logging in as the Domain Group Administrator. Do the following to create domain.

- Go to Settings > Mail Relay
- Click on Add Domain.
- Enter the Domain (eg “gfi.com”) and the host where the email server resides

4 **Update MX Record**
Update MX records to the GFI MailSecurity records. The instructions for this is available in the welcome email. For more information refer to Email Routing.

5 **Sending test mail**
Send a test mail. This will be routed through the GFI MailSecurity data center.
The DNS changes might take some time to take effect, and until such changes take effect not all emails would be routed through the service.

Topics in this section:

1.1 Email Routing

Use this information to plan and set up the email routing for using GFI MailSecurity.

Inbound Mail Routing Requirements

Configure your email domain's MX records to point to GFI MailSecurity. This enables all inbound email to get filtered by the Security service.

To do this, replace your current MX records with the following records:

MX Record	MX Preference
`EU DataCenter`	
`eu01.gfimailsecurity.com`	5
`eu02.gfimailsecurity.com`	10
`US DataCenter`	

MX Record	MX Preference
`us01.gfimailsecurity.com`	5
`us02.gfimailsecurity.com`	10
`us03.gfimailsecurity.com`	15

This ensures that all inbound emails get routed and processed by GFI MailSecurity before reaching your infrastructure.

> **NOTE**
> Secondary or other MX records are not usually required. Be aware that spammers sometimes target secondary or lower priority MX records which may not be protected by spam/virus filtering.

Ensure that your mail server accepts inbound messages from the GFI MailSecurity Data Center. If your gateway server blocks inbound messages that use your domains in the **From:** field. Add an exception to this rule to accept messages originating from GFI MailSecurity.

For example, if your domain is `mydomain.com` and you block all inbound mail with an SMTP address of `*@mydomain.com` as spam, modify this policy to exclude the GFI MailSecurity Data Center.

Firewall configuration

Configure your firewall to accept inbound SMTP traffic (port 25) from GFI MailSecurity. Also, configure GFI MailSecurity IP addresses to be a trusted forwarder, but not safe-listed.

MX Records for EU Data Center:

- eu01.gfimailsecurity.com - 52.58.249.172
- eu02.gfimailsecurity.com - 52.208.1.91

MX Records for US Data Center:

- us01.gfimailsecurity.com - 35.153.155.238
- us02.gfimailsecurity.com - 35.173.150.16
- us03.gfimailsecurity.com - 54.236.224.49

1.2 Logging into GFI MailSecurity

Log in to GFI MailSecurity to manage, configure and use the system.

When the user information is available in the Data Center and user permissions have been configured, all other organization users can also log in to GFI MailSecurity.

Users can authenticate using their Windows credentials if the organization uses Windows Authentication and one or more instances of Windows Authentication Manager are installed and functional.

If using Custom authentication, run the Welcome process to ask users to set a GFI MailSecurity password.

1.2.1 Logging in as Administrators

There are two types of administrators in GFI MailSecurity that can access the Admin Console:

- **Domain Group Administrators**: Organization users that are assigned privileges to access multiple domains simultaneously.

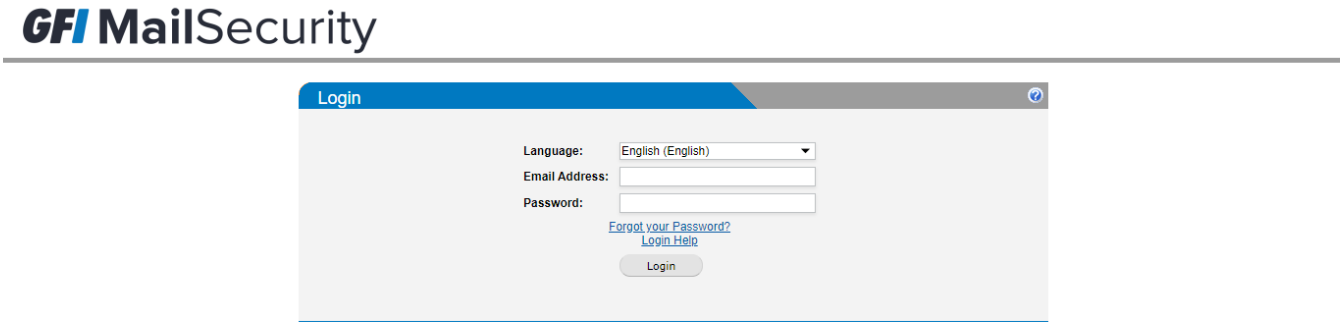
- **Domain Administrator**: Organization users that are assigned administrative privilege to access only one domain.

From your favorite web browser, go to https://eu.gfimailsecurity.com (For EU Datacenter) or https://us.gfimailsecurity.com (For US Datacenter) and key in your username and password. When logged in, the main page shows an overview of email statistics and detected spam/malware. Use the top menu bar to navigate to any screen in the system.

1.2.2 Logging in as a user

From your favorite web browser, go to https://eu.gfimailsecurity.com (For EU Datacenter) or https://us.gfimailsecurity.com (For US Datacenter) and key in your username and password.

For more information refer to the GFI MailSecurity user help from http://go.gfi.com/?pageid=mailsecurity_user_help



Language: English (English)

Screenshot 1: GFI MailSecurity user home page

1.3 Signing up to GFI MailSecurity

Create a GFI MailSecurity account to start using the software. Sign up to the service following the steps in this topic:

1. Go to https://eu.gfimailsecurity.com (For EU Datacenter) and https://us.gfimailsecurity.com (For US Datacenter) and fill in your account information. Note that in this step you are creating your Administrator Account that is used to login to GFI MailSecurity. Also you must select your Datacenter location - EU / US.

2. Click **Submit**.

An email is sent to your account with system set up instructions. The email content based on the Datacenter location includes:

- How to gain access to the GFI MailSecurity Console
- Link to Help/Manuals for further information
- How to set up MX Records
- Other General information

2 Managing GFI MailSecurity

The GFI MailSecurity service protects your inbound email from viruses, filters out spam and provides mail monitoring features.

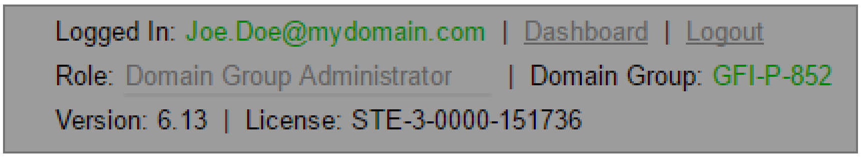
This section guides you through the process of configuring the Security service of GFI MailSecurity.

You can access the configuration console and log in to GFI MailSecurity using your administrator account provided.

When login is completed, the service provides three roles. Choose the role depending on the feature to configure or monitor:

Role	Description
User	Options related to your user's mailbox: » Configure your user's personal Blacklist & Whitelist » Manage the list of quarantined emails sent to your address. » Personal quarantine report settings
Domain Administrator	Manages a distinct domain/organization email security settings: » Configure Blacklist & Whitelist entries for the organization » Manage organization's quarantine » Generate mail usage reports at organization-level
Domain Group Administrator	Manage a set of distinct domains/organizations email security options: » Configure mail filtering options for protected domains » Configure Blacklist & Whitelist entries for the organization » Custom mail filtering policies for individual users » Manage organization's quarantine » Generate mail usage reports at organization-level

To switch the role, click the **Role** field in the top right corner and select the new role.



Logged In: Joe.Doe@mydomain.com | Dashboard | Logout
Role: Domain Group Administrator | Domain Group: GFI-P-852
Version: 6.13 | License: STE-3-0000-151736

Screenshot 2: The top-right corner section where to change role and domain

Topics in this section:

2.1 Security Dashboard

The Security Dashboard provides a summary and statistics of the service status.

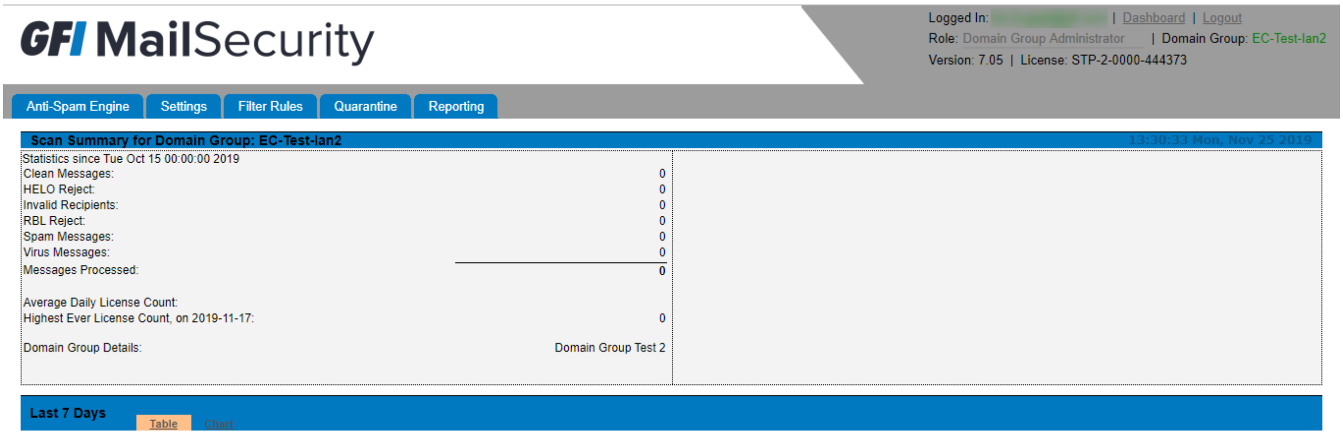
To access the Security Dashboard:

1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Click **Dashboard** from the top-right corner.



Logged In: [redacted] | Dashboard | Logout
Role: Domain Group Administrator | Domain Group: EC-Test-lan2
Version: 7.05 | License: STP-2-0000-444373

Scan Summary for Domain Group: EC-Test-lan2 13:30:33 Mon, Nov 25 2019

Statistics since Tue Oct 15 00:00:00 2019

Clean Messages:	0
HELO Reject:	0
Invalid Recipients:	0
RBL Reject:	0
Spam Messages:	0
Virus Messages:	0
Messages Processed:	0
Average Daily License Count:	
Highest Ever License Count, on 2019-11-17:	0
Domain Group Details:	Domain Group Test 2

Last 7 Days

Screenshot 3: The Security Dashboard

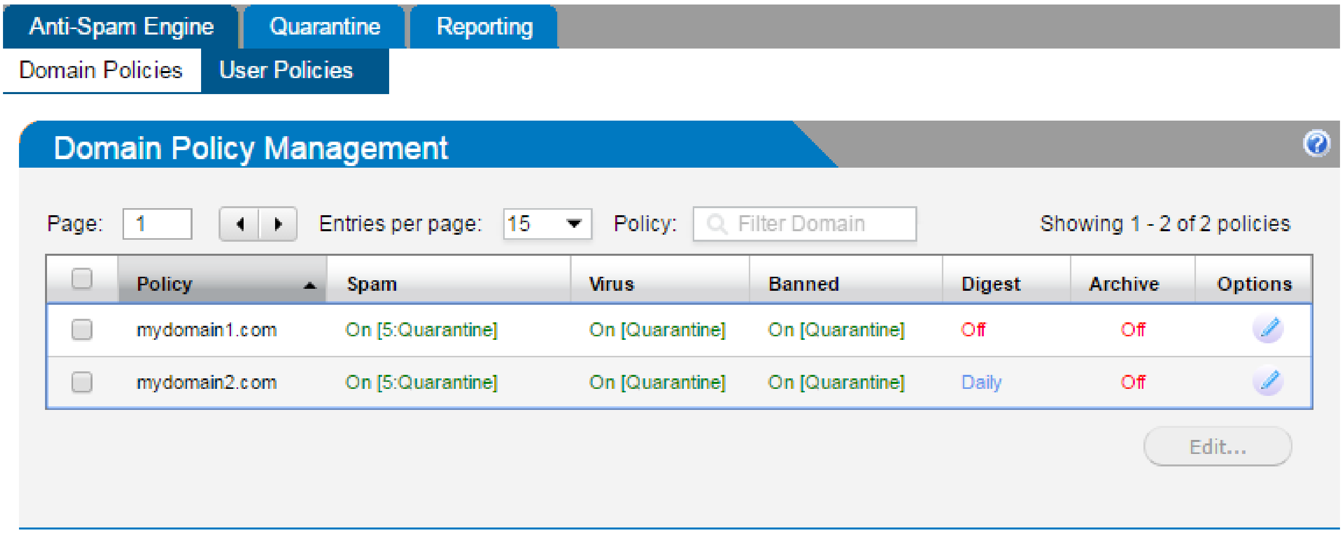
The **Scan Summary** section shows various metrics related to processed and blocked emails.

The **Last 7 days** section shows trends and counts of blocked emails during the previous seven days. Choose tab:

- **Table**: Counts of emails processed and blocked per day.
- **Chart**: A line chart of emails processed and blocked during the last seven days.

2.2 Domain Policies

Use the Security Domains Policy settings to apply anti-virus, anti-spam, and other filtering mechanisms on emails processed on a per-domain basis.



Domain Policy Management

Page: 1 Entries per page: 15 Policy: Showing 1 - 2 of 2 policies

□	Policy	Spam	Virus	Banned	Digest	Archive	Options
□	mydomain1.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off	Off	✎
□	mydomain2.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Daily	Off	✎

Screenshot 4: Domain Policies page

To access the Domain Policies screen:

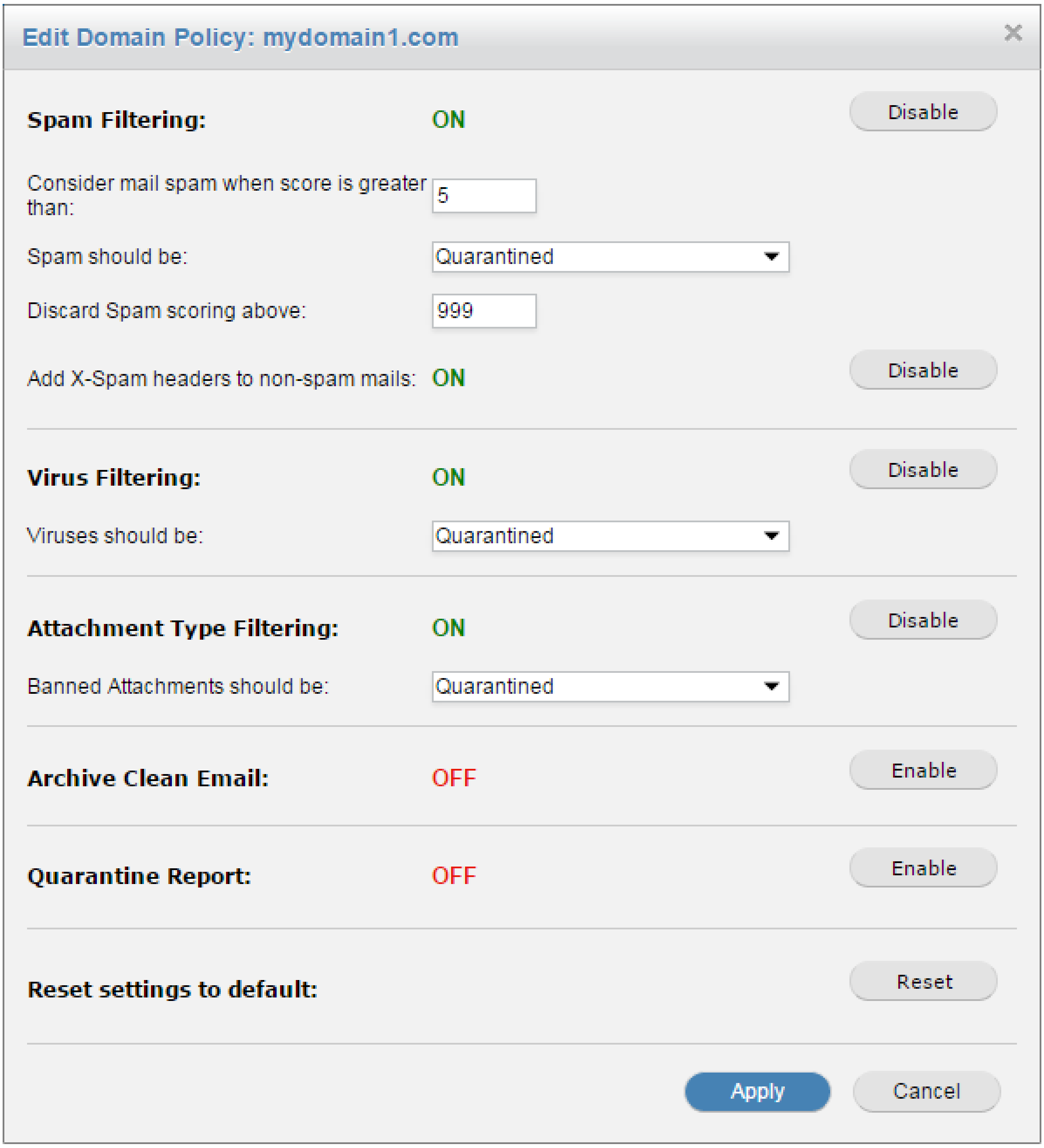
1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Navigate to **Anti-Spam Engine > Domains Policies**.

5. Choose a domain and click the ✎ icon to configure the domain's filtering options. These domain settings are inherited by all users in those domains.



Edit Domain Policy: mydomain1.com

Spam Filtering: ON

Consider mail spam when score is greater than: 5

Spam should be: Quarantined

Discard Spam scoring above: 999

Add X-Spam headers to non-spam mails: ON

Virus Filtering: ON

Viruses should be: Quarantined

Attachment Type Filtering: ON

Banned Attachments should be: Quarantined

Archive Clean Email: OFF

Quarantine Report: OFF

Reset settings to default:

Screenshot 5: Edit Domain Policy dialog

Configure the following options:

Option	Description	Default value
Spam Filtering	Specifies whether spam filtering is enabled for the selected domain. Toggle **Enable** / **Disable** to switch this option on or off.	**ON**
Consider mail spam when score is greater than	When scanning messages for spam, GFI MailSecurity applies various checks to determine an overall spam score for each message. Emails scoring above this threshold are considered as spam. Emails scoring below the threshold is considered legitimate and passed onto the recipient(s) If you find this setting too aggressive or not aggressive enough, then you can change the threshold.	**5**
Spam should be	Action to perform when a message is classified as spam: » **Quarantined**: The message is moved to the GFI MailSecurity Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » **Passed (Tagged):** Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » **Rejected**: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered.	**Quarantined**
Discard Spam scoring above	Messages scoring above the specified score is automatically discarded. This option is only available when the action is set to **Quarantined**.	**999** (no messages is discarded)
Spam Modifies Subject	Enable this option to prepend text to the Subject header, indicating that the message has been identified as spam. Specify an appropriate **Spam Subject Tag** to be added to the subject. This option is only available when the action is set to **Passed (Tagged)**.	**OFF**
Add X-Spam headers to non-spam mails	Specifies if additional headers are added to inbound messages, indicating the result of the spam analysis. The headers added are: » **X-Spam-Status**: This shows if the message exceeded the spam threshold and the score that it achieved. It also lists what rules were fired by the anti-spam engine. » **X-Spam-Score**: Lists the spam score achieved. Toggle **Enable** / **Disable** to switch this option on or off.	**ON**
Virus Filtering	Specifies whether virus filtering is enabled for the selected domain. Toggle **Enable** / **Disable** to switch this option on or off.	**ON**
Viruses should be	The action to perform when a message is identified as containing a virus. Refer to the actions documented in the anti-spam section above.	**Quarantined**
Attachment Type Filtering	Specifies whether the default GFI MailSecurity message attachment policy is applied to messages received by recipients in the selected domain. Toggle **Enable** / **Disable** to switch this option on or off. The blocked attachment types are: .vbs, .scr, .pif, .js, flv, .exe, .dll, .com, .cmd, and .bat.	**ON**
Banned Attachments should be	The action to perform when a message is blocked by Attachment Type Filtering: » **Quarantined**: The message is moved to the GFI MailSecurity Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » **Passed (Tagged):** Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » **Rejected**: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered.	**Quarantined**

Option	Description	Default value
Archive Clean Email	Enable this setting to store all clean messages received by this domain in the history. (Go to **Reporting** > **History** to view clean emails.) Toggle **Enable** / **Disable** to switch this option on or off.	**OFF**
Quarantine Report	This field specifies whether quarantine reports should be generated for recipients in this domain. A quarantine report is generated for each recipient who has at least one email quarantined. Toggle **Enable** / **Disable** to switch this option on or off.	**OFF**
Language	If enabling quarantine reports, select the default report language. Recipients may change the language of their report by logging into GFI MailSecurity and changing their preferences.	**English**
Email report every	If enabling quarantine reports, select the frequency of the reports. Reports may be generated every day, every weekday (Monday to Friday), every Friday, or every month. Recipients may change the frequency of their reports by logging into GFI MailSecurity and changing their preferences.	**Day**
Report contains	If enabling quarantine reports, choose the items to show in the report. Recipients may change this option of their report by logging into GFI MailSecurity and changing their preferences. The report may include: » All quarantined items » New items since last report only » All quarantined msgs (except viruses) » New items since last report (except viruses)	**New items since last report only**
Exclude spam mails scoring above	Usually, users are only interested in messages that fall just above the spam threshold to look for false positives. Spam messages scoring above a certain threshold can be unequivocally deemed as spam. If users get a significant amount of spam, then to keep the report size manageable you can exclude spam messages above, for example 30. This setting is set to 999 by default, meaning that no messages is excluded (as a message cannot score that high).	**999** (no messages is excluded)
Reset settings to default	Reset the policy to default values.	

6. Click **Apply** to save settings.

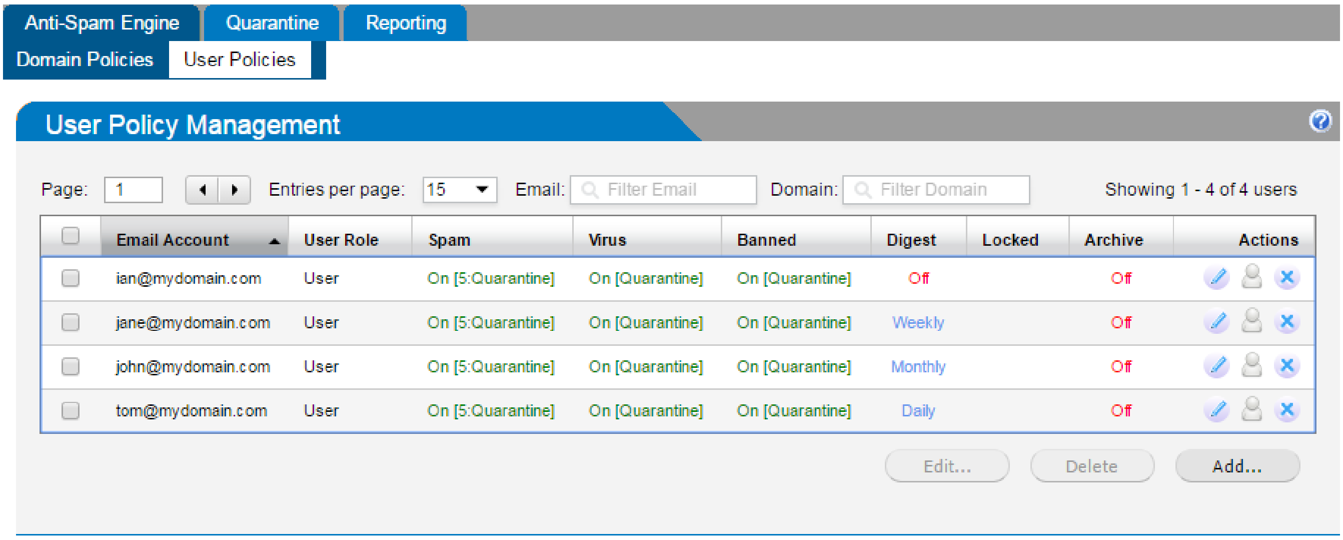
2.2.1 User Policies

By default, each recipient email address inherits the policy as set for that domain. GFI MailSecurity enables administrators to apply custom email filtering policies to individual users, that override the domain policies. User policies have a higher priority than domain policies. When an email is received for a user who does not have a user policy, then GFI MailSecurity uses the domain policy. If a user policy associated with the email address exists, then GFI MailSecurity uses the user policy.

GFI MailSecurity also enables end-users to customize their quarantine report preferences. The User policies screen shows these customizations, enabling administrators to track the changes applied.

User policies are created when:

- A user logs into the GFI MailSecurity UI the first time.
- A user whitelists a sender from their quarantine report.
- An *existing* user (who has already sent or received email) requests their password using the **Forgot Password** link on the GFI MailSecurity login page.
- An administrator manually creates a user policy rule as documented below.



Page: 1 Entries per page: 15 Email: Filter Email Domain: Filter Domain Showing 1 - 4 of 4 users

□	Email Account	User Role	Spam	Virus	Banned	Digest	Locked	Archive	Actions
□	ian@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off		Off	✎ 👤 ✕
□	jane@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Weekly		Off	✎ 👤 ✕
□	john@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Monthly		Off	✎ 👤 ✕
□	tom@mydomain.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Daily		Off	✎ 👤 ✕

Screenshot 6: User Policies page

To access the User Policies screen:

1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Navigate to **Anti-Spam Engine > User Policies**.

5. To create new user policies click **Add…** . To edit an existing user policy, click the ✎ icon in the options column.

6. Configure the following options:

Option	Description
Email Addresses	Specify one or more email addresses to create user policies for. Specify multiple email addresses in separate lines.
User Role	Choose **User**.
Spam Filtering	Specifies whether spam filtering is enabled for the selected user. Toggle **Enable** / **Disable** to switch this option on or off.
Consider mail spam when score is greater than	This is the anti-spam engine scoring threshold above which mail is considered to be spam.
Spam should be	Action to perform when a message is classified as spam: » **Quarantined**: The message is moved to the GFI MailSecurity Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » **Passed (Tagged):** Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » **Rejected**: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered.
Discard Spam scoring above	Messages scoring above the specified score is automatically discarded. This option is only available when the action is set to **Quarantined**.
Spam Modifies Subject	Enable this option to prepend text to the Subject header, indicating that the message has been identified as spam. Specify an appropriate **Spam Subject Tag** to be added to the subject. This option is only available when the action is set to **Passed (Tagged)**.

Option	Description
Add X-Spam headers to non-spam mails	Specifies if additional headers are added to inbound messages, indicating the result of the spam analysis. The headers added are: » **X-Spam-Status**: This shows if the message exceeded the spam threshold and the score that it achieved. It also lists what rules were fired by the anti-spam engine. » **X-Spam-Score**: Lists the spam score achieved. Toggle **Enable** / **Disable** to switch this option on or off.
Virus Filtering	Specifies whether virus filtering is enabled for the selected domain. Toggle **Enable** / **Disable** to switch this option on or off.
Viruses should be	The action to perform when a message is identified as containing a virus. Refer to the actions documented in the anti-spam section above.
Attachment Type Filtering	Specifies whether the default GFI MailSecurity message attachment policy is applied to messages received by this recipient. Toggle **Enable** / **Disable** to switch this option on or off. The default file types blocked are .bat, .cmd, .com, .dll, .exe, .flv, .js, .piv, .scr and .vbs.
Banned Attachments should be	The action to perform when a message is blocked by Attachment Type Filtering. The options are: » **Quarantined**: The message is moved to the GFI MailSecurity Quarantine. It appears in the recipient's Quarantine Report and may be later released from the quarantine if it is deemed by the user to be a false positive. » **Passed (Tagged):** Spam emails will be passed onto the end recipients, but headers are added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients mail client. » **Rejected**: The message will be rejected. The message are dropped before they are received by the mail server. Those messages cannot be recovered.
Archive Clean Email	Enable this setting to store all clean messages received by this domain in the history. (Go to **Reporting > History** to view clean emails.) Toggle **Enable** / **Disable** to switch this option on or off.
Lock Policy	When enabled, any changes applied to the parent domain policy does not affect the user policy. For example, if the domain policy for `example.com` changes the spam score to 1, any user policy under `example.com` also sees that change appears on their policy unless it has been locked.
Quarantine Report	This field specifies whether quarantine reports should be generated for recipients in this domain. A quarantine report is generated for each recipient who has at least one email quarantined. Toggle **Enable** / **Disable** to switch this option on or off.
Language	If enabling quarantine reports, select the default report language.
Email report every	If enabling quarantine reports, select the frequency of the reports. Reports may be generated every day, every weekday (Monday to Friday), every Friday, or every month.
Report contains	If enabling quarantine reports, choose the items to show in the report. The report may include: » All quarantined items » New items since last report only » All quarantined msgs (except viruses) » New items since last report (except viruses)
Exclude spam mails scoring above	If enabling quarantine reports, users are usually only interested in messages that fall just above the spam threshold to look for false positives. Spam messages scoring above a certain threshold can be unequivocally deemed as spam. If users get a significant amount of spam, then to keep the report size manageable you can exclude spam messages above, for example 30. This setting is set to 999 by default, meaning that no messages are excluded (as a message cannot score that high).

7. Click **Add** to save settings.

To impersonate a user, click on the 👤 icon in the options column. This automatically log you into that user interface with the same permissions as they would have.

2.3 Domain Whitelist & Blacklist

The Whitelist contains a list of sender email addresses and domains. Emails received from whitelisted addresses, are always classified as not spam, even if the message is detected as spam. Note however that GFI MailSecurity still scans emails received from whitelisted senders for viruses and malware.

On the contrary, emails received from email addresses or domains added to the Blacklist are always blocked and classified as spam, even if the message is not detected as spam by the scanning engine. Add to the Blacklist the senders from which you never want to receive emails.

Blacklist & Whitelist can be configured at domain level or at user level. GFI MailSecurity administrators can manage domain lists, applicable to emails received by the organization. End-users can manage their own lists for emails received by them only.

This topic describes how to configure domain-level Whitelist & Blacklist. For information on how end-users can manage User Blacklist/Whitelist, refer to User Whitelist & Blacklist.

To access the Domain Whitelist & Blacklist filter rules:

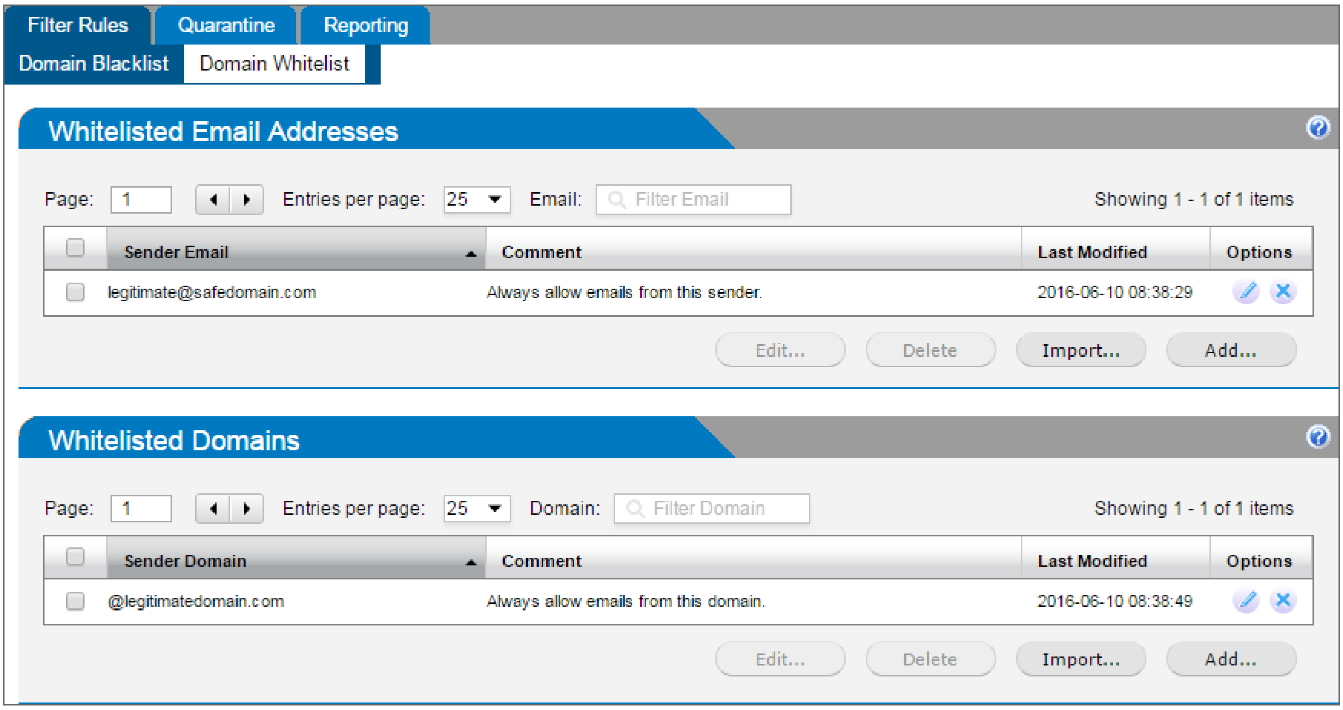
1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Navigate to the **Filter Rules** tab.

5. Select the list to access: **Domain Whitelist** or **Domain Blacklist**.



Whitelisted Email Addresses

Page: 1 | Entries per page: 25 | Email: Filter Email | Showing 1 - 1 of 1 items

□	Sender Email ▲	Comment	Last Modified	Options
□	legitimate@safedomain.com	Always allow emails from this sender.	2016-06-10 08:38:29	✎ ✕

Whitelisted Domains

Page: 1 | Entries per page: 25 | Domain: Filter Domain | Showing 1 - 1 of 1 items

□	Sender Domain ▲	Comment	Last Modified	Options
□	@legitimatedomain.com	Always allow emails from this domain.	2016-06-10 08:38:49	✎ ✕

Screenshot 7: The Domain Whitelist screen

Adding entries manually

1. Click **Add** in the **Email Addresses** or **Domain sections**.

2. Key in the domain or email address to add:

- Email Address must be entered in the form *user@example.com*.
- Domain entries must be in the form *example.com*.

3. (Optional) Add a comment. It may be helpful to remember why the item was added on that list.

4. Click **Save**.

Importing a list

1. Create a text file containing all the entries to whitelist or blacklist. Write one entry per line:

- Email addresses must be in the form *user@example.com*.
- Domain entries must be in the form *@example.com*.
- The text file may contain a mixed list of both email addresses and domains.

2. Click **Import...** in the **Email Addresses** or **Domain** sections.

3. Select the file to be imported and click **Open**.

Editing entries

1. Select the entry to modify and click **Edit...**.

2. Make the changes and click **Save**.

Deleting entries

1. Access the list you want to edit.

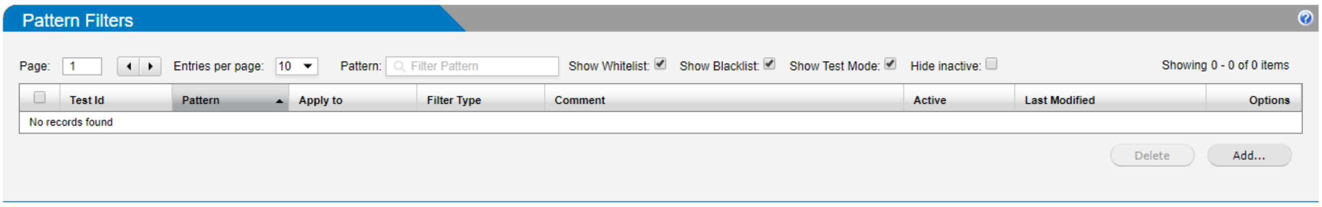
2. Select the entry and click **Delete**.

> **NOTES**
>
> » A sender may not be added to both the Whitelist and the Blacklist at the same time.
>
> » Whitelist and Blacklist entries specified by end-users at User level, overrule the domain level settings.

2.4 Pattern Filtering

Pattern filtering provides you with the functionality to add regular expression to filter out emails of desired pattern.

1. Login to GFI MailSecurity as Domain Group Administrator and navigate to **Filter Rules > Pattern Filtering**.



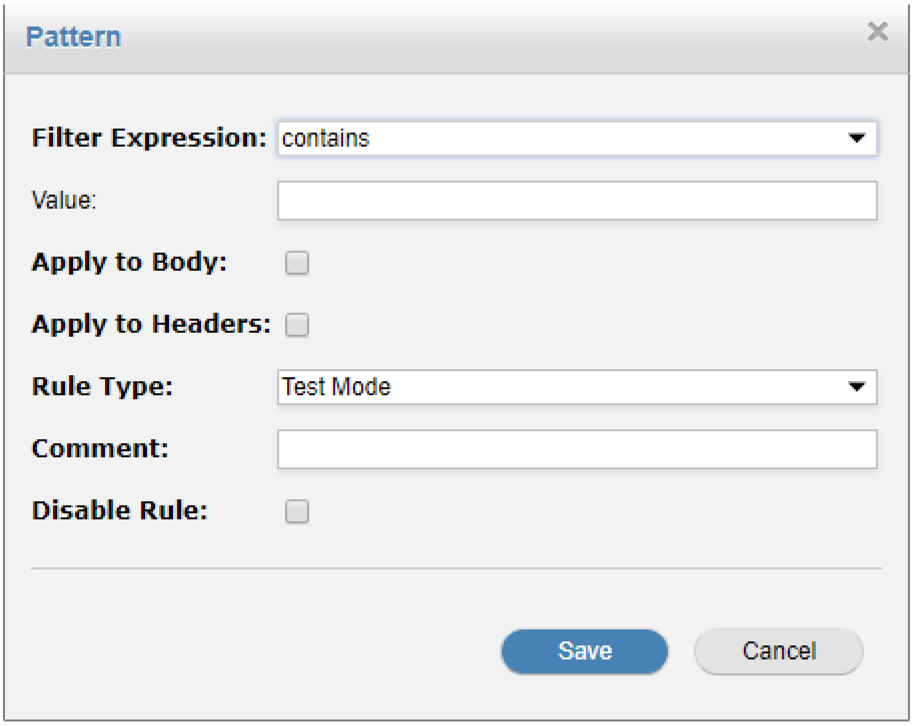
Pattern Filters

Page: 1 Entries per page: 10 Pattern: Filter Pattern Show Whitelist: ☑ Show Blacklist: ☑ Show Test Mode: ☑ Hide inactive: □ Showing 0 - 0 of 0 items

□	Test Id	Pattern	Apply to	Filter Type	Comment	Active	Last Modified	Options
No records found								

Screenshot 8: Pattern Filters page

2. On the **Pattern Filters** page, click **Add**. Set the fields on **Pattern** pop-up.



Pattern

Filter Expression: contains

Value:

Apply to Body: □

Apply to Headers: □

Rule Type: Test Mode

Comment:

Disable Rule: □

Screenshot 9: Set the fields in pattern pop-up

The following table describes the fields to be entered on **Pattern** pop-up:

Pattern pop-up fields	Description
Filter Expression	The filtering task that needs to be performed for the **Value**.
Value	The filtering value.
Apply to Body	If the filter needs to be applied on the email body, check this checkbox.
Apply to Headers	If the filter needs to be applied on the email subject/header, check this checkbox.
Rule Type	The type of filtering applied.
Comment	Any optional comment can be given.
Disable Rule	Check this to disable this pattern filter.

2.5 Anti-spoofing

Email spoofing is the creating and sending of email with a forged sender address to intentionally mislead the recipient about its origin. This is a phishing technique often used to get a user to click a link and share their credentials or reply with sensitive information.

GFI MailSecurity offers functionality to help prevent email spoofing. There are two types of *From* addresses in an email, both of which can be spoofed:

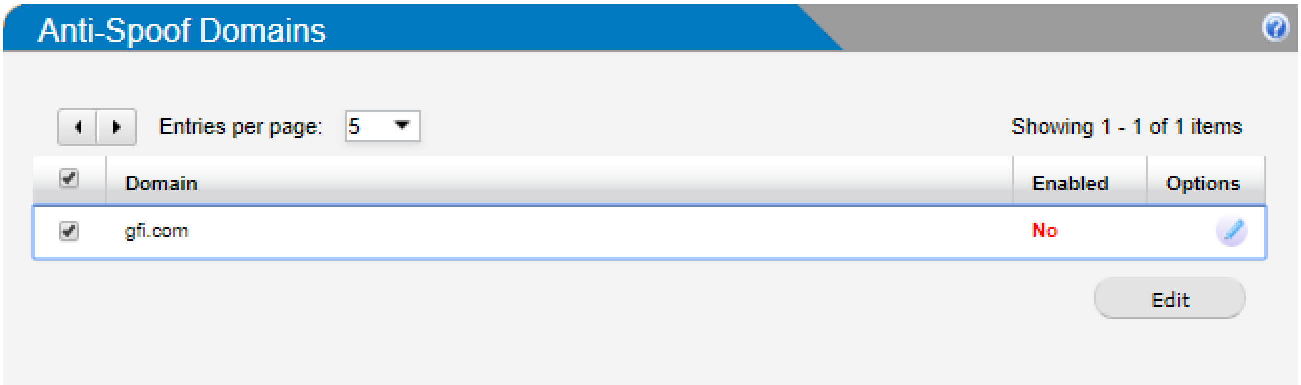
» **Envelope From:** This is sent during the MAIL FROM command. Envelope From is straight forward to protect and is not commonly used for legitimate mail to spoof. This is generally protected using SPF (Sender Policy Framework).

» **Mime-Encoded From:** This is sent during the DATA command. It is not protected by any SMTP mechanism and as such is open to spoofing.

2.5.1 Anti-Spoofing Settings

1. Login as Domain Group Administrator.

2. Go to **Filter Rules > Anti-Spoofing Settings**. The **Anti-Spoof Domains** window is displayed showing a list of your domains:



Anti-Spoof Domains

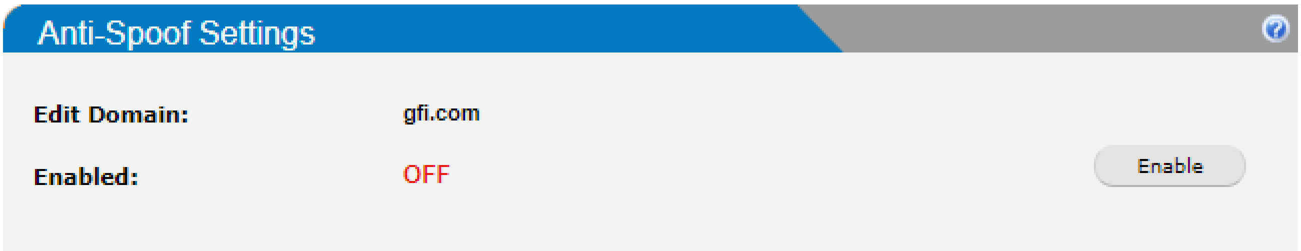
Entries per page: 5

Showing 1 - 1 of 1 items

☑	Domain	Enabled	Options
☑	gfi.com	No	✎

Screenshot 10: Check the box and click edit to display anti-spoofing settings window

3. Check the box ☑ to the left of the domain you want to edit and click ✎ (edit). (Check multiple boxes to edit multiple domains at once). The **Anti-Spoof Settings** window displays for your selected domain(s).



Anti-Spoof Settings

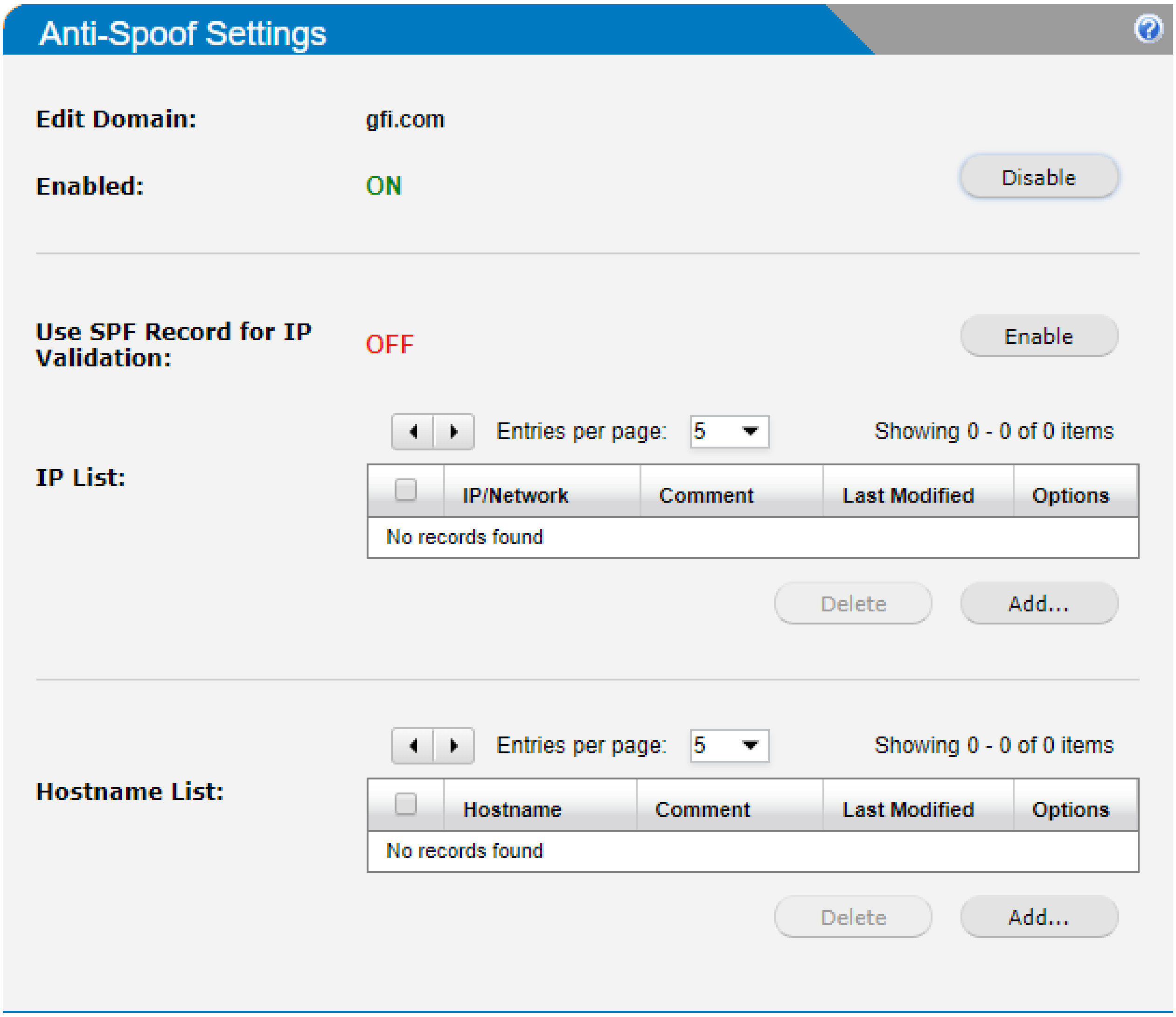
Edit Domain: gfi.com

Enabled: OFF

Screenshot 11: Click enable to switch ON anti-spoofing

Follow the steps below to enable and modify your anti-spoof settings:

4. Click **Enable** on the A**nti-Spoof Settings** panel. The **Anti-Spoof Settings** panel expands.



Anti-Spoof Settings

Edit Domain:	gfi.com	
Enabled:	ON	Disable
Use SPF Record for IP Validation:	OFF	Enable

IP List:

◀ ▶ Entries per page: 5 ▾ Showing 0 - 0 of 0 items

□	IP/Network	Comment	Last Modified	Options
No records found				

Delete Add...

Hostname List:

◀ ▶ Entries per page: 5 ▾ Showing 0 - 0 of 0 items

□	Hostname	Comment	Last Modified	Options
No records found				

Delete Add...

Screenshot 12: Set the fields on this form as per instructions given below

5. Enable **Use SPF Record for IP Validation** (disabled, by default) to use your SPF record to determine if a sender is valid. Instead you can add a list of CIDR notation ranges in the **IP List** that are allowed to send email using your domain.

6. Click **Add...** to add an entry. Click ✎ (edit) to edit an IP, or ✖ (delete) to delete an entry from the list.

Using **IP List** is more secure than using **Hostname List**. Generally, try to use **Hostname List** only if you are not using SPF and a service you are using has too many IPs to list.

7. On **Hostname List** section click **Add...** to enter hostnames that are allowed to send email using your domain, e.g. "www.example.com".

> **Note**
>
> If using regular expression, the more generic the expression, the easier it is to bypass spoofing.

8. If you are editing multiple domains, click **Save** to save changes to all domains and return to the **Anti-Spoof Domains** window.

Important

If you do not click **Save** when editing multiple domains, only changes to the first domain checked is saved.

2.6 Quarantine

The GFI MailSecurity Quarantine provides a central store where all emails detected as spam or malware are retained. This ensures that users do not receive unwanted messages in their mailbox and processing on the mail server is reduced.

Administrators and end-users can review quarantined emails by accessing the quarantine interface from a web browser. GFI MailSecurity can also send regular quarantine email reports to end-users to review their blocked emails.

This chapter describes the quarantine management system, and how the administrator manages the organization's quarantined messages. End-users can also review their personal quarantine.

Note that emails get quarantined only when GFI MailSecurity is configured to quarantine blocked emails. The action taken can be customized by the Administrator from the Domain Policies and from User Policies

Using the quarantine

The Quarantine is accessible by logging in to GFI MailSecurity. From the Quarantine, administrators can review blocked emails and apply various actions, for example, release a false positive, whitelist the sender or permanently delete emails.

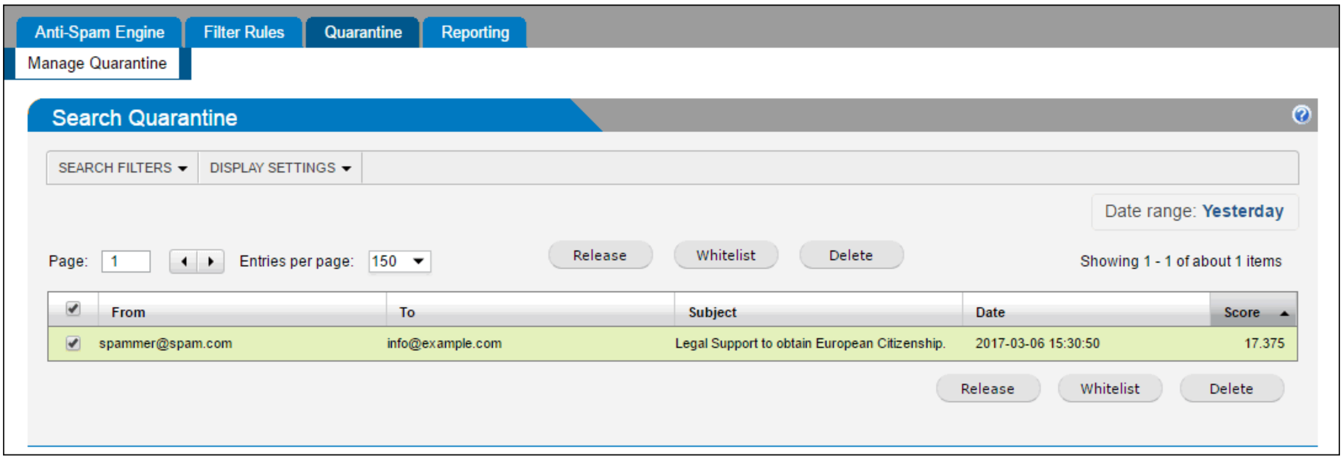
To access the organization's Quarantine:

1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Go to **Quarantine > Manage Quarantine**.



Date range: Yesterday

Page: 1 Entries per page: 150

Showing 1 - 1 of about 1 items

☑	From	To	Subject	Date	Score
☑	spammer@spam.com	info@example.com	Legal Support to obtain European Citizenship.	2017-03-06 15:30:50	17.375

Screenshot 13: Manage Quarantine page

The **Manage Quarantine** page shows the emails in quarantine.

Use the **Search Filters** tab to filter through the list of quarantined emails on a number of different criteria including message type, email address, score, subject and message flow direction.

The following actions may be performed on messages in the Quarantine:

Action	Description
View Message	To safely view a message that is in the quarantine click the From, To, or Subject of a particular quarantined message from the list. This opens the message in a separate window. Note that the images are blocked from this preview to prevent possible inappropriate content. If a message is subsequently released and delivered, then the original images are present.
Release Message	Messages in the quarantine that are misidentified as spam (False positives) can be released for delivery to their intended recipients. Click **Release** to perform this action.
Delete Message	Users can choose to permanently delete messages one at a time, or in bulk by checking the check boxes of messages to delete. Note that if a message is deleted from the quarantine then that message does not appear in the quarantine report. NOTE Deleted messages are permanently purged and are not recoverable.
Whitelist Sender	Adds the sender of the selected message(s) to the whitelist so that all future emails from this sender bypass the GFI MailSecurity anti-spam engine. Selecting this option also automatically releases the message from the quarantine. Note that the sender email address that is added to the Whitelist is the envelope email address. This is sometimes different from the address that appears in the From header of the message. Check **Reporting > History** to see the envelope sender email address.

> NOTE
> Quarantined items are automatically deleted from the quarantine store after 21 days. Deleted items are not recoverable.

Enabling Quarantine reports for the users

Administrators can enable quarantine reports to be sent to users on a daily basis. A quarantine report is generated for each recipient who has at least one email quarantined.

The report contains a list of items in quarantine and a link for the users to access their personal quarantine.

To enable quarantine reports for the users:

1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Navigate to **Anti-Spam Engine > Domains Policies**.

5. Choose a domain and click the ✎ icon to configure the domain's filtering options.

6. On the **Quarantine Report** option click **Enable**.

2.7 GFI MailSecurity Reports

GFI MailSecurity enables administrators and end-users to create reports based on emails processed and blocked by the service.

The GFI MailSecurity Administrator can access and generate reports for the whole organization or specific domains. End-users can generate reports for emails addressed to them.

To access the GFI MailSecurity Reports:

1. Login to GFI MailSecurity.

2. Key in your Administrator account credentials in the login screen.

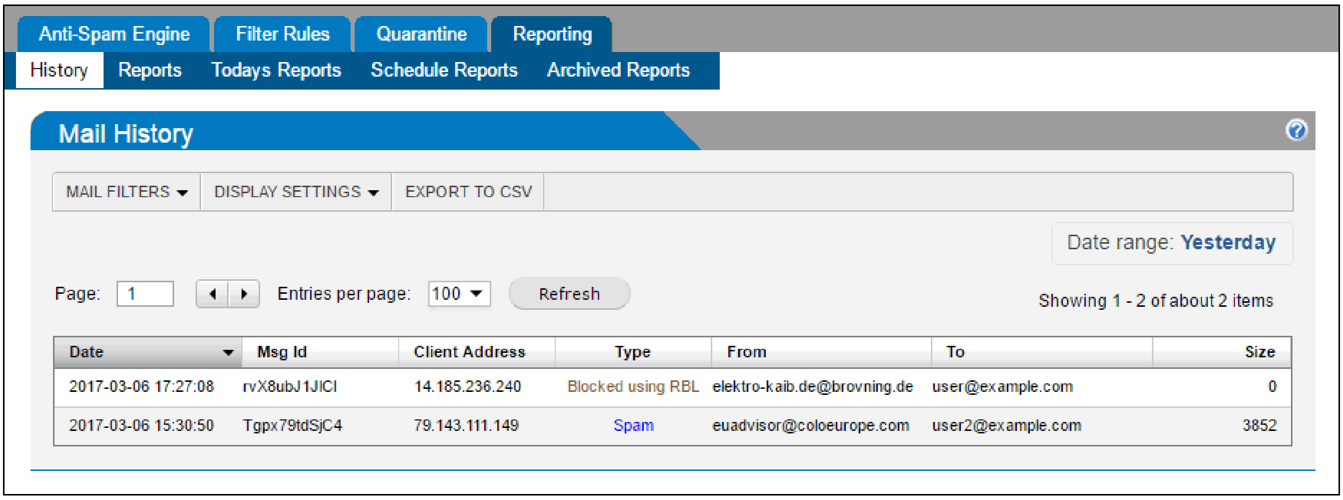
3. Choose the **Domain Group Administrator** role from the top-right corner **Role** field.

4. Go to the **Reporting** tab and choose the required action:

- Review mail transactions (history)
- Generate a report
- Scheduled reports
- Archived reports

Activity Log & History

The **Reporting > History** page enables you to monitor all processed emails and review all mail transactions that have passed through GFI MailSecurity.



Date range: Yesterday

Page: 1 Entries per page: 100

Showing 1 - 2 of about 2 items

Date	Msg Id	Client Address	Type	From	To	Size
2017-03-06 17:27:08	rvX8ubJ1JICI	14.185.236.240	Blocked using RBL	elektro-kaib.de@brovning.de	user@example.com	0
2017-03-06 15:30:50	Tgpx79tdSjC4	79.143.111.149	Spam	euadvisor@coloeurope.com	user2@example.com	3852

Screenshot 14: History page

The Mail History table

The **Mail History** table shows a row for each processed email and its attributes.

By default, the table does not show all the columns documented here. Use the **Display Settings** tab to add more columns as required. For more information, refer to Display Settings (page 23).

The **Export to CSV** link allows you to download all transactions for the given search criteria to a Microsoft Excel spreadsheet.

Click the **Refresh** link to refresh the history view. Since the entire history is not shown on one page, use the links at the bottom of the page to jump to other pages.

The following table describes each of the columns that are displayed in the Mail History table.

Column	Description
Date	Specifies the time and date that the message was processed.
Msg Id	The internal message identifier that GFI MailSecurity has assigned to the message. Click the Message ID to view extended details in a pop-up window.

Column	Description
Client Address	The source IP address of the host that sent the message to GFI MailSecurity. Note that if all your mail is relayed through an upstream mail relay before arriving at GFI MailSecurity, then this column only contains the address of the upstream mail relay.
Type	The message type as classified by GFI MailSecurity during scanning.
From	The envelope sender address.
To	The envelope recipient address.
Size	The size of the message
Subject	If enabled in **Display Settings**, this column shows the subject header of the received message.
Flow	If enabled in **Display Settings**, this column shows the direction of the message » Inbound » Outbound » Internal
TLS	If enabled in **Display Settings**, this column indicates if TLS was applied to the message. The value may be one of the following: » Received over encrypted TLS channel » Sent out over encrypted TLS channel » Received and sent out over encrypted TLS channel
Delivery	If enabled in **Display Settings**, this column indicates the delivery status of the message. The delivery status may be one of the following: » Any » Sent » Deferred » Bounced » Expired Note that rejected or quarantined emails have no delivery status as they have not been delivered.
Delivery Response	If enabled in **Display Settings**, this column shows the SMTP response from the destination server. This can be useful to indicate, for instance, why a remote server rejected a message.

Mail Filters

Various filters can be applied to narrow the number of logs in the Mail History table. The following table describes the various mail filters that can be employed. Multiple filters can be applied together to narrow the search further.

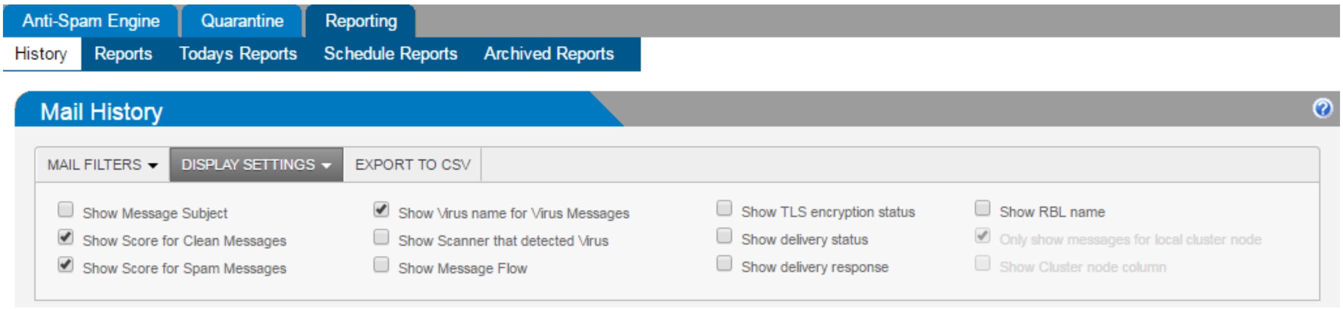
Filter	Description
Message Flow	Indicates the message flow direction: Inbound or Outbound
Message Type	Filter messages based on how they were classified by GFI MailSecurity. Select **Choose types** and select the scan result types to show.
Recipient email address	Filter results using the recipient email address. Use * as a wildcard character. For example, to filter all messages sent to domain **example.com** enter `*@example.com`
Sender email address	Filter results using the sender email address. Use * as a wildcard character. For example, to filter all messages from the **.co.uk** domain enter `*@*.co.uk`

Filter	Description
Source IP address	Filter results based on the connecting client IP address.
Security ID	The internal GFI MailSecurity SecurityID which is assigned to every message.
Score	The GFI MailSecurity spam score assigned to a message. Note that messages which are not analyzed for spam has no score (e.g. rejected messages)
Delivery Status	The delivery status may be one of the following: » Any » Sent » Deferred » Bounced » Expired Note that rejected or quarantined emails have no delivery status as they have not been delivered.
Subject	Filter based on message subject. Use * for wildcards.

Press the **Apply** button after selecting your search filters to refresh the display.

Display Settings

The options in the **Display Settings** tab allow you to control what columns and information are displayed in the mail history table.



□ Show Message Subject
☑ Show Score for Clean Messages
☑ Show Score for Spam Messages
☑ Show Virus name for Virus Messages
□ Show Scanner that detected Virus
□ Show Message Flow
□ Show TLS encryption status
□ Show delivery status
□ Show delivery response
□ Show RBL name
☑ Only show messages for local cluster node
□ Show Cluster node column

Screenshot 15: Configuring History Display settings

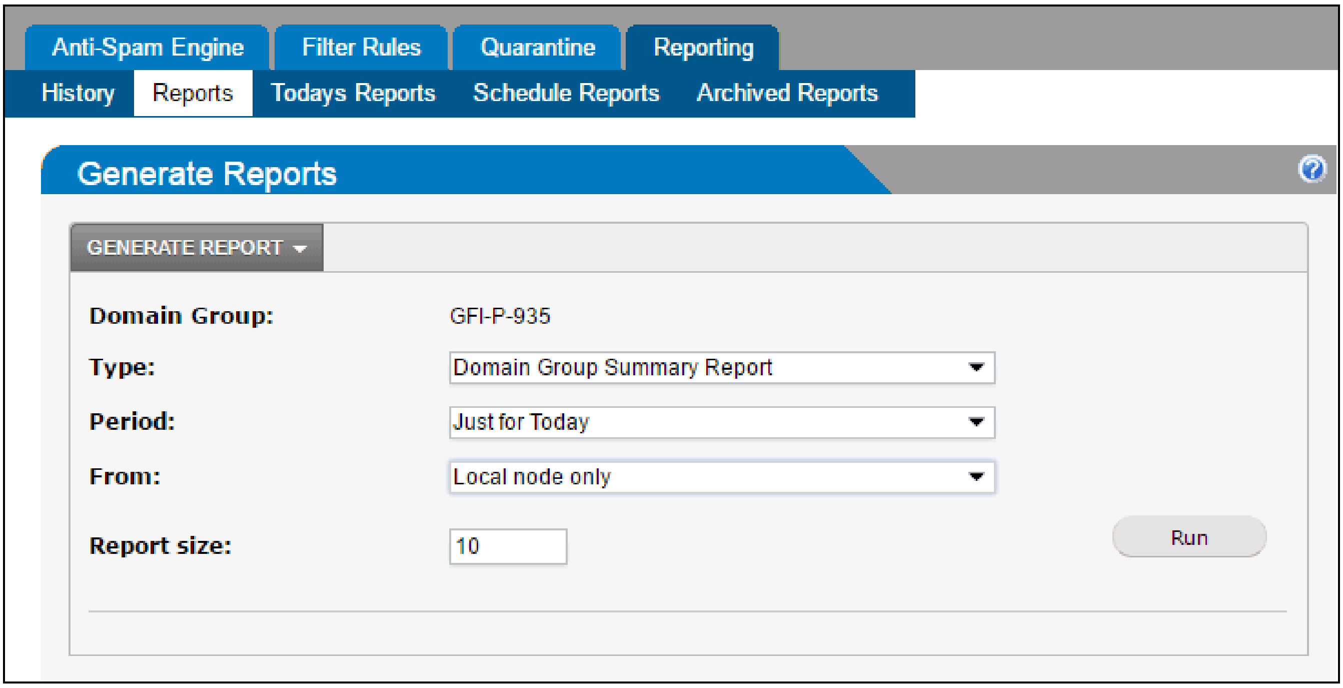
The following table describes the various Display Settings:

Display Setting	Description
Show Message Subject	Displays the subject of the message
Show Score for Clean Messages	Shows the score assigned by GFI MailSecurity for messages classified as **Clean** in the **Type** column.
Show Score for Spam Messages	Displays the score assigned by GFI MailSecurity for messages classified as **Spam** in the **Type** column .
Show Virus name for Virus Messages	Shows the virus name that the scanner detected in the **Type** column of for virus messages. Note that GFI MailSecurity uses multiple virus scanners. If the virus scanners have different names for the virus, the name of the virus as identified by the virus scanner which identified the virus first is used.
Show Scanner that detected Virus	Displays the name(s) of the virus scanner(s) that detected the virus in the **Type** column for virus messages.

Display Setting	Description
Show Message Flow	Shows the direction of the email.
Show TLS encryption status	Shows the status of the Transport Layer Security (TLS)
Show delivery status	Shows the delivery status.
Show delivery response	Shows the SMTP response from the destination server.
Show RBL name	Shows the name of the Real-time Blackhole List (RBL) that blocked the message.

Generating reports

The **Reporting > Reports** page allows you to generate a number of on-demand reports.



Domain Group: GFI-P-935

Type: Domain Group Summary Report

Period: Just for Today

From: Local node only

Report size: 10

Screenshot 16: Generating reports

The following table describes the options available when generating on-demand reports:

Field	Description
Type	Select the type of report to generate. The report types groups the information that includes overview of mail usage, top spam and viruses recipients .
Period	Choose the period for which the report is generated. Options available are: » Just for Today » From Yesterday » Last 7 Days » All Note that a report period of **All** generates a report based on all the records in the database. As records can be automatically purged, this may not include all records since subscribing to GFI MailSecurity.

Field	Description
From	Choose the option that matches the scope of report. The options are: Local node only: Restricted to the server from where the report is been generated. Cluster: Include the entire cluster.
Report Size	Indicates the number of items to include in the report. This value is only relevant for top-ten type reports. Note that the pie chart is limited to a maximum of 25 items.

Click **Run** to start generating the report.

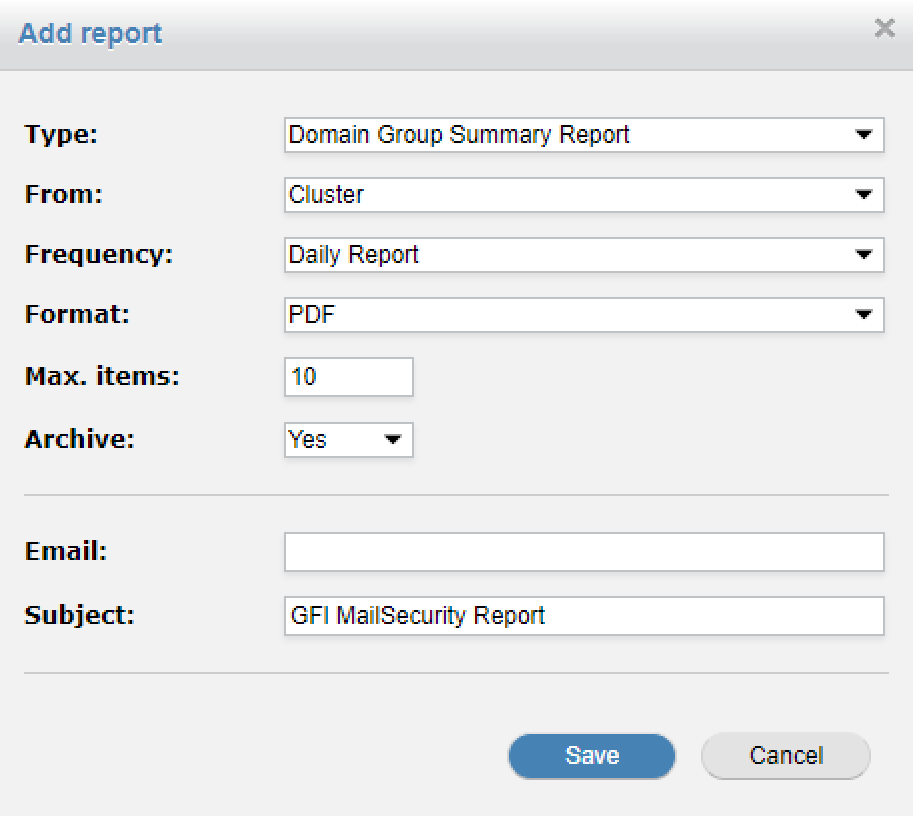
Go to **Reporting > Today's Report** to access all the on-demand reports that were requested today. The latest report is displayed on top. Click **View** to see the report data.

The following actions can be performed on generated reports:

Option	Description
View	Click to view your generated report. The displayed information depends on the type of report selected. Some reports display in the form of a table and some display as a pie chart.
Generate PDF Report	Generate and download a PDF version of the report.
Download to Spreadsheet	Generate and download a Microsoft Excel spreadsheet version of the report.
Delete	Delete the selected report. Note that deleted reports are not recoverable.
Archive	Generated reports are automatically purged on a daily basis. To save the report for longer, then you can archive it by clicking Archive. The Archive is accessible from **Reporting > Archived Reports** tab. For more information, refer to Archived Reports (page 27).

Scheduled Reports

GFI MailSecurity reports enable you to generate reports on a pre-defined schedule to automate the generation of reports that are required on a regular basis. Scheduled reports are sent via email to a custom list of email addresses at a particular frequency.



Type: Domain Group Summary Report
From: Cluster
Frequency: Daily Report
Format: PDF
Max. items: 10
Archive: Yes
Email:
Subject: GFI MailSecurity Report

Screenshot 17: Scheduled Reports options

Access the **Reporting > Schedule Reports** and configure the following report parameters:

Option	Description
Type	Select the type of report to generate. The reports available may vary depending on the role. The Domain Group Administrator role has access to organizational reports, and the data includes metrics for all domains. The Domain Administrator role can generate reports for the selected domain only. Change the role and the domain from the top-right corner of the screen.
From	Choose the option that matches the scope of report. The options are: » Local node only: Restricted to the server from where the report is been generated. » Cluster: Include the entire cluster.
Frequency	Choose how frequent you need to receive the report: » **Daily**: a report for the previous day's activity. » **Weekly**: run report every Monday covering the previous Monday-Sunday period. » **Monthly**: run report on the 1st day of every month covering the data for the previous month.
Format	Reports can be generated in a **PDF** document, a **text** file, a Microsoft **Excel** spreadsheet or all three.
Max Items	The maximum number of items to display in the report.
Archive	Specifies if the report should be saved in the Archive.
Email Address	Enter the addresses where to send the reports. Separate multiple emails addresses with spaces.
Subject	The subject to use for emailed reports.

Click **Save** to save the scheduled report.

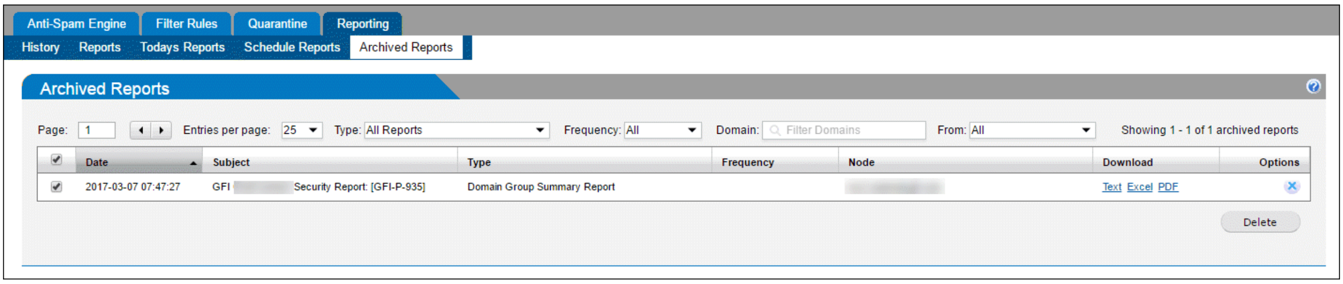
Archived Reports

Generated on-demand reports are by default stored only temporarily, unless users opt to store a copy of the report in the Archive. The Archive page also stores copies of scheduled reports that are configured to be archived.

The **Reporting > Archived Reports** page lists all the reports that have been archived on GFI MailSecurity.

From this page you can download reports in Text, Microsoft Excel or PDF formats or permanently delete the archived report.

Use the **Type**, **Frequency** and **Domain** settings to filter the list of displayed reports.



Archived Reports

Page: 1 Entries per page: 25 Type: All Reports Frequency: All Domain: Filter Domains From: All Showing 1 - 1 of 1 archived reports

☑	Date	Subject	Type	Frequency	Node	Download	Options
☑	2017-03-07 07:47:27	GFI [redacted] Security Report: [GFI-P-935]	Domain Group Summary Report		[redacted]	Text Excel PDF	✕

Screenshot 18: Archived Reports

3 System Settings

The topics in this section describe how to customize and configure GFI MailSecurity system settings.

Access/Authentication

Relay Settings

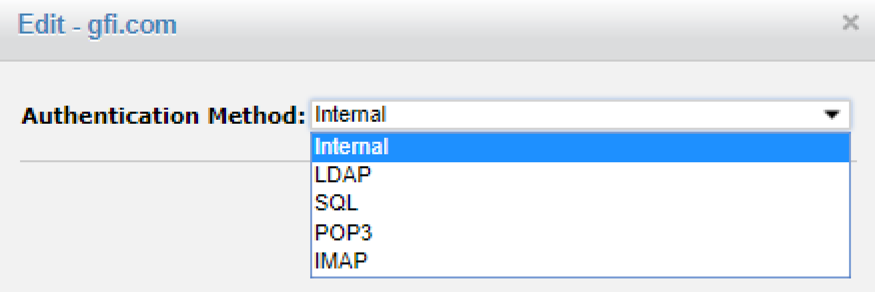
Change Password

Topics in this section:

3.1 Access / Authentication

The Web Authentication settings allow you to configure and manage the user authentication method for each internal domain to access the GUI.

Go to **Settings** > **Access/Authentication**. Edit <Domain> pop up is displayed.



Edit - gfi.com

Authentication Method: Internal

Screenshot 19: Select your authentication method

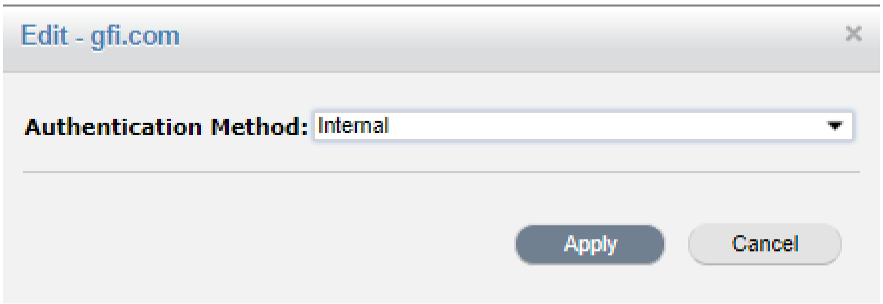
The following authentication methods are supported:

3.2 Internal

This is the default authentication method.

GFI MailSecurity generates a unique password for each internal email address for which it processes mail.

If you forget your password you can receive it via email by clicking the **Forgot your Password?** link on the Login page and entering your email address. You can then change your password after logging in.



Authentication Method: Internal

Screenshot 20: Internal is the Default authentication method

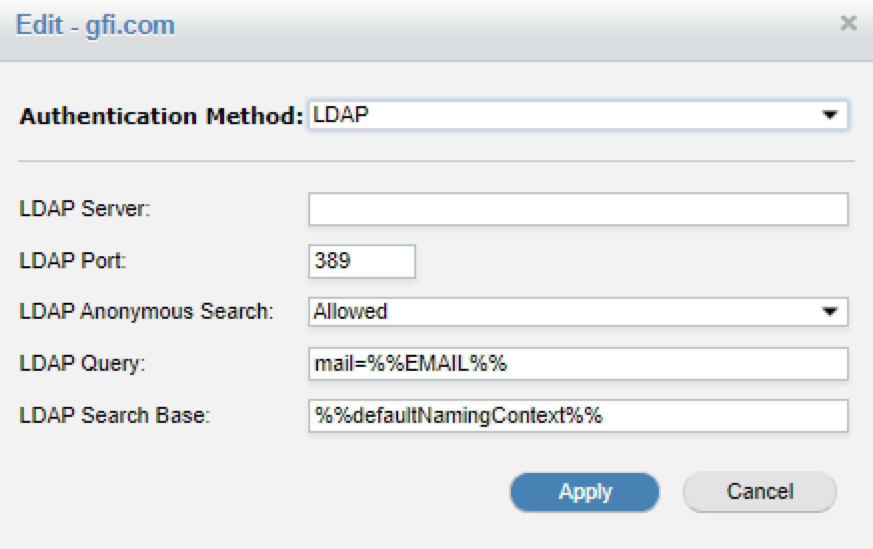
3.3 LDAP

Here you can specify an external LDAP enabled directory to authenticate and authorize users on a per-domain basis. GFI MailSecurity can be configured to support any LDAP compliant director including Microsoft Active Directory, Lotus Domino, SunOne/iPlanet Directory Server and Novell eDirectory.

To authenticate with an external LDAP server you can specify LDAP as the **Authentication Method** for that domain and enter the LDAP server details.

The following table describes the LDAP fields to be entered:

LDAP Settings	Description
LDAP Server	The name of the LDAP server that GFI MailSecurity attempts to connect to for authentication purposes.
LDAP Port	The port GFI MailSecurity uses to connect to the LDAP server for authentication purposes. This is set to `389` by default.
LDAP Anonymous Search	Some LDAP directories require a valid username/password to bind to the server in order to perform LDAP searches. Use this drop-down list to specify if anonymous bind is allowed to the LDAP server.
LDAP Search User DN	If anonymous bind is not permitted then you must specify the DN of the user that is used to bind to the Directory server specified in the LDAP server and port field as administrator. This is usually an email address or directory object of the form: cn=user,dc=company,dc=com.
LDAP Password	This field contains the password for the administrator profile specified in the LDAP Search User DN field.
LDAP Query	This field specifies the attribute that contains the username of the person authenticating. The default is `mail=%%EMAIL%%` (here `%%EMAIL%%` is replaced with the email of the user authenticating. For example, if the email address of the authenticating user is joe@domain.com then `%EMAIL%%` is replaced with joe@domain.com. Similarly, `%%USER%%` can be used to specify the left-hand side of the email address.
LDAP Search Base	This field specifies the point of commencement of the search in the directory. If the LDAP server is able to determine the `defaultNamingContext` (Active Directory only) then you can specify `%%defaultNamingContext%%` and the authentication module determines this before doing the search.



Edit - gfi.com

Authentication Method: LDAP

LDAP Server:

LDAP Port: 389

LDAP Anonymous Search: Allowed

LDAP Query: mail=%%EMAIL%%

LDAP Search Base: %%defaultNamingContext%%

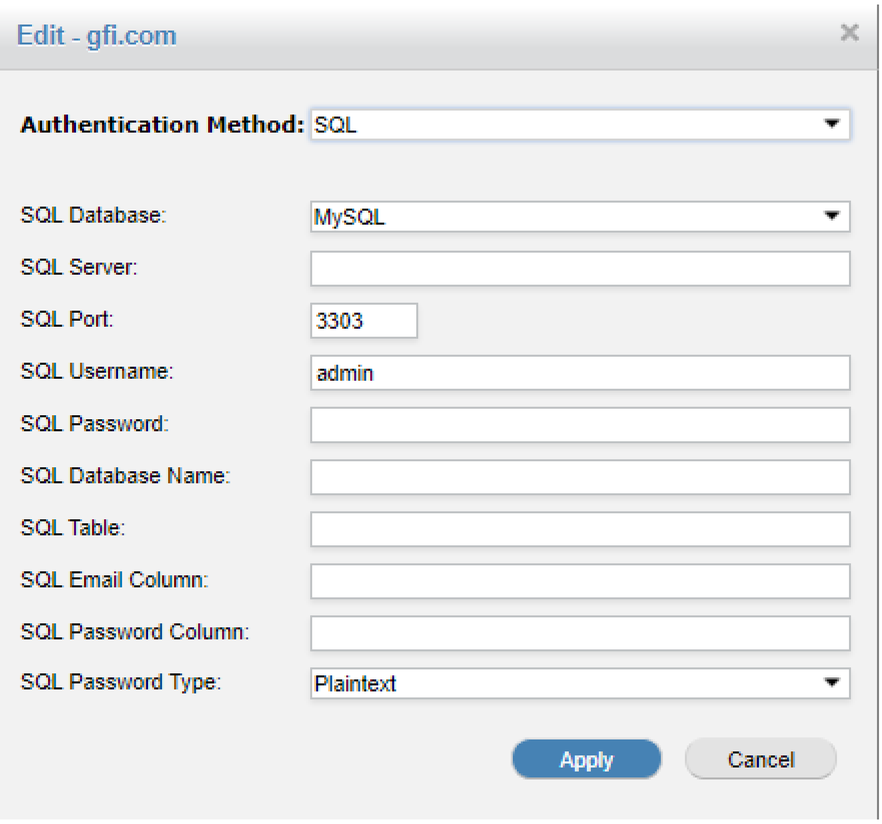
Screenshot 21: Enter the fields on this pop up. See the above table for help

3.4 SQL Server

SQL Authentication allows you to perform authentication against an external SQL server. Specify SQL as the **Authentication Method** and enter the credentials that the appliance uses to connect to the SQL server.

The following table describes the SQL authentication settings:

SQL Settings	Description
SQL Database	This field specifies the SQL database type.
SQL Server	The IP address or hostname of the SQL server that GFI MailSecurity attempts to connect to for authentication purpose.
SQL Port	The port GFI MailSecurity uses to connect to the SQL Server for authentication purpose. This is set to 3306 by default.
SQL Username	The username used to connect to the SQL server in order to perform the authentication.
SQL Password	The password associated with the username.
SQL Database Name	The field contains the name of the database containing the authentication tables.
SQL Table	The SQL table to be queried for the authentication.
SQL Email Column	The column that contains the list of email addresses.
SQL Password Column	This field specifies the column that contains the password.
SQL Password Type	The password may be stored in plaintext format, or as a MD5 checksum, or encrypted.



Authentication Method: SQL

SQL Database: MySQL

SQL Server:

SQL Port: 3303

SQL Username: admin

SQL Password:

SQL Database Name:

SQL Table:

SQL Email Column:

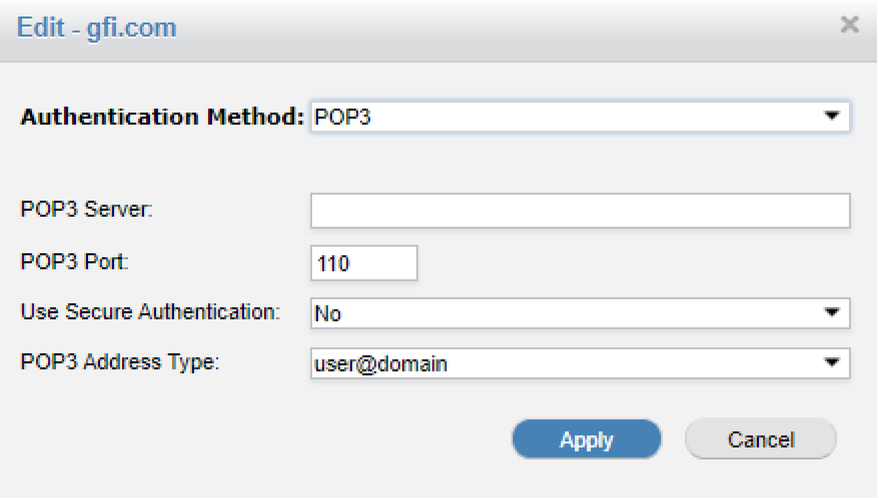
SQL Password Column:

SQL Password Type: Plaintext

Screenshot 22: Enter the fields on this pop up. See the above table for help

3.5 POP3

When authentication against a POP3 server is enabled, users attempting to login to the GUI have their credentials authenticated via a POP3 server.



Authentication Method: POP3

POP3 Server:

POP3 Port: 110

Use Secure Authentication: No

POP3 Address Type: user@domain

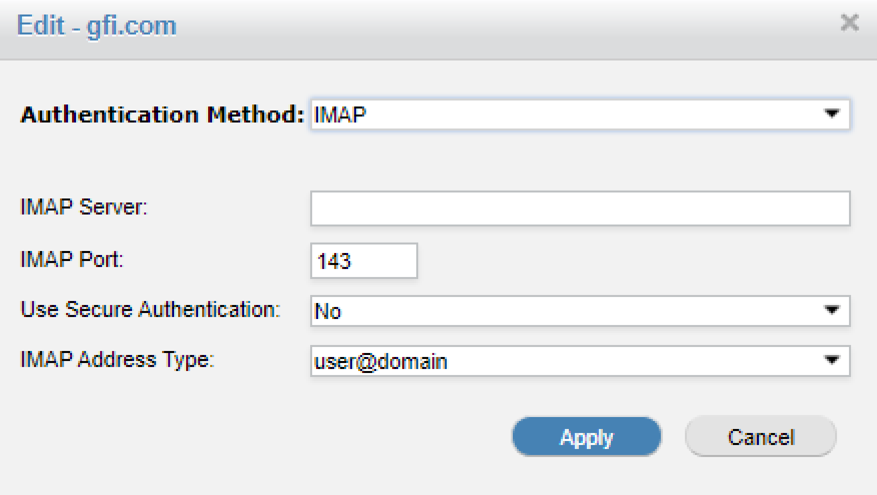
Screenshot 23: Enter the fields on this pop up. See the above table for help

The following table describes the POP3 authentication settings:

POP3 Settings	Description
POP3 Server	The IP address or hostname of the POP3 server that GFI MailSecurity attempts to connect to for authentication purposes.
POP3 Port	The port GFI MailSecurity uses to connect to the POP3 server for authentication purposes. This is set to `110` by default.

POP3 Settings	Description
POP3 Address Type	This is the format required by the pop3 server for the username. If the pop3 server requires only the mailbox name for authentication, then select the user. GFI MailSecurity then truncates the domain name from the user supplied email.

3.6 IMAP



Edit - gfi.com

Authentication Method: IMAP

IMAP Server:

IMAP Port: 143

Use Secure Authentication: No

IMAP Address Type: user@domain

Screenshot 24: Enter the fields on this pop up. See the above table for help

The following table specifies the IMAP fields to be entered if using IMAP as the authentication method for the GUI:

IMAP Settings	Description
IMAP Server	The IP address or hostname of the IMAP server that GFI MailSecurity attempts to connect to for authentication purposes.
IMAP Port	The port used by GFI MailSecurity to connect to the IMAP server for authentication purposes. This is set to 143by default.
IMAP Address Type	This field specifies the format expected by your IMAP server. Some IMAP servers require the credentials to be specified as an email address, while others require just the left-hand side of the email address (the username).

You can use the **Test Authentication** feature on the **Settings > Access/Authentication** page to ensure that your settings are correct.

To test Authentication, enter the **Email Address** and **Password** of a user to test in the Test Authentication section and click **Test**.

GFI MailSecurity determines the authentication method to use for that domain and validate the supplied password.

3.7 Relay Settings

You can login as **Domain Group Administrator** and create as many domains as you want. Each domain can have its own domain administrators created.

Creating a domain is very simple, in GFI EmailSecurity. Follow the below steps:

1. Login to GFI MailSecurity as the Domain Group Administrator.

2. Go to **Settings > Relay Settings**.

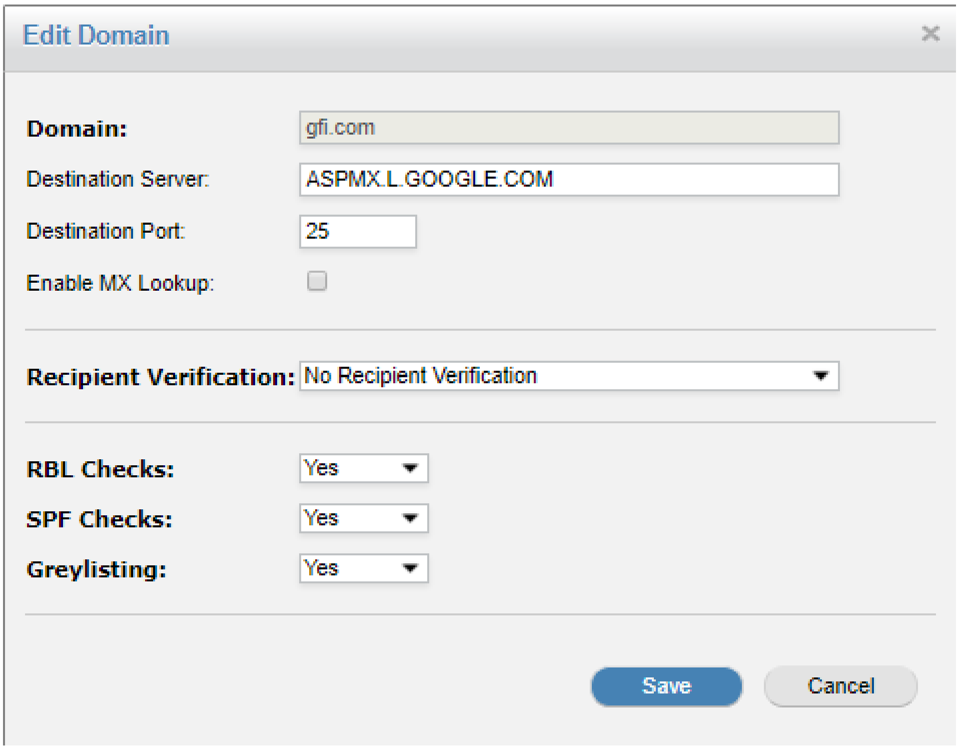
3. On **Mail Relay Settings** page , click **Add** .

4. Enter the fields on **Add Domain** pop up. (eg "gfi.com")

The following table describes the **Add Domain** fields to be entered:

Field	Description
Domain	The Domain name.
Destination Server	The host where the email server resides.
Destination Port	The port GFI MailSecurity used to connect to the IMAP server for authentication purposes. This is set to `143` by default.
Enable MX Lookup	Check this to enable MX lookup.
Recipient Verification	Set this field to **Dynamic Recipient Verification** if your mail server supports it. This checks the address of incoming email with the mail server. If the intended recipient is unknown then the email is dropped with a DSN (Delivery Status Notification) message and no further processing is performed. If **Dynamic Recipient Verification** is not supported then you can select other options and make the required settings accordingly. » **No Recipient Verification**: Recipient verification does not happen. » **LDAP Recipient Verification** if you are running Active Directory then select this verification type and enter your LDAP (Lightweight Directory Access Protocol)server details. The LDAP query filter then queries the LDAP server to check if the intended recipient(s) are valid or not. » **Specify Allowed Recipients**: You can enter a list of valid email address manually or import a list from a text file. Specify one email address per line. » **Specify Regular Expression**: You can specify regular expression for the valid email address type.
RBL Checks	Select whether RBL (**Realtime Blackhole Lists**) check is required or not. This is used to check if an incoming message has passed through one or more machines which are blacklisted as spam sources or relays.
SPF Checks	Select whether SPF (**Sender Policy Framework**) check is required or not. SPF allows the owner of a domain to use special DNS records to specify which machines are authorized to transmit e-mail for that domain.
Greylisting	Select whether **Greylisting** is required or not. It is an anti-spam technique which initially does not accept an email from an unknown source but after some time it accepts.

To edit a domain, click ✎ corresponding to the domain you want to edit. On the **Edit Domain** pop up, make the required changes and click **Save**.


Edit Domain

Domain: gfi.com

Destination Server: ASPMX.L.GOOGLE.COM

Destination Port: 25

Enable MX Lookup: □

Recipient Verification: No Recipient Verification

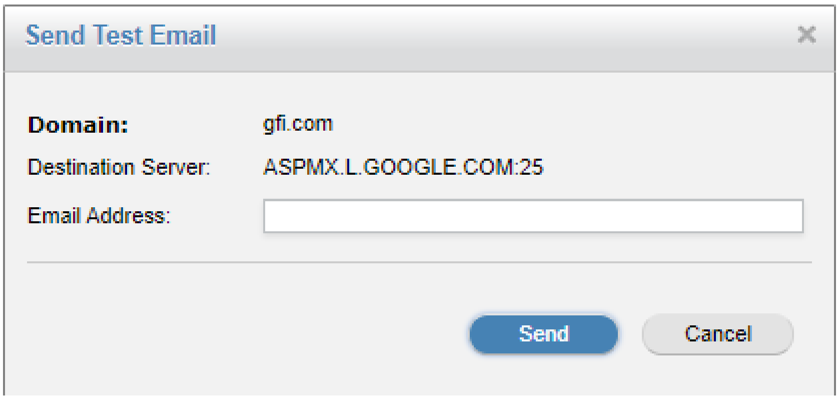
RBL Checks: Yes

SPF Checks: Yes

Greylisting: Yes

Screenshot 25: Use this window to edit domain information

To test a domain, click ✓ corresponding to the domain you want to test. On the **Send Test Mail** pop up, enter the **Email Address** and click **Send**.


Send Test Email

Domain: gfi.com

Destination Server: ASPMX.L.GOOGLE.COM:25

Email Address:

Screenshot 26: Use this window to send test mail

> **Note:** The DNS changes might take some time to take effect, and until such changes take effect not all emails would be routed through the service.

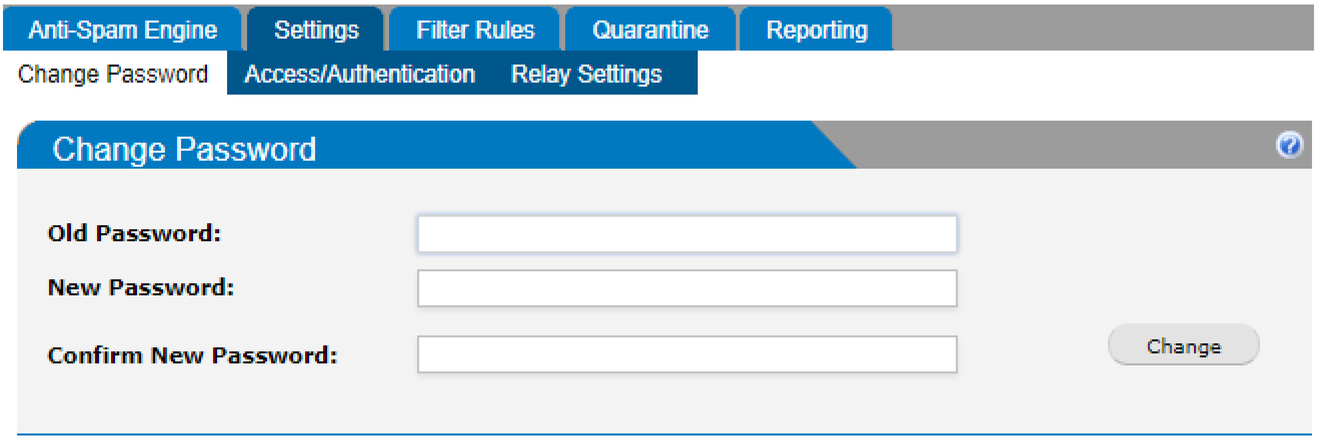
3.8 Change Password

To change password follow the below steps:

1. Go to **Settings > Change Password**

2. Enter the **Old Password**, **New Password**, **Confirm New Password** and click **Change**.

The password is changed.

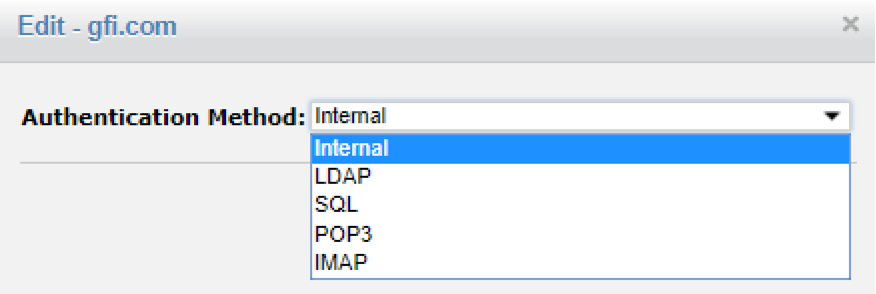


Screenshot 27: Use this window to change your password

3.9 Access / Authentication

The Web Authentication settings allow you to configure and manage the user authentication method for each internal domain to access the GUI.

Go to **Settings** > **Access/Authentication**. Edit <Domain> pop up is displayed.



Screenshot 28: Select your authentication method

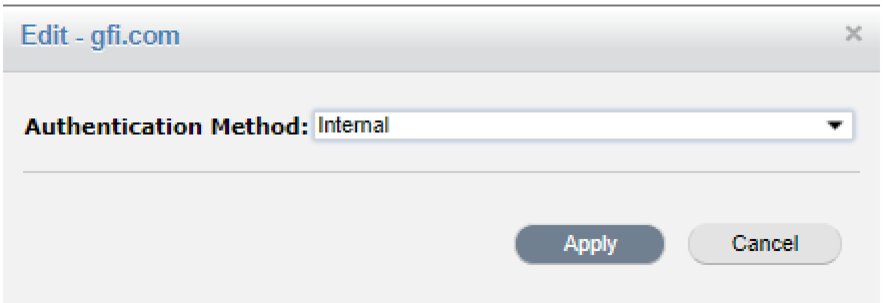
The following authentication methods are supported:

3.10 Internal

This is the default authentication method.

GFI MailSecurity generates a unique password for each internal email address for which it processes mail.

If you forget your password you can receive it via email by clicking the **Forgot your Password?** link on the Login page and entering your email address. You can then change your password after logging in.



Authentication Method: Internal

Screenshot 29: Internal is the Default authentication method

3.11 LDAP

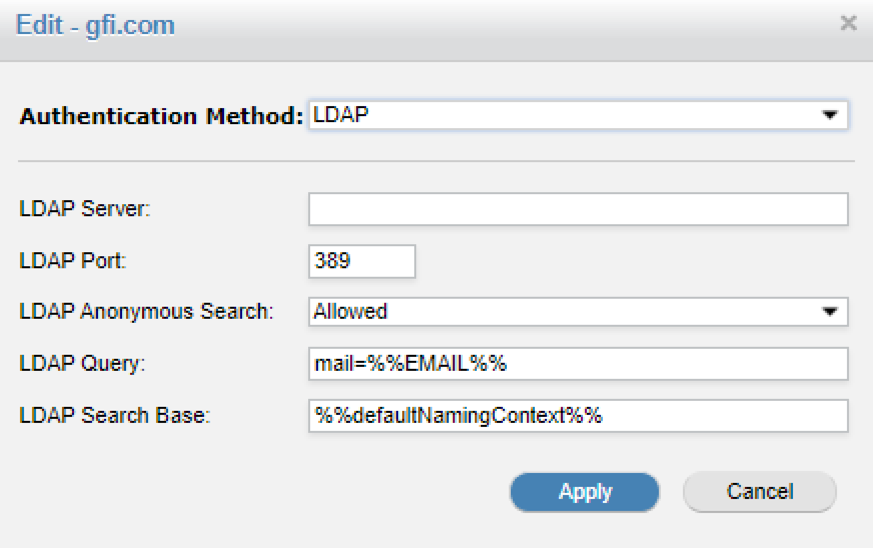
Here you can specify an external LDAP enabled directory to authenticate and authorize users on a per-domain basis. GFI

MailSecurity can be configured to support any LDAP compliant director including Microsoft Active Directory, Lotus Domino, SunOne/iPlanet Directory Server and Novell eDirectory.

To authenticate with an external LDAP server you can specify LDAP as the **Authentication Method** for that domain and enter the LDAP server details.

The following table describes the LDAP fields to be entered:

LDAP Settings	Description
LDAP Server	The name of the LDAP server that GFI MailSecurity attempts to connect to for authentication purposes.
LDAP Port	The port GFI MailSecurity uses to connect to the LDAP server for authentication purposes. This is set to `389` by default.
LDAP Anonymous Search	Some LDAP directories require a valid username/password to bind to the server in order to perform LDAP searches. Use this drop-down list to specify if anonymous bind is allowed to the LDAP server.
LDAP Search User DN	If anonymous bind is not permitted then you must specify the DN of the user that is used to bind to the Directory server specified in the LDAP server and port field as administrator. This is usually an email address or directory object of the form: cn=user,dc=company,dc=com.
LDAP Password	This field contains the password for the administrator profile specified in the LDAP Search User DN field.
LDAP Query	This field specifies the attribute that contains the username of the person authenticating. The default is `mail=%%EMAIL%%` (here `%%EMAIL%%` is replaced with the email of the user authenticating. For example, if the email address of the authenticating user is joe@domain.com then `%EMAIL%%` is replaced with joe@domain.com. Similarly, `%%USER%%` can be used to specify the left-hand side of the email address.
LDAP Search Base	This field specifies the point of commencement of the search in the directory. If the LDAP server is able to determine the `defaultNamingContext` (Active Directory only) then you can specify `%%defaultNamingContext%%` and the authentication module determines this before doing the search.


Edit - gfi.com

Authentication Method: LDAP

LDAP Server:

LDAP Port: 389

LDAP Anonymous Search: Allowed

LDAP Query: mail=%%EMAIL%%

LDAP Search Base: %%defaultNamingContext%%

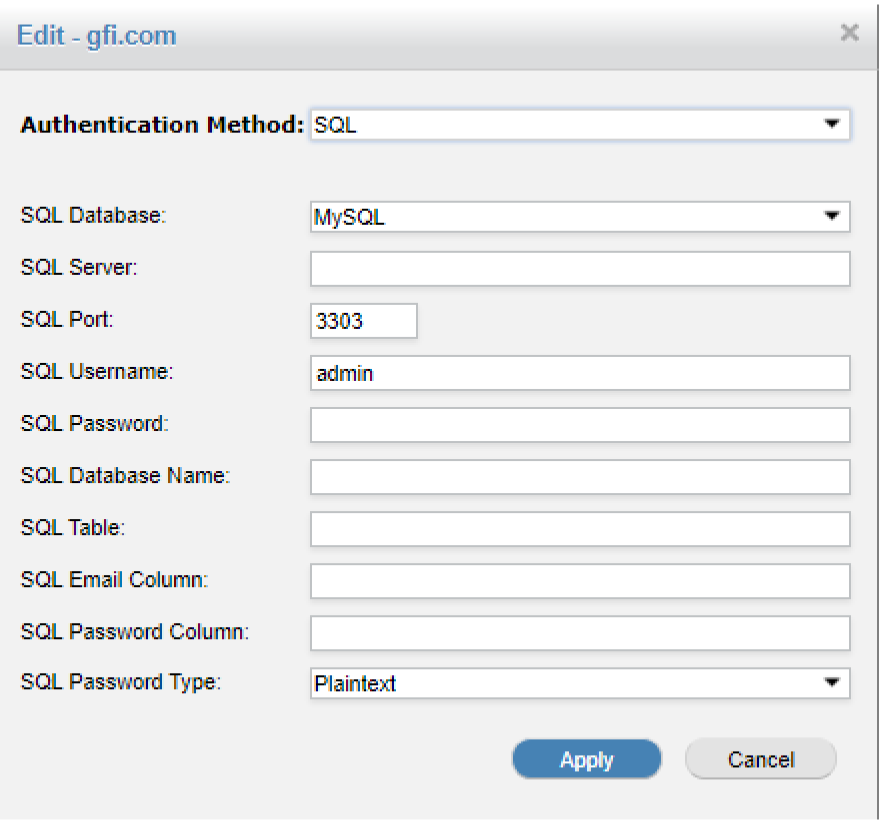
Screenshot 30: Enter the fields on this pop up. See the above table for help

3.12 SQL Server

SQL Authentication allows you to perform authentication against an external SQL server. Specify SQL as the **Authentication Method** and enter the credentials that the appliance uses to connect to the SQL server.

The following table describes the SQL authentication settings:

SQL Settings	Description
SQL Database	This field specifies the SQL database type.
SQL Server	The IP address or hostname of the SQL server that GFI MailSecurity attempts to connect to for authentication purpose.
SQL Port	The port GFI MailSecurity uses to connect to the SQL Server for authentication purpose. This is set to 3306 by default.
SQL Username	The username used to connect to the SQL server in order to perform the authentication.
SQL Password	The password associated with the username.
SQL Database Name	The field contains the name of the database containing the authentication tables.
SQL Table	The SQL table to be queried for the authentication.
SQL Email Column	The column that contains the list of email addresses.
SQL Password Column	This field specifies the column that contains the password.
SQL Password Type	The password may be stored in plaintext format, or as a MD5 checksum, or encrypted.



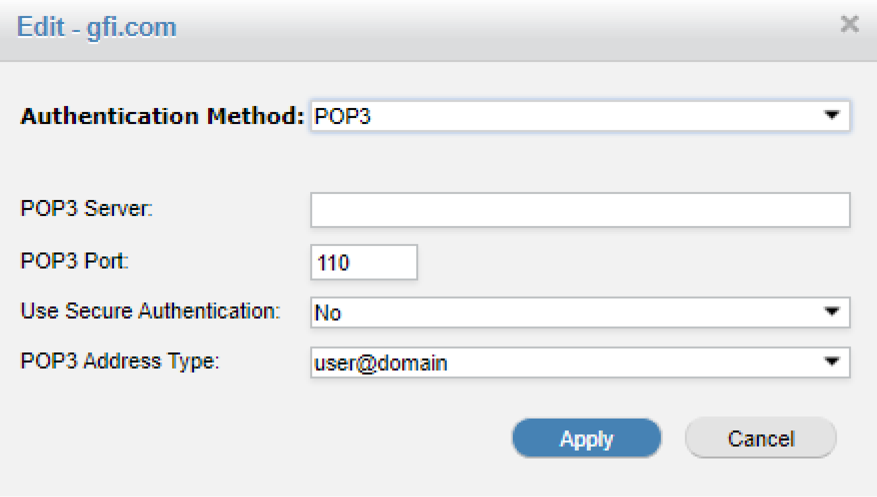
Authentication Method: SQL

SQL Database:	MySQL
SQL Server:	
SQL Port:	3303
SQL Username:	admin
SQL Password:	
SQL Database Name:	
SQL Table:	
SQL Email Column:	
SQL Password Column:	
SQL Password Type:	Plaintext

Screenshot 31: Enter the fields on this pop up. See the above table for help

3.13 POP3

When authentication against a POP3 server is enabled, users attempting to login to the GUI have their credentials authenticated via a POP3 server.



Edit - gfi.com

Authentication Method: POP3

POP3 Server:

POP3 Port: 110

Use Secure Authentication: No

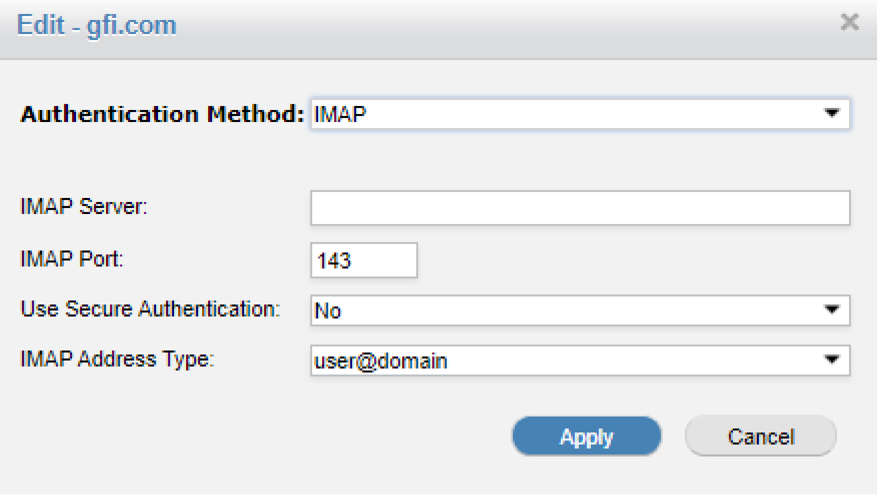
POP3 Address Type: user@domain

Screenshot 32: Enter the fields on this pop up. See the above table for help

The following table describes the POP3 authentication settings:

POP3 Settings	Description
POP3 Server	The IP address or hostname of the POP3 server that GFI MailSecurity attempts to connect to for authentication purposes.
POP3 Port	The port GFI MailSecurity uses to connect to the POP3 server for authentication purposes. This is set to 110 by default.
POP3 Address Type	This is the format required by the pop3 server for the username. If the pop3 server requires only the mailbox name for authentication, then select the user. GFI MailSecurity then truncates the domain name from the user supplied email.

3.14 IMAP



Edit - gfi.com

Authentication Method: IMAP

IMAP Server:

IMAP Port: 143

Use Secure Authentication: No

IMAP Address Type: user@domain

Screenshot 33: Enter the fields on this pop up. See the above table for help

The following table specifies the IMAP fields to be entered if using IMAP as the authentication method for the GUI:

IMAP Settings	Description
IMAP Server	The IP address or hostname of the IMAP server that GFI MailSecurity attempts to connect to for authentication purposes.

IMAP Settings	Description
IMAP Port	The port used by GFI MailSecurity to connect to the IMAP server for authentication purposes. This is set to `143`by default.
IMAP Address Type	This field specifies the format expected by your IMAP server. Some IMAP servers require the credentials to be specified as an email address, while others require just the left-hand side of the email address (the username).

You can use the **Test Authentication** feature on the **Settings > Access/Authentication** page to ensure that your settings are correct.

To test Authentication, enter the **Email Address** and **Password** of a user to test in the Test Authentication section and click **Test**.

GFI MailSecurity determines the authentication method to use for that domain and validate the supplied password.

4 Glossary

A

Active Directory

A technology that provides a variety of network services, including LDAP-like directory services.

Admin Console

A web interface for adminsitrators to manage and configure GFI MailSecurity.

Adminstrator Account

Account of a user with administrative rights to manage and configure GFI MailSecurity.

Antivirus

A software countermeasure that detects malware installed on a computer without the user's knowledge.

Auto-reply

An email reply that is sent automatically to incoming emails.

B

Blacklist

A list of email addresses and domains from which emails are always blocked.

C

CSV

A comma serperated values file format.

D

Dashboard

A graphical representation that indicates the status and statistics of various operations.

Data Center

A remote location on a GFI MailSecurity Server through which the email traffic is santized and then routed to the Exchange Server. It is also used for queuing emails during outage and for storing archives and synchronized calender and contact information.

Directory Harvesting

Email attacks where known email addresses are used as a template to create other email addresses.

DN

DN stands for Distinguished names. The DN is the name that uniquely identifies an entry in the directory.

DNS

Domain Name System (DNS) is a database used by TCP/IP networks that enables the translation of hostnames into IP numbers and to provide other domain related information.

Domain

Address or URL of a particular network.

Domain Controller

A server that responds to security authentication requests within a domain, such as when logging in and checking permissions.

E

EWS

Exchange Web Services

F

False Positives

Legitimate emails that are incorrectly identified as spam.

G

GPO

Group Policy Object (GPO) is an Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

H

Hyper-V

Microsoft's virtual machine capability.

I

inbound email

Email to be received.

Infrastructure

A collection of physical or virtual resources that supports an overall Email environment

J

Journaling

A feature that generates and sends a copy of every email that passes through the mail server. Do not confuse it with Archiving.

L

LDAP

Lightweight Directory Access Protocol (LDAP) is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an (IP) network.

M

Mail server

The server that manages and stores client emails.

Mailbox

A directory or folder on the mail server used for receipt, filing, and storing emails.

Malware

All malicious types of software that are designed to compromise computer security and which usually spread through malicious methods.

MX Records

A mail exchanger record. It is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient's domain, and a preference value used to prioritize mail delivery if multiple mail servers are available.

N

NETBIOS

An acronym for Network Basic Input/output. This system provides services to allow applications on different computers within a network to communicate with each other.

O

outage

Refers to a situation when the email server is down or offline.

outbound email

Email to be sent.

P

Partial Activation

Activating Continuity for a subset of your users only.

Q

Quarantine

A email database where emails detected as spam and/or malware are stored in a controlled enviornment. Quarantined emails are not a threat to the network

R

Real-time Blackhole List

A list of domains and IP addresses that have been classified as spammers

Redirectors

Transport agents that enable dynamic rerouting of messages in Exchange environments.

Reviewer Group

Archive users who have the ability to search and read emails that are within the scope of a group of users.

Root Account

The user credentials used to register for a GFI MailSecurity account.

S

SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard used by GFI OneGuard for electronic mail (email) transmission. SMTP by default uses TCP port 25.

Spam

An irrelevant or unsolicited email sent over for the purposes of advertising, phishing, spreading malware, etc.

SSL

Secure Sockets Layer (SSL) is a computer networking protocol for securing connections between network application clients and internet.

T

TCP ports

Acronym for Transmitting Control Protocol. This protocol is developed to allow applications to transmit and receive data over the internet using the well-known computer ports.

TLS

Transport Layer Security (TLS) is a predecessor of Secure Sockets Layer (SSL), and just like SSL, it provide communications security over a computer network.

U

URL

The Uniform Resource Locator (URL) is the address of a web page on the world wide web.

W

Whitelist

A list of email addresses and domains from which emails are always received.

5 Index