



Quick Start Guide for Administrators

GFI MAX MailProtection[™]
Hosted Email Security and Continuity

Quick Start Guide for Administrators

Welcome

Thank you for choosing GFI MAX MailProtection™ (formerly Katharion™).

As a leader in combating spam, GFI is committed to providing a highly effective solution to help you significantly reduce junk email. This document will guide you through the basic GFI MAX MailProtection set-up process quickly and easily. For more information on advanced settings and customization options, please contact your GFI MAX MailProtection account representative or authorized GFI MAX Mail Services Partner.

Your Login Information

Domain login [typically yourdomain.com-dom]: _____

Domain password: _____

Please record your administrative login in the space above.

Step 1: Adding mailboxes

In order to work properly, GFI MAX MailProtection needs to know all of the valid email addresses for your domain. The list of mailboxes (sometimes referred to as email accounts or users) within GFI MAX MailProtection can be maintained via several methods:

1. You can manually add or remove mailboxes in the control panel. See Part 1 below for a step-by-step description.
2. GFI MAX MailProtection can periodically connect to your mail server to automatically mirror the email addresses and aliases already established on your mail server. This is typically done via the LDAP protocol and requires a simple one-time process, after which all of the mailboxes will be maintained automatically without further intervention.

Part 1: Add users

- » Log into the control panel at <https://maxmail.gfi.com>.
You will find your administrative user name and password on the first page of this document.
- » Click on the Management tab at the top of the screen.
- » Select User Management on the Management Overview page.

Quick Start Guide for Administrators

Add, Change, or Replace User(s)

Select Method for Updating Your User List

This page is for manually adding/updating users only. If you use LDAP or another synchronization method to handle your users, please use the [Synchronization page](#).

UPLOAD a file containing a list of user accounts and passwords:

ENTER or CUT AND PASTE addresses and passwords into a text box:

- » Click on the Add/Change User(s) link in the left-hand menu.
- » You have the option to upload a file containing a list of email addresses and passwords, or you can manually enter the information. You can also enter any aliases (also known as forwarding addresses) by following the format recommended on that page, or you can set up any aliases separately later (see Part 2 below).
- » Once you have uploaded or entered your user information, click the Next button.
- » You will now have the chance to review the new user information. If you see any errors, simply go back to the previous page and make any necessary revisions.

Part 2: Add aliases

An alias is a secondary email address, such as **info@yourcompany.com**, that is forwarded to another email address used by the same person. All aliases should be entered into GFI MAX MailProtection so that they too can be filtered for spam. An alias will inherit the spam handling rules and configuration of its primary account. Aliases can be configured when you create users for the domain as described above, or by following these directions:

- » Click on the Management tab at the top of the screen.
- » Select User Management on the Management Overview page.
- » From the Manage Existing Users page, find the user to which you wish to add an alias address and select the icons within the Manage Aliases Column on the right.

Quick Start Guide for Administrators

» Type the full alias address into the text box and click Save Changes.

User Alias Management

Each account may have one or more alternate addresses or "aliases." If you enter these aliases below, messages sent to them will be screened using the same settings that are used for the user's main account.

Please enter one alias address per line in the box below. To remove an existing alias, simply delete the alias from the box.

[Return to user list](#)

Step 2: Adjusting your spam handling settings

Now that your email addresses have been entered into the system, you can select from one of several spam handling options. You can change the domain-wide setting by clicking on the Management tab, then clicking on Inbound Filtering.

Delivery of Detected Spam Messages ?

Detected spam should be:

- Dropped silently
- Redirected to the recipient's junk mail quarantine
- Delivered to the intended recipient
- Delivered to:

Quick Start Guide for Administrators

You have several options for handling spam messages detected by GFI MAX MailProtection:

1. The first option is for GFI MAX MailProtection to simply drop the message. Be advised that, with this option enabled, any message detected as spam will be gone for good. As a result, we generally do not recommend selecting this option, particularly when first using the service.
2. The second option is for GFI MAX MailProtection to forward detected spam to the intended recipient. This setting is generally used in conjunction with the "Add **SPAM** to the subject line of every detected spam" option.
3. The third option is for GFI MAX MailProtection to redirect all the junk mail to a single email address at your domain, i.e. spam@yourcompany.com. This allows for administrator-level review.
4. The fourth option is for GFI MAX MailProtection to redirect junk mail to individual, password-protected junk mail quarantines for each user. **This is the recommended spam-handling option.** The quarantine is hosted by GFI MAX MailProtection and can be reviewed at any time by end-users. The use of the quarantine reduces the bandwidth requirements for an organization's network as well as the load on its mail server(s).

Optional – Configuring Message Digest delivery for the domain

If you have elected to redirect spam into the junk-mail quarantines, we recommend also activating Message Digest delivery for all users. The Message Digest is a list of all emails that have been delivered to the user's quarantine since the last Digest was issued. It allows users to easily review spam and release any false positives (messages that were erroneously flagged as spam) from the quarantine.

To manage Message Digest settings for all users in the domain, navigate to Management > Inbound Filtering > Message Digests.

Select the desired Digest delivery frequency (anywhere from once a week to three times a day) and click the 'Save Changes' button. You can also configure our system to withhold empty junk mail digests for users who have received no junk mail.

From the additional tabs, you can resend a previously generated junk mail digest, or set up a periodic emailed statistics report which shows the volume of legitimate messages, spam, and viruses we caught for the domain.

Quick Start Guide for Administrators

Send Digests on These Days:

Mon Tue Wed Thu Fri Sat Sun

Send to this address:

Skip Empty Digests?

Do not send empty digests

Time of Day

Users may receive up to three digests on each day selected above:

1st: 2nd: 3rd:

Please note that times are approximate. Digests generally will be sent within 30 minutes of the time(s) specified above.

Highly Recommended – Blocking spam sent to bogus email addresses

Because a large percentage of junk mail is sent to email addresses that do not actually exist – i.e. **aaa@yourcompany.com, aab@yourcompany.com**, etc. – this can put unnecessary strain on your network and your mail server by forcing it to process unwanted junk.

Once you have entered all the valid email addresses – and aliases – for your domain, GFI MAX MailProtection should be configured to not accept messages sent to invalid email addresses at your domain. The GFI MAX MailProtection servers will simply block these messages before they reach your network. To enable this feature, navigate to Management > Inbound Filtering > Spam

Quick Start Guide for Administrators

Mail Sent to Unknown Recipients

What should be done with messages sent to user accounts that do not exist on your email server?

- BLOCKED: rejected during SMTP conversation
- DROPPED SILENTLY: accepted during SMTP conversation then silently deleted
- PASSED THROUGH: all messages to unknown addresses will be delivered (unfiltered) to the customer mail server
- USE DOMAIN: all messages to unknown addresses will be filtered and delivered to the customer mail server

Save Changes

Handling Settings, then click the “Unknown Users” tab under that section.

1. **BLOCKED:** If this option is selected, any messages sent to email addresses not listed in GFI MAX MailProtection will be rejected with a delivery failure notice. **This is the recommended option.**
2. **DROPPED SILENTLY:** If this option is selected, any messages sent to unknown email addresses will be accepted and then silently deleted. The sender will NOT be notified of the message’s failure.
3. **PASSED THROUGH UNFILTERED:** This should only be used if you have not entered all your email addresses and aliases into GFI MAX MailProtection. Any messages sent to unknown email addresses will be passed on to your mail server, without queuing or filtering.

Quick Start Guide for Administrators

Step 3: Specifying your mail server

Before the filtering is enabled, GFI MAX MailProtection needs to know where to deliver incoming mail for your domain. This is specified by clicking on the Management tab, then clicking on Inbound Filtering, and then on the Mail Delivery link at the left. The destination mail server can be in the form of a hostname, such as mail.yourdomain.com, or it can be an IP address such as 1.2.3.4.

If you have multiple mail servers or multiple IP addresses for your mail server, you can configure GFI MAX MailProtection to load balance between those servers or to deliver to a back-up mail server if the primary mail server is not reachable.

If your mail server or anti-spam solution uses SPF (as may be true with the GFI MailEssentials™/GFI MailSecurity™ software products) be sure to enable the checkbox for SPF.

Mail Delivery Settings

Destination Mail Servers SPF

Destination Mail Servers

In addition to specifying one or more primary mail servers, you may also specify a set of one or more backup mail servers below.

Specify Primary Mail Server(s)

SERVER	IP ADDRESS OR SERVER NAME	PORT	LOAD %
Primary #1	71.127.117.224	25	100 %

[Show more primary servers](#)

TOTAL LOAD: 100 %

Specify one or more **backup mail servers** in addition to the primary server(s) listed above

[Save Changes](#)

Quick Start Guide for Administrators

Step 4: Activating your account

To begin filtering, all that is necessary is a change in the “MX” records for your domain. The MX records are part of your domain’s DNS information, and are responsible for directing incoming email. By making this change, you are enabling the GFI MAX MailProtection systems to filter your inbound email for spam and viruses before those messages are routed to your mail server.

Typically, your DNS records are maintained by your ISP or hosting provider, and they should be able to make this change for you. Some customers have access to a web-based control panel through which the change can be made.

In most cases the new MX records for your domain will look similar to this:

```
yourcompany.com. IN MX 10 yourcompany.com.pri-mx.smtproutes.com.
```

```
yourcompany.com. IN MX 90 yourcompany.com.bak-mx.smtproutes.com.
```

Your GFI MAX MailProtection account representative or authorized GFI MAX MailProtection Partner will provide you with the new MX entries. **Please note that unless instructed otherwise, you should not update any “A” records in your DNS – the only changes that should be made are the replacement of your previous “MX” entries with the new ones for GFI MAX MailProtection.**

After this change has been made, your email will be automatically filtered through GFI MAX MailProtection before being delivered to your mail server. The filtering usually starts within a few minutes of the DNS change, though in some cases it can take up to a day or two for the change to take full effect.

If you have any questions or would like any assistance with changing your MX entries, please don’t hesitate to contact your GFI MAX MailProtection account representative or authorized GFI MAX Mail Services Partner.

We hope that you have found this Quick Start Guide useful. Again, thank you for choosing GFI MAX MailProtection and we look forward to being of service!