

Syntax To sort alphabetically: `<input type=hidden name="sort" value="alphabetic">`. To sort by a set field order: `<input type=hidden name="sort" value="order:name1,name2,etc...">`

redirect

If you wish to redirect the user to a different URL, rather than having them see the default response to the form, you may use this hidden variable to send them to another webpage.

Syntax To choose the URL the user will redirected to: `<input type=hidden name="redirect" value="http://your.address/file.html">`. To allow the user to specify a URL he wishes to travel to once the form is filled out: `<input type=text name="redirect">`

require

You can require that users fill in certain fields before the user can successfully submit the form. Simply place all field names that you want to be mandatory into this field. If the required fields are not filled in, the user will be notified that information is missing, and a link back to the form they just submitted will be provided.

Syntax If you want to require that the user fill in the email and phone fields in your form, so that you can reach them once you have received the mail, use a syntax similar to: `<input type=hidden name="required" value="email,phone">`

env_report

You may include environment variables in the email message you receive after a user has filled out your form. This is useful if you wish to know what browser they were using, what domain they were coming from, or any other attributes associated with environment variables. The following is a short list of environment variables you may find useful:

- REMOTE_HOST sends the hostname making a request.
- REMOTE_ADDR sends the IP address of the remote host making the request.
- HTTP_USER_AGENT is the browser the client is using to send the request.

Syntax If you wanted to find the remote host and browser sending the request, you would put the following into your form: `<input type=hidden name="env_report" value="REMOTE_HOST,HTTP_USER_AGENT">`

title

This form field allows you to specify the title and header that will appear on the resulting page if you do not specify a redirect URL.

Syntax If you wanted a title of Feedback Form Results: `<input type=hidden name="title" value="Feedback Form Results">`

return_link_url

This field allows you to specify a URL that will appear on the report page. This field will not be used if you have the redirect field set, but it is useful if you allow the user to receive the report on the following page, but want to offer them a way to get back to your main page. You may set the text of the link in the return_link_title field.

Syntax `<input type=hidden name="return_link_url" value="http://your.host.xxx/main.html">`

return_link_title

This is the title that will be used to link the user back to the page you specify with return_link_url. The two fields will be shown on the resulting form page as: ` return_link_title `

Syntax `<input type=hidden name="return_link_title" value="Back to Main Page">`

background

This form field allows you to specify a background image that will appear if you do not have the redirect field set. This image will appear as the background of the form results page.

Syntax `<input type=hidden name="background" value="http://your.host.xxx/image.gif">`

bgcolor

This form field allows you to specify a background color for the form results page in much the way you specify a background image.

Syntax For a background color of white: `<input type=hidden name="bgcolor" value="#FFFFFF">`

text_color

This field works in the same way as bgcolor, except that it will change the color of your text.

Syntax For a text color of black: `<input type=hidden name="text_color" value="#000000">`

link_color

This field changes the color of links on the result page and works in the same way as text_color. If redirect is defined, then this link will have no effect.

Syntax For a link color of red: `<input type=hidden name="link_color" value="#FF0000">`

vlink_color

This field changes the color of visited links on the result page and works in the same way as text_color. If redirect is defined, then this link will have no effect.

Syntax For a visited link color of blue: `<input type=hidden name="vlink_color" value="#0000FF">`

alink_color

This field changes the color of active links on the result page and works in the same way as text_color. If redirect is defined, then this link will have no effect.

Syntax Note: For a visited link color of blue: `<input type=hidden name="alink_color" value="#0000FF">`

Example .FormMail.conf File:

```
#### NMS Secure FormMail v2.20 2002/11/21 (Release 1.0)
####
#### *Configuration File*
#### If any values are not set properly, FormMail WILL NOT work.
####
#### Save this file in your home directory (/home/username/) named '.FormMail.conf'
####
# Set this to '1' if you receive any errors. They will
# Be displayed to the browser in a more verbose manner.
[DEBUGGING]
0
[/DEBUGGING]
# This address will receive bounced messages if any of the emails
# cannot be delivered, and should be set to your email address.
#
[postmaster]
you@yourdomain.com
[/postmaster]
# A list of the email addresses that formmail can send
# email to. The elements of this list can be either
# simple email addresses (like 'you@your.domain') or
# domain names (like 'your.domain'). If it's a domain
# name then *any* address at the domain will be allowed.
#
# Also see NOTE below for aliases.
#
# NOTE: One address/domain per line
```

```

#
[allow_mail_to]
yourdomain.com
you@yahoo.com
[/allow_mail_to]
# A hash for predefining a list of recipients in the
# script, and then choosing between them using the
# recipient form field, while keeping all the email
# addresses out of the HTML so that they don't get
# collected by address harvesters and sent junk email.
#
# For example, suppose you have three forms on your
# site, and you want each to submit to a different email
# address and you want to keep the addresses hidden.
#
# In the HTML form that should submit to the recipient
# 'me@mydomain.com', you would then set the recipient
# with:
#
# <input type="hidden" name="recipient" value="me" />
#
# NOTE: If an alias is set for any email address, then it is
# not required to be in the [allow_mail_to] block, it
# is automatically allowed.
#
# NOTE: One alias per line.
#
[recipient_alias]
me=>you@yourdomain.com
him=>you@yaoo.com,you@hotmail.com
[/recipient_alias]
# If this flag is set to 1 then an additional email
# will be sent to the person who submitted the
# form.
#
# CAUTION: with this feature turned on it's
# possible for someone to put someone else's email
# address in the form and submit it 5000 times,
# causing this script to send a flood of email to a
# third party. This third party is likely to blame
# you for the email flood attack.
#
[send_confirmation_mail]
0
[/send_confirmation_mail]
# The header and body of the confirmation email
# sent to the person who submits the form, if the
# [send_confirmation_mail] flag is set. In the
# example below, everything between the lines:
#
#     [confirmation_text]
# and
#     [/confirmation_text]
#
# is treated as part of the email.

# !!IMPORTANT!!
# Everything before the first blank line is taken as part of
# the email header, and everything after the first

```

```
# blank line is the body of the email.
[confirmation_text]
From: you@yourdomain.com
Subject: Your Form Submission
Thank you for your submission.
[/confirmation_text]
# The Cascading Style Sheet (CSS) used for the 'thank you' page
# if a redirect is not used. This is an absolute URL.
#
# i.e. /css/site.css would be http://yourdomain.com/css/site.css
#
# This may be left blank.
#
[style]
css/site.css
[/style]
# The Character set used for parsing form data and for the resulting
# 'Thank You' page after form submission.
#
# This may be left blank.
#
[charset]
iso-8859-1
[/charset]
```

Chapter 12: SpamGuard

Feature Overview

SpamGuard assists you in dealing with emails you do not wish to receive, namely spam. Spam is the digital equivalent of *junk mail*, that is, unsolicited email sent to a large number to addresses, generally for the purpose of advertising.

To access SpamGuard for installation purposes:

Click the SpamGuard icon in your Control Panel.



To access SpamGuard for management purposes:

- 1 Click the Mail Manager icon in your Control Panel
- 2 Click the SpamGuard link in the left menu.

Installing SpamGuard

The first time you click on the SpamGuard icon, you will be informed that SpamGuard has not be installed on your domain.

To enable SpamGuard:

Click Enable SpamGuard. You will see a confirmation screen asking you to wait 10 minutes.

You will now be able to go to your Mail Manager and configure SpamGuard.

Turn On SpamGuard

When this option is checked, the rules for blocked and spam e-mails are activated. Make sure to click Save Settings after you make the change.

Blocked E-mails

Based on the rules below, the program will take e-mails that contain words that you indicate as unwanted, and either delete the e-mails or store them in the blocked mails file.

Block E-mail address

Enter an e-mail address, click on Add Block, and then click Save Settings to add that e-mail address to the list of Blocked Addresses.

Blocked addresses

Any e-mail from an e-mail address in this list will be blocked. Select one or more of the addresses, click on Remove Block, and then click on Save Settings to remove them from the list.

Block words

Enter a single word, click on Add Block, and then click on Save Settings to add that word to the list of Blocked Words. If there is an occurrence of any word on this list in an e-mail, then that e-mail will be blocked. Select one or more of the words, click on Remove Block, and then click on Save Settings to remove them from the list.

Note: Entering sport will only block sport as a standalone word, and will not block words such as transportation.

Blocked mails will be stored to file

If you want blocked e-mails to be deleted, then leave this field blank. To empty the contents of the file, click on the Empty link.

Note: To delete all blocked e-mails, you need to make sure this field is blank, not merely empty the file of its contents.

If you do not want blocked e-mails to be deleted, enter a filename in the field. You may also indicate the directory in which this file will be stored. The directories and filename must be made up of alphanumeric characters, the underscore, or the dash. No other special characters can be used, e.g., the period. Once you make the change, make sure to click on Save Settings. Valid Examples: blocked_mail, mail/blocked_mail. Invalid Examples: domain-mail/blocked_mail.txt, mail/blocked.txt.

Note: You can store e-mails that the program has blocked to your -mail directory, and then create a user in your mail manager that matches the name of the 'blocked mails' file. This will allow you to retrieve an e-mail that you know is not spam.

Spam E-mails

The program will determine whether an e-mail is spam based upon a scoring system that uses the lists of Spam and non-spam words. The more spam words in an e-mail, the greater potential for the program to mark the e-mail as Spam. Conversely, the more non-

spam words in an e-mail, the greater potential for the program to not mark an e-mail as spam.

To add to either the spam words or non-spam words list, type phrases into the appropriate text box. The program will consider each line in the text box as a phrase. Then click on Save Settings. For example, if you enter 'God is great' on one of the lines, the program will search for every instance of 'God is great' in an e-mail and not just for a single instance of any of those words. For example, if an e-mail had 'God is awesome', the program will not take that phrase into consideration because it does not exactly match the phrase, 'God is great'.

Execute SpamGuard Command

SPAM If you already have a file with spam e-mails, choose SPAM from the drop down menu, enter the filename to the right, and then click on Save Settings. This will teach SpamGuard which e-mails it should consider as Spam.

GOOD If you have a file with good e-mails, choose GOOD from the drop down menu, enter the filename to the right, and then click on Save Settings. This will teach SpamGuard which e-mails it should consider as non-spam.

REMOVE If SpamGuard is marking a good e-mail as spam, then create a file with that good e-mail, choose REMOVE from the drop down menu, enter the filename to the right, and then click on Save Settings. This will remove that e-mail from the database of e-mails that SpamGuard considers to be spam. Spam mails will be stored to file. All e-mails the program marks as spam will be stored in the file listed here

You can also indicate the directories that these files will be placed in. The directories and filename must be made up of alphabetic characters, the underscore, or the dash. No other special character can be used, e.g., the period. Once you make the change, click on Save Settings. Valid Examples: spam_mail, mail/spam-mail. Invalid Examples: domain-mail/spam_mail.txt, mail/spam.txt.

Note: You can store e-mails that the program has determined to be spam to your -mail directory, and then create a user in your mail manager that matches the name of the spam mails' file. This will allow you to retrieve an e-mail that you know is not spam. To empty the contents of the file, click the Empty link.

Secure Mail Manager

Overview

Secure Mail will allow you to send emails more securely, if you have installed a secure certificate. You must install a secure certificate to use Secure Mail.

The internet is not a secure medium for sending information, unless the information is sent over a secure server. Normally, any text (such as your credit card number) sent from a user's browser to your server is sent as plain text. This means that someone could potentially intercept the information and read it. A secure server encrypts the information before it leaves users' browsers, so that even if data is intercepted, it's useless.

Once Secure Mail is enabled, you can use form mail to embed forms on secure pages, so that your users can send you information without worrying about interception by malicious persons.

To access the Secure Mail Manager:

Click the Secure Mail icon in the Control Panel.



To enable secure mail:

Once you have a secure certificate installed, click Enable Secure Mail. A confirmation will be displayed, stating that your request will be processed within ten (10) minutes.

To test secure mail:

Click Test Secure Mail. The system will run a test of Secure Mail and if it is successful, you will receive a confirmation.

Sending Secure Mail

From your website, make sure that the link to the page the form is in is created with a full path that includes `https://`. For example, to access a page called `mail.html`, you would have to link to `https://<domain>/mail.html`, NOT `http://<domain>/mail.html`, or simply `mail.html`. You will use `https://` again in your form call.

Your code will look similar to the following:

```
<form method="post" action=https://<server>/<domain>/cgi-bin/formmail.pl>
```

```
<input type="hidden" name="recipient" value = "<user>@<domain>">
<input type="hidden" name="subject" value="whatever">
<input type="hidden" name="return_link_URL" value=https://<server>/<domain>/
yourpage.html>
<input type="hidden" name="return_link_title" value="Back to your Page">
</form>
```

In the code above, `<server>` represents the name of the server your domain rests on. You were given this information when you received your account setup information. `<domain>` is the full name of your domain.

You may include any of the other fields normally used with form mail.

Chapter 14: Quaranteen

Feature Overview

Quaranteen Manager aids in detecting and taking care of any virus that may affect your domains. It can also be set up to filter all emails containing attachments with certain extensions. Quaranteen is configured through the Mail Manager.

To access Quaranteen (to enable):

Click the Quaranteen icon in your Control Panel.



To access Quaranteen (after installation):

Click the Mail Manger icon in your Control Panel.

Enabling Quaranteen

If Quaranteen is not yet installed on your domain, you will have to enable it to access its anti-virus features.

To enable Quaranteen:

Click Enable Quaranteen. You will receive a message confirming that your request will be processed within ten (10) minutes.

You will be able to now go into your Mail Manager and configure Quaranteen. The following help notes will be listed on the page that appeared when you enabled Quaranteen.

Configuring Quaranteen

Turn On Quaranteen When Turn On Quaranteen is checked, one of four things will happen to an email.

- If the email has an attachment that could be executed on Windows, then the program will rename the attachment. This email will arrive at its regular destination.
- If the name of an attachment matches the name of a very well known virus in the virus database, then the attachment will be renamed and the email will be placed in the Emails with known issues file.
- The *Blocked extensions* feature explained below will be activated.

- If the email does not match any of the conditions above, then the email will remain unchanged and will arrive at its regular destination.

Note: After reviewing the attachment and deeming it safe, you may rename the file to its former name to run it.

Note: To change the setting, check or uncheck, and then click Save Settings.

Enter extensions of attachments to be blocked (For example: exe, doc) Enter a filename extension, click Add Blocked, and then click Save Settings to add that extension to the **Blocked Extensions** list.

Blocked extensions Any email with an attachment that ends in an extension listed here will be stored in the Emails with known issues file and a warning will be sent to the administrator's email address. Select one or more of the extensions, click on Remove Block, and then click on Save Settings to remove them from the list.

Enter administrator's email address When the program determines that an email is problematic, it will send a warning message to this address.

Emails with known issues will be stored to file When the program determines that an email is problematic, it will store that email in this file. To change the name of the file, you need to highlight the text in the field, enter the new filename, and then click on Save Settings. You can also indicate directories. The directories and filename must be made up of alpha characters, the underscore, or the dash. No other special character can be used, e.g., the period. Once you make the change, make sure to click on Save Settings. Valid Examples: *virus_mail*, *mail/virus_mail*. Invalid Examples: *domain-mail/virus_mail.txt*, *mail/virus.txt*. To empty the contents of the file, click on the Empty link.

Note: You can store e-mails that the program has determined to be problematic to your -mail directory, and then create a user in your mail manager that matches the name of the Emails with known issues file. This will allow you to retrieve an email that you know is not problematic.

Select security level Select the level of tolerance the program uses to determine whether an email is problematic. To change this, click on the menu, select the level, and then click on Save Settings. Please note that this program does not offer full virus protection. For protection against viruses, it will be necessary to acquire a virus protection program for your mail client.