

# **i-MailDS NoSpam Users Guide**

© Digital Integration Ltd / IO Software Ltd 2003

Information in this document is subject to change without notice. No portion of this document may be reproduced, stored or transmitted in any form or by any means without the express written permission of the copyright holders.

<b>SYSTEM REQUIREMENTS</b> .....	<b>3</b>
<b>ENABLING NOSPAM</b> .....	<b>3</b>
<b>UPDATING RULES</b> .....	<b>4</b>
<b>NOSPAM CONFIGURATION FILES</b> .....	<b>4</b>
<b>CREATING CUSTOM RULES</b> .....	<b>5</b>
<b>ANALYZING MAIL</b> .....	<b>6</b>

## **System Requirements**

NoSpam for i-MailDS is a complex system and has fairly high resource requirements to run. It is important that your system has the capacity to handle NoSpam prior to using it, as you may starve your server of system resources and in turn potentially cause the server to crash. If your server is near the limits of the system requirements it is recommended that you test loading when no one is logged in to your server.

By itself, NoSpam has little requirements, all the overhead comes from the complexity of the rules.

The default set of rules provided with i-MailDS requires approximately 100Mb of free memory during loading, and will settle down to require about 30Mb one running. Reloading the rules requires the load time memory again, so a total of 130Mb free memory is typically required. So to make it clear for those who don't read the full manual:

Memory Required: 130Mb

Adding or removing rules, and their inherent complexity will change this figure up or down.

## **Enabling NoSpam**

NoSpam is enabled within the i-MailDS administration tool. The setup can be found on the 'services/security' tab by hitting the 'Antispam' button. i-MailDS will autoload the NoSpam NLM when it is enabled.

NoSpam can take some time to start, so be patient while it loads. Our test server has a Pentium 4 chip running at 1.5Ghz and is dedicated to this task. With the default rules it takes approximately 3 minutes to load.

During the rule load time your server will also come under a fairly excessive load and the server may report that NoSpam is not relinquishing control. This is by design to get the system up and running in a timely fashion. Once loaded, the rules do not affect system performance.

## Updating Rules

After modifying, updating or installing new NoSpam rules the i-MailDS server needs to be prompted to reload the new rule set. This can be done in one of three ways.

In the i-MailDS admin antispam page press the 'Reload Rules' button.  
At the i-MailDS server console, press 'CTRL-A'.  
Unload and reload i-MailDS

## NoSpam Configuration Files

NoSpam is configured with rule files which are located in the spamcfg directory under the imail\config directory.

There are two file types that NoSpam recognises as containing rules - \*.cf and \*.cfg - in that order.

The default rules provided with i-MailDS are contained in the \*.cf files, and these should generally not be modified.

User rules should be placed in \*.cfg files for several reasons. Firstly NoSpam reads \*.cf files followed by \*.cfg files. Any duplicate rules found in \*.cfg rule files will override rules from the \*.cf files. This is the suggested method of removing, or changing default rules, as user based changes will be retained even after a default ruleset update.

By maintaining user defined rules in \*.cfg files it also makes it easy to distinguish user defined rules from the default set.

## Creating Custom Rules

In the war against spam it is very difficult to get a perfect solution, as new spam is defined every day, and spammers are continually building new and different ways to get their messages to you.

NoSpam, however good it may be, is not infallible and will require your input to continue catching spam.

When a message bypasses the antispam system, a rule can be written to detect future messages of its type.

To do this, firstly create a rule file in the `imail\config\spamcfg` directory. The rule file needs a `.cfg` extension, such as `MyRules.cfg`.

A full explanation of how rules are defined can be found in the rule writing guide.

Rules within a configuration file are defined by three entries, the rule, a description and a score. These can be defined anywhere within the config files and each component can be stored in different files, however for basic custom rules it is easiest to place these items together.

Here are a couple of examples of custom rules. Note that a score of 100 has been used. Custom rules built to definitively prevent mail should have a score of at least 100 as this forces an extreme score that will cause the NoSpam engine to tag the message as spam based on the default score limit of 5. It also makes finding problem rules easy as they have a clearly defined large score.

```
body      CATCH_VIAGRA  /viagra/i
describe  CATCH_VIAGRA  Catch the word viagra in the message body
score     CATCH_VIAGRA  100

subject   SAVE_MONEY   /save (hundreds|thousands)/i
describe  SAVE_MONEY   Spam suggesting we can save a lot of money
score     SAVE_MONEY   100
```

## Analyzing Mail

At times, spam will get past the NoSpam scanner, and there may be the chance that non-spam may get caught if it appears spammy (these are termed false positives).

To determine how the NoSpam system scored a message it can be forwarded to one of two a special e-mail address inside your i-MailDS server for analysis.

The addresses are 'spamalyze' and 'spamalyzeattached' and these are at your local domain. Your i-MailDS server will only respond to this address if the sender is from a local domain.

If your primary domain was defined as company.com, then you would send your message to 'spamalyze@company.com'.

To get a straight analysis of a message, typically to test if a custom rule is working, send a message to 'spamalyze@company.com'.

To analyze a message that is in your mailbox, forward the message to 'spamalyzeattached@company.com' and the server will detach the forwarded message and analyze it in its original form.

After analysis you will be returned a message detailing all the rules that fired, their respective scores and the total score of the message. Use this information to determine new rules and any changes that you might deem necessary to existing rules and scores.