

MailWarden Pro

Technical FAQ

Disclaimer:

The information contained within this document is provided "as-is," "as available," and all warranties, express or implied, are disclaimed (including but not limited to the disclaimer of any implied warranties of merchantability and fitness for a particular purpose). While every reasonable effort has been made to provide accurate information, the information may contain errors, problems or other limitations. our sole and entire maximum liability for any inaccurate information, for any reason, and user's sole and exclusive remedy for any cause whatsoever, shall be limited to the amount paid by the customer for the information received (if any). we are not liable for any indirect, special, incidental, or consequential damages (including damages for loss of business, loss of profits, litigation, or the like). whether based on breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damage. the limitations of damages set forth above are fundamental elements of the basis of the bargain between us and you. No representations, warranties or guarantees whatsoever are made as to the accuracy, adequacy, reliability, currentness, completeness, suitability or applicability of the information to a particular situation. All information contained within this document is subject to change without notice

MailWarden Pro FAQs

How does MailWarden Pro deter Spam from entering a network?

MailWarden Pro is designed as a messaging firewall and filters the entire message. MailWarden Pro employs state of the art real time technology to ensure that spam is identified before it enters your email server. This technology protects you from both current and emerging spam techniques.

Our Global Service Centre Anti-Spam technology:

Filtration based on real-time spamming information protects you from spamming by filtering messages based on real-time spamming data. Through our Global Service Centre MailWarden Pro can identify spam outbreaks by monitoring spam as it originates around the world, in any language, and in real time. This detection of a spam attack takes place long before the individual spam message reaches MailWarden Pro. When it does reach your MailWarden Pro server, a quick lookup against our Global Service Centre databases will quickly confirm the message as being Spam or not, and MailWarden Pro can reject or quarantine these suspect messages, based on your preferences.

This technology is content, geography, and language neutral and so can protect you from the next new wave of spam messaging without intervention.

I want to stop my spam, but am concerned about also stopping good emails. How does MailWarden Pro protect me from these false positives?

Because our Global Service Centre is detecting spam attacks from multiple locations around the globe in real time, the only messages that are confirmed to be spam are ones that have been seen to have wide distributions with un-solicited content. This is independent of content and so is not prone to the errors that rules based and probabilistic systems make. Only genuine spam messages are stopped.

Can MailWarden Pro do the work of a traditional content filter?

Yes. As well as having the most sophisticated anti-spam technology available, MailWarden Pro also has a traditional rules based engine allowing you to configure a wide variety of content based rules to suit your companies own unique content policy. These rules can be configured to filter messages based on combinations of key words, phrases, and attachment types, or can also filter email messages based on email addresses, domains, and originating IP addresses. MailWarden Pro can reject, redirect or quarantine these messages.

Do I have to install MailWarden Pro on my Email Server?

No. MailWarden Pro does not need to be installed on the email server. It can be installed onto any PC that has connectivity to the email server. For further information on how to install MailWarden Pro, please download the MailWarden Pro installation guide (www.seattlelab.com).

How is MailWarden Pro licensed?

MailWarden Pro is licensed based on the number of email users that you have. The anti-spam and anti-virus features can be purchased through annual subscription and will be licensed individually.

I have more than one email server. Do I need to install MailWarden Pro on each server in my company?

No. Typically a company will only require one MailWarden Pro installation, which can cover many servers, and even multiple domains.

I am concerned about the performance of my email server(s). Will installing MailWarden Pro decrease their performance?

With extremely high volumes of email you may notice a fall off in performance on the server that is running the MailWarden Pro application (not necessarily the email server). If mail volumes are high we recommend that you install MailWarden Pro on a dedicated PC. Remember, because MailWarden Pro is stopping your spam, it is relieving your email server of a very large burden. Installing MailWarden Pro will for most companies have a very positive effect on the performance of the email server.

What does 'quarantine' mean and why is it a critical feature in MailWarden Pro?

Even though MailWarden Pro protects you against false positives, don't take our word for it. By implementing a quarantine you are giving yourself the option to review and audit effectiveness, release email that you may wish to keep and set rules for Black and White lists. MailWarden Pro can automatically clear out the quarantine for you after 'n' days, further relieving the maintenance and administration burden.

Why does my MailWarden Pro need to connect to the Internet?

The intelligent anti-spam feature in MailWarden Pro needs to connect to the internet in order to cross-check potential spam emails with the spam databases in our Global Service Centre. This feature ensures that MailWarden Pro can identify spam emails that it has not encountered before. In this way, MailWarden Pro can take the preventative action of quarantining new and emerging spam messages before they infiltrate the email system.

Will I need to change my rules for changing spam techniques?

No. MailWarden Pro has an intelligent anti-spam feature that ensures that new spam techniques are quickly identified, in fact this is done in real time as they happen. This ensures that MailWarden Pro will adapt automatically to changing spam patterns without any need for operator intervention.

Can I install this version over my previous installation?

Yes. MailWarden Pro can be installed over any previous installation of MailWarden Pro. See the SeattleLab website for upgrade instructions (www.seattlelab.com).

I already have a content filter, can I run the MailWarden Pro Evaluation without removing my current system?

Yes. MailWarden Pro can run silently alongside any content filtering system that you have in place. Additionally, MailWarden Pro brings the increased protection of intelligent anti-spamming.

What happens at the end of the evaluation period?

At the end of the evaluation period, MailWarden Pro automatically stops interrogating emails for spam and virus content. There is no disruption to the email service - it will simply be less effective as a result of not having the MailWarden Pro features enabled. If you upgrade to a full purchase MailWarden Pro licence, all of the features will be immediately activated without the loss of any of the configuration changes that were carried out as part of the evaluation.

Where are quarantined messages kept?

There are two different types of quarantined messages. There are the message files that are quarantined by the *Rules* queries and message files that are captured by the *Virus Control* portion of MailWarden Pro.

The messages that are quarantined by the *Rules* are kept in the `\Program Files\Mail Warden Pro\Quar` directory.

Messages quarantined by the *Virus Control* component are kept in the `\Program Files\Mail Warden Pro\Infected` directory.

Can I do bulk reference/deletion from the quarantine?

Yes. It is possible to sort the MailWarden Pro quarantine based on a wide variety of fields, for example, source of email, date of email, type of message – even the subject of the message. Once sorted, a bulk action may be applied to any group of messages – for example, a bulk deletion. You can even have MailWarden Pro automatically clear out quarantine entries that are over 'N' days old.

How do I update my Virus definitions?

Open the MailWarden Pro Configuration applet and select the *Virus Control* tab. Select the *Check for Updates Now* button (at the bottom of the applet window). The Norman Internet Update will start. If there are updates to the virus definitions they will be downloaded and added to the configuration.

Can I set the Virus definition update to happen automatically?

Yes, open the MailWarden Pro Configuration applet and select the *Virus Control* tab. Select the *Configure Update Mode* button (at the bottom of the applet window). The Configuration Editor will start. Select the *Update Mode* tab in the Configuration Editor and select the desired update mode (daily, weekly, etc.).

What if I already have Virus Control software on my system?

In order to install MailWarden Pro you must disable all other anti-virus software (until the installation is complete). After installation you must prevent your existing anti-virus software from scanning the following MailWarden Pro (\Program Files\Mail Warden\...) directories: In, Out, System, Infected.

Note: These directories are excluded by the MailWarden Pro Virus Control by default.

Once the installation is complete and the directory exclusions have been added to your existing anti-virus software, you may enable the software.

If someone sends a zip file that is password protected, will my Virus Control detect it?

If you receive a password protected Zip file as an attachment in an email, the virus control is set to quarantine this immediately.

What RBL Service Provider should my company use?

There is an extensive choice in RBL filters. Many are free and have varying levels of aggressiveness. For this reason, we have provided a link to a widely known website that tests many RBL filters on a monthly basis for comparison. We encourage you to learn about their blocking philosophy to determine which one fits your corporate philosophy the best before implementing one.

<http://www.declude.com/junkmail/support/ip4r.htm>

<http://www.sdsc.edu/~jeff/spam/cbc.html>