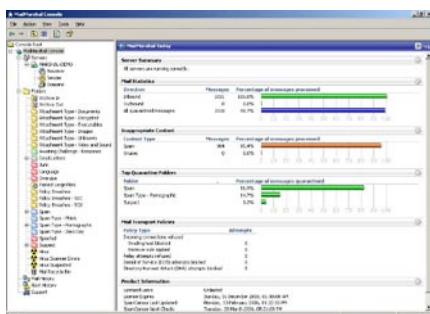


WHAT'S NEW AND COOL?

# MailMarshal SMTP 2006

Marshal is pleased to announce the release of MailMarshal SMTP 2006. This latest release offers important new security features - providing convenience and enhanced protection against email threats.

MailMarshal SMTP 2006 delivers a range of new security enhancements designed to protect your organization against current and future email threats. Whether your concerns are managing spam, phishing exploits, or direct attacks on your email network, MailMarshal SMTP 2006 is the ideal solution – protecting more than 7 million users around the globe.



Updated look & feel for the MailMarshal SMTP 2006 Console.



MailMarshal SMTP 2006 Configurator is clear and makes defining your policies easy

## NEW FEATURES IN MAILMARSHAL SMTP 2006:

- “Zero-Day” attack protection
- Denial of Service (DOS) gateway protection
- Directory Harvesting Attack (DHA) gateway protection
- Transport Layer Security (TLS) encryption support
- Spam categorization and reporting
- CountryCensor – anti-spam by country of origin
- URLCensor – anti-spam / anti-phishing using real-time URL lookups
- Support for Norman Anti-Virus ‘sandbox’ functionality
- HELO support for MailMarshal ESMTX Receiver Policies
- Additional reports; including new anti-spam categorization reports

## FEATURES AND BENEFITS EXPLAINED

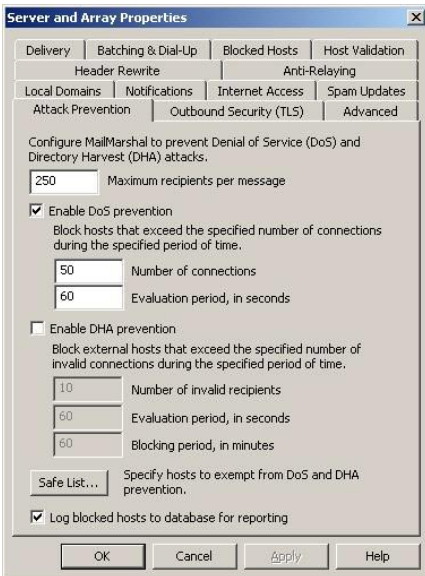
MailMarshal SMTP 2006 provides an impressive list of new features - but what do they actually mean for your business?

### SECURITY | Zero-Day Attack Protection

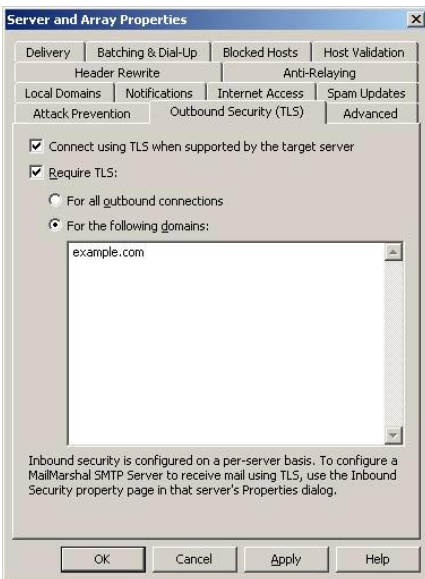
Zero Day protection allows Marshal to provide new security updates to your MailMarshal server(s) with same-day efficiency. When new email threats are detected by Marshal’s Threat Team, Marshal can release “zero-day” updates to secure your MailMarshal SMTP 2006 server automatically. This not only provides rapid response security but reduces administration for your organization. Zero-Day attack protection is a key part of Marshal’s “set & forget” ethos – Marshal can identify new spam, virus or other email exploits and ensure that your email network remains secure and protected.



## WHITEPAPER - MailMarshal 6.0 SMTP



DOS and DHA Gateway Protection are easy to configure under server properties.



TLS Encryption involves a simple configuration from the server properties tab.

### SECURITY | DOS Gateway Protection

A Denial of Service (DOS) attack on an email server involves rapidly 'flooding' the server with continuous email connections. The end effect is that the email server is overwhelmed by the sheer volume of email connections. This results in your organization either experiencing dramatically reduced email service or being deprived of email altogether. Naturally, this can be catastrophic for many organizations that depend on email.

DOS Gateway Protection in MailMarshal SMTP 2006 is designed to look for unusual email activity that indicates a potential DOS attack, such as multiple, rapid connection attempts from a single IP address. MailMarshal SMTP 2006 then automatically escalates preventative measures depending on the nature of the anomalous activity. This can include throttling back response times or dropping the connection and blocking the offending IP address for a period. This provides your organization with substantial DOS protection. In the event that one of your customer's servers is commandeered by a spammer and your organization is attacked, MailMarshal SMTP 2006 will take steps to manage the attack. MailMarshal SMTP 2006 will then automatically resume normal service with your customer's email system, once the attack has passed.

### SECURITY | DHA Gateway Protection

A Directory Harvesting Attack (DHA) is a malicious activity usually employed by Spammers to 'harvest' valid email address from an email server. This can sometimes explain why a new email address may receive spam within days of being activated. DHAs involve a systematic approach, trying different combinations of email addresses to determine which addresses the target server considers valid or invalid. MailMarshal SMTP 2006 can detect the patterns of these systematic harvesting techniques and take appropriate action, including denying connections from the attacking server. This ultimately results in your organization being sent less spam and denying spammers access to your organizations valid email address list.

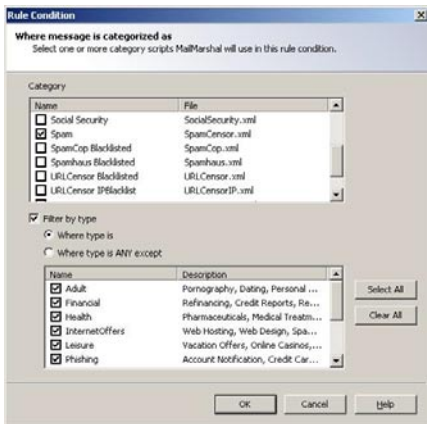
### SECURITY | TLS Encryption

Transport Layer Security is a method of email encryption that allows two servers to create a secure SMTP connection between them. TLS is effectively SSL for SMTP email connections and ensures that any communications between two TLS enabled servers remain private and confidential. TLS is easy and cost effective to establish, providing an ideal way for organizations to communicate securely.

### ANTI-SPAM | Spam Categories

MailMarshal SMTP 2006 can sort spam into related categories such as Adult, Health, Stocks, Financial and Phishing. This allows your organization to apply different polices to different types of spam. For example, you may choose to quarantine Health and Financial spam for your employees to manage directly via the SQM system (Spam Quarantine Management). Conversely, you may choose to delete Adult and Phishing spam automatically without exposing end users to such spam. Spam Categories also allow you to report on and analyze the types of spam that your organization receives. This may help you fine-tune your anti-spam polices to be more effective.

## WHAT'S NEW AND COOL? - MailMarshal SMTP 2006



Spam categories are very easy to use. Simply select them from within the SpamCensor policy wizard.

### ANTI-SPAM | CountryCensor

MailMarshal SMTP 2006 employs a multi-faceted approach to anti-spam, utilizing a range of technologies to analyze messages and identify spam and other threats. CountryCensor is one of the latest technologies available in MailMarshal SMTP 2006. CountryCensor identifies the country that an email message has originated from allowing you to apply whatever policy you desire. For example, your business may be entirely locally focused, only dealing with suppliers and customers from within your own country. As a result, you may choose to simply deny any email message that does not originate from within your own country. Another use may be to apply different policies to messages from different countries, such as making anti-spam rules more stringent for emails that originate from some countries than from others. CountryCensor also allows you to classify, and then report on, which countries you receive email from and monitor changes in those trends over time.

### ANTI-SPAM, ANTI-PHISHING | URLEncisor

As with CountryCensor, URLEncisor is another method that MailMarshal SMTP 2006 uses to examine email messages and determine any potential security risk. URLEncisor specifically examines URLs that may be included in an email and references them against a real-time blacklist of known spam and phishing web sites. These real-time blacklists or RBLs are maintained by independent 3rd parties. MailMarshal SMTP 2006 can be configured to utilize more than one RBL, making for improved accuracy and security. If a message contains a URL that is listed on a RBL, MailMarshal SMTP 2006 can quarantine the message automatically.

### ANTI-VIRUS | Norman Sandbox Support

Norman is a 3rd party anti-virus (AV) vendor (one of many that Marshal supports). Standard AV solutions use virus signature files that are created when a new virus appears in the wild. This requires that the AV solution is regularly updated to keep it current with the latest virus threats.

Norman's sandbox technology is specifically designed to identify potential viruses that have not been seen before. The concept is that if an unknown executable file type is encountered, the sandbox feature will place the file into a secured, safe environment and allow the file to execute. Norman then monitors the behavior of the file to determine whether or not it exhibits any potentially malicious characteristics. If the file's activity appears to be safe, it will allow the file to pass. If on the other hand, the file's activity appears to be malicious, it will treat it like a virus and take quarantine action.

The Norman Sandbox feature can not only detect viruses but also spyware applications or other malicious files. MailMarshal SMTP 2006 directly supports the Norman Sandbox feature, allowing you to scan email messages with unknown attachments in real-time. You can learn more about the sandbox technology at the Norman web site - <http://www.norman.com/Virus/Sandbox/en-us>

## WHAT'S NEW AND COOL? - MailMarshal SMTP 2006



HELO SMTP Receiver policies are configured from within MailMarshal's award winning Policy Wizard. As a rule condition, you simply select the options you desire and then apply them to your policy.

### SECURITY | HELO SMTP Receiver Support

MailMarshal SMTP 2006 has two general methods of applying security policies – Receiver Rules and Standard Rules. Standard Rules can apply a wide range of policies to email messages that have been received by MailMarshal. Receiver Rules are used to reject email messages before they are even received. For example, if you want to block messages that are bigger than a defined size limit, receiver rules can identify oversized messages when the sending server first tries to establish a connection. This ensures that your bandwidth is protected – the key reason for placing a size limit on messages in the first place.

HELO refers to the very first messages that are transferred between SMTP email servers when trying to establish a connection, before sending an email. HELO strings identify the email server and provide properties about that server and what it wants. HELO support can allow MailMarshal SMTP 2006 to force a connecting email gateway to adhere to the industry standard SMTP connection process. This may include requiring the connecting email gateway to provide a Fully Qualified Domain Name (FQDN). This process has benefits in blocking spam. Spammers do not normally adhere to the HELO standards, often failing to provide a FQDN. This means that MailMarshal SMTP 2006 can apply different policies to email servers that do not match the HELO standards, such as refusing connections altogether.

### UPGRADING

MailMarshal SMTP customers with current maintenance agreements may upgrade to MailMarshal SMTP 2006 at no additional charge. If you are using an earlier version, we recommend upgrading to take advantage of the new features and security benefits offered by MailMarshal SMTP 2006.

### TECHNICAL SUPPORT

The procedure for upgrading your MailMarshal server is documented in the official User Guide. If you require assistance during your upgrade (and you have a current maintenance agreement) please don't hesitate to contact your local Technical Support representative via our web site – [www.marshal.com](http://www.marshal.com)

If you have any suggestions or requests for our next version, we would love to hear them. Please let your technical support or sales representative know what you would like to see added.



Marshal's Worldwide and EMEA HQ  
Marshal Limited,  
Renaissance 2200,  
Basing View,  
Basingstoke,  
Hampshire RG21 4EQ  
United Kingdom

Phone: +44 (0) 1256 848080  
Fax: +44 (0) 1256 848060

Email: [emea.sales@marshal.com](mailto:emea.sales@marshal.com)

Americas  
Marshal Inc.  
5555 Glenridge Connector,  
Suite 200,  
Atlanta,  
GA 30342  
USA

Phone: +1 404 459 2890  
Fax: +1 404 759 2549

Email: [americas.sales@marshal.com](mailto:americas.sales@marshal.com)  
[info@marshal.com](mailto:info@marshal.com) | [www.marshal.com](http://www.marshal.com)

Asia-Pacific  
Marshal Software (NZ) Ltd  
Suite 1, Level 1, Building C  
Millennium Centre  
600 Great South Road  
Greenlane, Auckland  
New Zealand

Phone: +64 9 984 5700  
Fax: +64 9 984 5720

Email: [apac.sales@marshal.com](mailto:apac.sales@marshal.com)