

Mail Sentinel



The Mail Sentinel Anti-Spam subscription option and Anti-Virus feature filter emails through the GTA firewall email proxy to provide the first defense against spam and virus attacks at the network perimeter.

Mail Sentinel Key Features

Mail Sentinel Anti-Spam

- Detects and blocks spam in real time
- Delete, tag or quarantine email based on your spam category criteria
- Greylisting
- Blocks SMTP email spam
- Real-time spam blocking statistics
- Logging & reporting
- Automatic update of rules

Mail Sentinel Anti-Virus

- Detects and eliminates computer viruses in real time
- Scans incoming attachments for viruses
- Blocks SMTP email viruses
- Tag, quarantine or delete email identified as containing viruses
- Real-time virus blocking statistics
- Customizable parameters for handling email with recognized viruses
- Automatic update of virus definitions



Anti-Spam and Anti-Virus Protection for GTA Firewall UTM Appliances

If you use the Internet for communication today, you are likely flooded with spam and susceptible to viruses from email attachments. Spam and virus attacks are real world problems that every network administrator must deal with on a daily basis. If left unchecked, these threats can account for lost revenue by crippling your network, corrupting or even leaking valuable data. Lost productivity as employees sift through hundreds of emails to delete spam quickly reduces the bottom line profitability of any organization.

Mail Sentinel[®], a component of GTA's Gateway Sentinel suite of threat management products and services, addresses these issues at your network's perimeter. All GTA Firewall UTM Appliances come standard with Mail Sentinel's basic set of features which provide a foundation that gives you the tools to regain control of your email.

Powerful Standard Features

Mail Sentinel email proxy features provide a solid foundation that allows administrators to take control of unsolicited email by using fully customizable policies with allow and deny lists, reverse DNS lookups, and file size restrictions for basic spam blocking.

Policies based on IP Address, domain or email address can be created to customize Mail Sentinel email filtering for specific groups or departments. Establishment of MAPS policies utilizing RBL lists provides basic verification of email domains against servers known to distribute spam or virus emails. MAPS policies can be further enhanced with the addition of Allow or Deny lists for specific domain names. Allow and deny lists are easily implemented into Mail Sentinel settings to globally accept or deny connections from known email servers. Reverse DNS lookups are used to verify the identity of an email server, while file size restrictions can be used to prevent harmful email attachments. Mail Sentinel's basic features provide the settings required to create a flexible, yet powerful email solution.

Total Email Threat Management

The Mail Sentinel Anti-Virus feature and Mail Sentinel Anti-Spam subscription option build upon the capabilities of Mail Sentinel's basic feature set to help ward off malicious spam and viruses. Mail Sentinel Anti-Spam and Anti-Virus are used to add an additional layer of strong defense at the network's perimeter by implementing an extraordinary gateway-level solution.

GTA has integrated the 'best of breed' in anti-spam engines from technology leading Mailshell into Mail Sentinel's Anti-Spam subscription option. Mailshell's Anti-Spam with SpamCompiler AI™ technology compiles, optimizes, and executes over 300,000 checks in fractions of a second to determine whether or not a message is unsolicited spam.

Simple Configuration and Implementation

Mail Sentinel is fully integrated into GB-OS[®]. The Mail Sentinel email proxy is easily enabled with a single click. Once the Mail Sentinel proxy is enabled, simply create policies to accept or deny emails based on network and departmental needs.

There is never a need to purchase additional hardware or install cumbersome client-side software in order to activate and use Mail Sentinel Anti-Spam subscription option. Configuring the Mail Sentinel subscription option to meet your networking requirements is simple and fast. Network administrators will appreciate the powerful configuration options GB-OS provides in a user-friendly environment. The Mail Sentinel Anti-Spam subscription option is licensed on a per subscription basis to best meet the needs of SME businesses.

Mail Sentinel Anti-Spam Product Part Numbers (Annual Subscription)

Mail Sentinel Anti-Spam GB-250/e
Mail Sentinel Anti-Spam GB-820, GB-800/e
Mail Sentinel Anti-Spam GB-2100, GB-2000/e/x

ETAS00-0AR5-12M00
ETAS00-0AR6-12M00
ETAS00-0AS4-12M00

Mail Sentinel Anti-Spam Gb-2500, GB-3000
Mail Sentinel Anti-Spam GB-Ware Restricted
Mail Sentinel Anti-Spam GB-Ware Enterprise

ETAS00-0AF1-12M00
ETAS00-0SP2-12M00
ETAS00-0SP3-12M00

Mail Sentinel

System Requirements

- Mail Sentinel Anti-Spam is available on GTA systems operating GB-OS 3.6 or higher. GB-Ware requires a 512 MB flash card or hard disk.
- Mail Sentinel Anti-Virus is available on GTA firewall UTM systems operating GB-OS 5.1.2 or higher. GB-250 and GB-250e must be Rev B models. GB-Ware requires a 512 MB flash card or hard disk. See www.gta.com for specific product compatibility.

Option Availability

GB-3000	✓
GB-2500	✓
GB-2100	✓
GB-2000/GB-2000e/GB-2000X	✓
GB-800/GB-800e	✓
GB-250/GB-250e	✓
GB-Ware	✓

Contact your local GTA Channel Partner or GTA Sales for information on option availability for legacy products.

Free 30-Day Evaluation

GTA firewall owners may request a 30-day evaluation of Mail Sentinel, at no charge, via the GB-OS Web interface in version 5.1 (and above). Simply click on [Request Evaluation] in the Mail Sentinel header on the System Overview screen. 30-day evaluations are also available via the GTA Web site at:

www.gta.com/options

Mail Sentinel Anti-Spam Subscription Option

The Mail Sentinel Anti-Spam subscription option is a fully customizable, easy-to-use SMTP spam blocking solution. There is no additional software to install on your GTA Firewall UTM Appliance. Activation and configuration of the subscription option is a simple process.

Mail Sentinel Anti-Spam's greylisting settings offer enhanced email filtering before the email reaches the email server. Greylisting is designed to protect users from spammers that use "fire and forget" email applications, which are created to send spam messages, but never attempt to retry delivery if the first attempt fails. Greylisting significantly reduces the number of emails which are scanned by spam rules, so email processing is more efficient. With a two pronged attack on email, spam is virtually eliminated while legitimate email is efficiently processed and received at the user's inbox.

Mail Sentinel Anti-Spam is powered by MailShell Anti-Spam's Spam Recognition System. Each message is reviewed by four separate spam identification engines that utilize over 300,000 rules to identify unsolicited email. Mailshell's four spam identification engines check for a variety of characteristics that exhibit spam-like behavior, such as spam attacks, phishing techniques, image spam, and others. This unique spam identification system provides a high accuracy rate, all while preventing false positives.

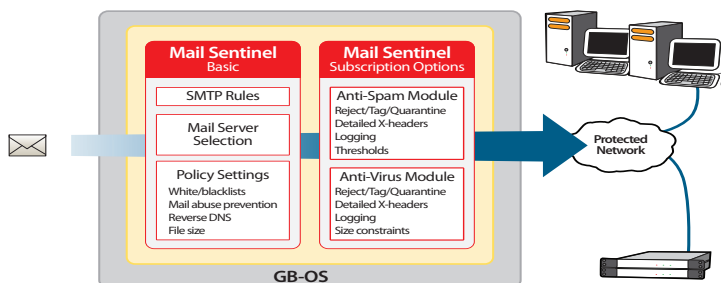
The result of the proprietary Bayesian engine are combined into a SpamScore, a final spam probability rating. Messages with a high rating are flagged as spam, while messages with low ratings are delivered to their destination. Administrators can establish thresholds based on SpamScores for confirmed and probable spam to fine-tune spam filtering to match corporate needs. Once Mail Sentinel Anti-Spam thresholds have been established, administrators may choose to accept, reject, tag or quarantine confirmed or suspected spam.

GTA Firewall UTM Appliances with the Mail Sentinel Anti-Spam subscription option receive automatic updates to ensure the accurate weighting of rules when formulating the SpamScore probability rating. With automatic updates, network administrators can rest assured knowing Mail Sentinel Anti-Spam remains up-to-date to combat the latest spam tactics.

Mail Sentinel Anti-Virus Feature

The Mail Sentinel Anti-Virus feature is your first line of defense against virus attacks. Activating the Mail Sentinel Anti-Virus option through GTA firewall's email proxy for SMTP email means real-time scanning for viruses and other malware is done at the perimeter before they reach your network. By employing highly effective and respected open source virus definition lists, Mail Sentinel Anti-Virus users receive the most complete and inclusive virus and malware protection available.

When using Mail Sentinel Anti-Virus, each email message is quickly scanned and its contents reviewed against a growing database of over 200,000 open source and proprietary virus definitions that includes malware definitions for classic viruses, network worms, trojan programs, DoS and hacking tools, flooders and virus writing tools. Even unknown viruses are detected and prevented using proactive virus detection mechanisms, providing sought after zero-day protection. If a virus is detected, Mail Sentinel Anti-Virus will disinfect the contents when possible.



The Mail Sentinel Anti-Virus feature provides flexible implementation to match network bandwidth and corporate security policies. Network administrators can customize how emails are handled with choices to accept, reject, tag or quarantine emails with known viruses. Email containing viruses can be tagged for easy recognition by the end users, who can then choose to filter tagged messages using email rules. To optimize performance, email and attachment size limits can also be established. Mail Sentinel Anti-Virus automatically receives periodic updates of virus definitions to ensure effective and accurate virus protection. As new virus definitions are discovered, your GTA Firewall UTM Appliance is updated to provide the best possible protection against email based virus attacks.



Global Technology Associates, Inc.
3505 Lake Lynda Drive, Suite 109
Orlando, FL 32817 USA
Tel: +1.407.380.0220 • Fax: +1.407.380.6080
Email: info@gta.com • www.gta.com

© 2011 Global Technology Associates, Incorporated (GTA). All rights reserved.

'GB-OS', 'Surf Sentinel', 'Mail Sentinel' and 'GB-Ware' are registered trademarks of Global Technology Associates, Incorporated. 'GB Commander' is a trademark of Global Technology Associates, Incorporated. 'Global Technology Associates' and 'GTA' are service marks of Global Technology Associates, Incorporated. Features and specifications subject to change without notice.

Document ID: MS201102-01