SECUREMAIL GATEWAY RULES & FILTERS

The SecureMail Gateway provides a highly flexible set of capabilities for filtering email content according to the needs of your organization. The Gateway is able to scan messages based on a number of conditions, and perform actions according to the results of the conditions set by the user. The Gateway is capable of supporting multiple rules and filters simultaneously, each with different conditions and actions to fully enable an organization to protect their confidential information.

Message Conditions

The following table describes the conditions which can be scanned for in a message. Messages that match the condition will be subject to the actions specified for the rule.

Condition	Description
Message time	The message has been sent within the specified time period (time starts at 0:00 and ends at 23:59, this span is broken into 1 hour and 59 minute time frames).
Source IP Address	The message has been sent from the specified IP Address or IP range. More advanced settings can be applied to choose certain IP Addresses, or none at all from a list the user enters.
Header field match	A field in the header contains a match to the specified criteria. The criteria can be entered manually or imported via a file
From, To, CC, BCC or Recipient field match	The sender or recipient list contains a match to the specified criteria
Recipient domains	The recipient(s) are in a specified domain
Subject, Body or Attachment match	The Subject, message Body or an attachment contains a match to the specified criteria
Attachment name match	The attachment name contains a match to the specified criteria
Message Size	The size of the message is larger than the specified value
Message priority	The message is set to the specified priority

200 Park Ave Florham Park NJ 07932 Tel: 800.672.7233 www.datamotion.com

Condition	Description
All Messages	All messages will have the specified action(s) performed on them.

Message Actions

The following table describes the actions that can be taken once a message is found to meet the specified criteria.

Action	Description
Append disclaimer	Appends a footer to the message being sent. The footer is contained within the body of the message.
Modify Subject or Content	Replace specified entries with different words. The original subject can also be included by using %subject% anywhere in the text.
Modify header information	Allows for header modification through text, regular expressions, or the removal of the header entirely.
Message Archiving	Make a copy of the message in a specified directory.
Send in a special manner	Send the message to a different SMTP server, don't send it all, or send it securely.
Remove attachments with specified filenames	Will strip attachments with matching filenames.
Send notify message	Can send a new message (such as a notice the message was delivered securely instead of insecurely)
Stop processing remaining Rules in the Policy	Stops processing any rules that still remain in the policy when the condition is met.
Stop processing any further Policies	Stops processing any remaining policies if the condition is met.

Criteria Matching

The core of any filtering product is the engine for performing the content scanning. The SecureMail Gateway is built on the Microsoft Indexing Service, and as such is capable of scanning over 300 types of files for content matching in addition to the message body (and header) itself. This system provides the flexibility to add new IFilters as your needs change or as newer versions provide better support (or new product version support) without needing to completely change the Gateway software every time.

The following table shows the types of filters which can be used to scan your messages on the Gateway. These filters are used to scan the content of your messages for matches.

Filter	Description
Static list	A static list of words (or strings) created by you to scan for
Email addresses	Specific addresses as well as domains
Regular Expressions (Regex)	Regex pattern matching, includes built-in matches for: ▪ Social Security Numbers ▪ US Phone Numbers ▪ US Zip Code ▪ Credit Cards ▪ Email Address ▪ IP Address ▪ URL ▪ HTML tag
Regulatory Compliance – HIPAA	Matching for codes and terminology from the following: ▪ Clinical Lexicon ▪ HCPCS Codes/Descriptions ▪ ICD-10 Codes/Names ▪ ICD-9 Codes ▪ FDA NDC eList Codes/Names

Filter	Description
Regulatory Compliance – Financial	Matching for terminology for the following financial lexicons: ▪ Laws & Regulations ▪ Analysis, Formulas and Theory ▪ Trading ▪ Insurance ▪ Funds & Bonds ▪ Taxes ▪ Accounting ▪ Real Estate
Dynamic Lists	A dynamic list is a text file list that can be independently updated (such as from a SQL query on a schedule), and every time the file is updated, it will be immediately reloaded into memory for active use. This is used most commonly to provide exact match scanning for content such as customer account numbers where you know the exact numbers instead of attempting to create Regex matching as a "best guess" attempt at determining whether it is included in the content. This type of matching significantly reduces false positives.