DataMotion SecureMail Gateway Administration Guide

December 28, 2015
Part # 050014–02

DataMotion® is a registered trademark of DataMotion, Inc. All other brand and product names are trademarks or registered trademarks of their respective companies.

The information contained in this document is subject to change without notice. THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL DATAMOTION BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING FROM ANY ERROR IN THIS DOCUMENT, INCLUDING WITHOUT LIMITATION ANY LOSS OR INTERRUPTION OF BUSINESS, PROFITS, USE, OR DATA.

DataMotion SecureMail Gateway Administration Guide v2

Publication Date: December 28, 2015

Printed in the United States of America.

DataMotion, Inc. Confidential and Proprietary Information.

Published By:

DataMotion, Inc.
200 Park Ave., Suite 302
Florham Park, NJ 07932
USA

1 800-672-7233 or +1 973-455-1245

http://www.datamotion.com/

TABLE OF CONTENTS

TABLE OF FIGURES

REVISION HISTORY

This section summarizes significant changes, corrections, and additions to the document. The history appears in chronological order with the most recent changes listed first.

Version 2

Provided general formatting updates, and changed the company information present in the document as it was incorrect.

Version 1

The initial version of this document.

1
About This Publication

Welcome to the DataMotion SecureMail Gateway. The purpose of this guide is to provide information for:

- Configuring the SecureMail Gateway
- Managing message policies
- Monitoring the SecureMail Gateway services

To simplify locating information and answering questions about functionality, each chapter in this guide is focused on a specific task or type of information.

The remainder of this chapter contains important general information about this guide.

INTENDED AUDIENCE

This guide is intended for administrators in an organization that will be managing email security.

PREREQUISITES

It is helpful if the reader is familiar with email systems and email message flow within the organization.

Users of this guide are not expected to be security experts.

TERMINOLOGY

This guide contains several terms, conventions, and acronyms that may be unfamiliar to the reader.

2
Introduction

OVERVIEW OF THE DATAMOTION SECUREMAIL GATEWAY

DataMotion SecureMail Gateway (SMGW) analyzes the contents of outgoing email messages and performs appropriate actions based on their content. It enables the organization to transparently implement email policies at the network server level, and does not require end users to have special software or training.

DataMotion SecureMail Gateway (SMGW) assists organizations in meeting various regulatory and legislative requirements relating to email, including those placed on the healthcare, insurance, banking and financial industries. To help meet these requirements, a wide range of content scanning features are provided, including advanced pattern matching for values such as policy or social security number, rapid wordlist searching (e.g. medical lexicon), and analysis of the entire contents of the email message and attachments. Based on the criteria found, specific actions are implemented including secure sending via the optional DataMotion Server, message archiving, appending a disclaimer, message blocking, and notifying the administrator.

COMPONENTS

SMGW is comprised of a Windows-based SecureMail Gateway for administration, and a high-performance, multi-threaded SMTP Engine. These components were developed with the Microsoft .Net development platform, providing state of the art memory management, and integrated security features such as automatic buffer overflow protection. Based on standard Internet mail protocols, interoperability has been tested with popular e mail servers such as Microsoft Exchange, Lotus Notes, Novell GroupWise, SendMail, Exim and IMail, as well as SMTP gateways providing anti-spam and anti-virus functionality.

Administrative Client - DataMotion SecureMail Gateway

A Windows-based client that allows management of all SMTP service and content filter settings. These include network settings, routing and relay control, abuse detection and prevention, user groups, policies and their corresponding rules and actions.

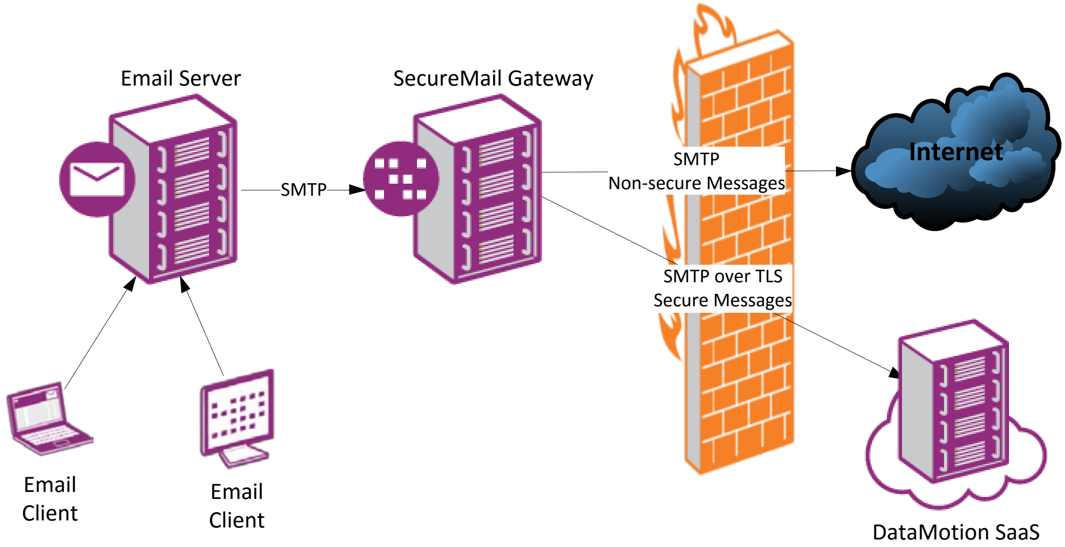
Windows Service - DataMotion SecureMail Gateway SMTP Engine

The SMTP Engine is a high performance, multi-threaded SMTP gateway with integrated policy enforcement and content filtering capabilities. In a typical configuration, this service will receives messages from your mail server, scan their contents based on policy rules, apply corresponding policy actions, and perform SMTP message delivery. The SMTP Engine seamlessly interfaces with the DataMotion Secure Messaging System (DataMotion Server) for secure delivery of email messages to recipients, and can interoperate with your own DataMotion Server or to a corporate secure email account you may have on the DataMotion SaaS site.

ARCHITECTURE

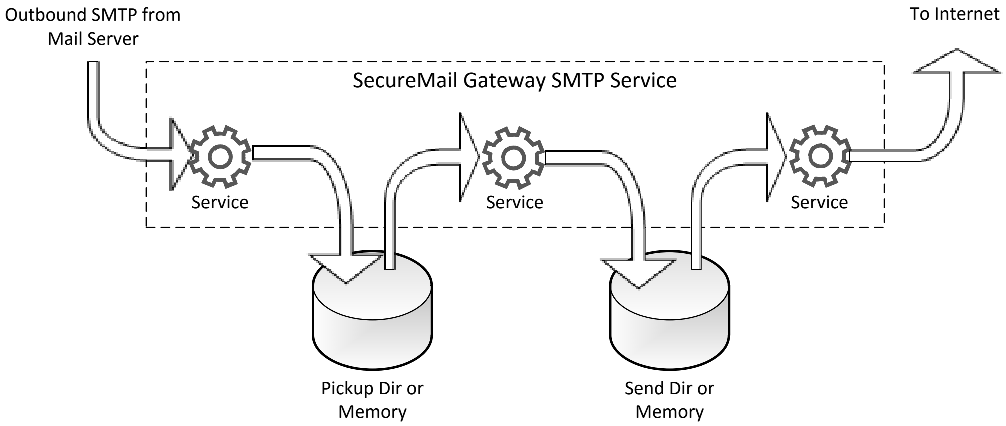
SMGW acts as an SMTP hop in your network. It is designed to accept and process outgoing SMTP messages from your existing email servers, and send them to their recipients or to an outbound SMTP gateway.

Figure 1 – DataMotion SecureMail Gateway Architecture



SMGW is built upon a multi-threaded, multistage queuing architecture that is designed for high performance and reliability. The following diagram shows how messages flow through the system.

Figure 2 – SMTP Flow Process



In the above process flow, the SMTP Service is contained in the dashed rectangle; with messages in each stage either being stored to disk or to memory with a disk overflow. The basic process flow is as follows:

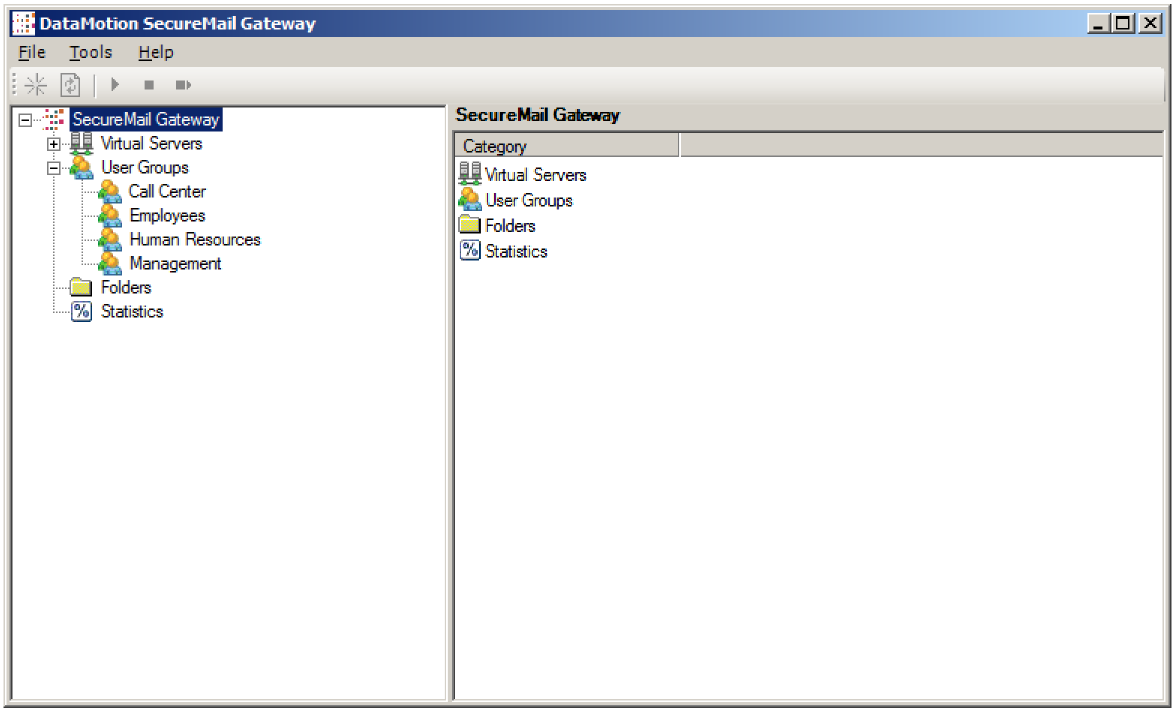
1. Email destined for outbound delivery is routed to the IP address and port of the SMGW , typically by overriding DNS delivery in your mail server to use a SmartHost instead.
2. SMTP Service grants access to authorized computers by IP Address and receives mail from them. By default, these messages are written to a Pickup directory, but can be optionally set to remain in memory. The benefit of writing to disk is that messages in processing will not be lost in the event of a power failure to the server. However, if you are using a battery backup system that will prevent power loss, the queue method can be set to "Memory".
3. SMTP Service polls the Pickup directory for the arrival of new messages, or triggers direct memory transfer of the message to the next stage, which processes the message against its list of Policy rules.
4. Messages designated for traditional SMTP delivery are placed in the Send directory, or transferred directly in memory to the delivery stage. Messages designated for secure DataMotion delivery are written to the \CMSQueue directory (by default) for processing by the DataMotion Server, or can be routed to the DataMotion SaaS site over an encrypted TLS link for secure delivery.
5. SMTP Service polls the Send directory for processed messages that now must be sent, or receives direct memory transfer of messages from the Policy stage. It then delivers these messages to their Internet recipients, or routes outbound messages to a designated gateway or SmartHost server.

3
Main Window

DESCRIBES THE SECUREMAIL GATEWAY AND ITS MAJOR FEATURES

The SecureMail Gateway allows the administrator to manage all aspects of SMGW. For quick access, a shortcut to it is located in the DataMotion SecureMail Gateway Program Group located under the Start menu. After starting the SecureMail Gateway, the following screen will be displayed:

Figure 3 – DataMotion SecureMail Gateway Main Window



Using standard Windows management conventions, the SecureMail Gateway main window is divided into left and right halves and utilizes a Windows Explorer-styled interface. The left half of the main window displays an expandable tree of categories, and the right half displays specific elements of the selected category.

The SecureMail Gateway utilizes a context-sensitive toolbar and right-click popup menu. Based on the highlighted item in the interface, the appropriate toolbar icons and popup menu items are displayed.

For rapid manipulation of certain settings, mouse-based drag and drop can be used to speed up the management of User Groups, Policies and Rules. Using drag and drop, it is possible to move and copy users among User Groups, change the order of Policies, and also change the order of Rules.

SECUREMAIL GATEWAY MANAGEMENT CATEGORIES

Management of SMGW is divided into the following categories:

- Virtual Servers
- User Groups
- Policies
- Folders
- Statistics
- Reporting

Each of these categories is described in detail in the following chapters.

The SecureMail Gateway also provides a pull down menu giving access to a range of features. These menu choices are as follows:

FILE MENU

File | Save Settings

This menu choice will commit all Group and Policy settings to disk. The SMTP Engine will automatically detect these setting changes without needing to be restarted.

File | Reload Settings

Select this menu choice to reload Policies and User Groups from disk to their previously saved values. If any changes have been made and not yet saved, a warning prompt will be displayed prompting whether to override the existing changes without saving them.

File | Exit

Choose this menu item to exit the SecureMail Gateway program. If any changes have been made since the last time changes were saved, you will be prompted to save the changes before the program is exited.

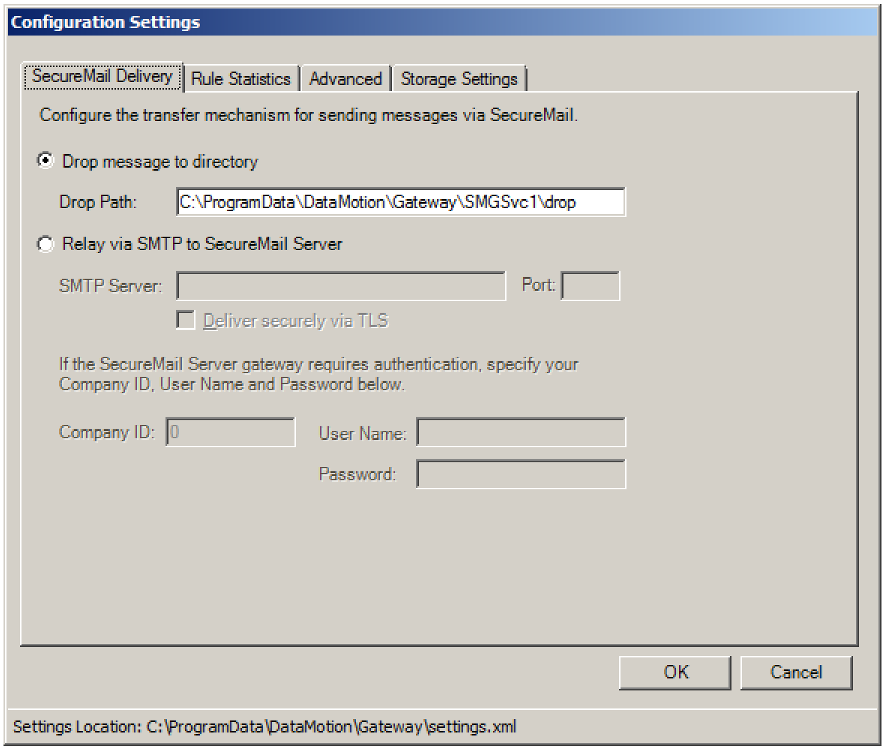
TOOLS MENU

Tools | Settings

Select this menu item to access system wide values such as database type and connection parameters, DataMotion Server integration options, and message queuing method.

Tools | Settings: SecureMail Delivery Tab

Figure 4 – Configuration Settings: SecureMail Delivery



Configure the transfer mechanism for sending messages via SecureMail.

● Drop message to directory

Drop Path: C:\ProgramData\DataMotion\Gateway\SMGSvc1\drop

○ Relay via SMTP to SecureMail Server

SMTP Server: Port:

□ Deliver securely via TLS

If the SecureMail Server gateway requires authentication, specify your Company ID, User Name and Password below.

Company ID: 0 User Name:

Password:

Settings Location: C:\ProgramData\DataMotion\Gateway\settings.xml

SMGW provides seamless integration with the DataMotion Server, allowing designated messages to be delivered securely to any Internet recipient. Select from one of the two options provided for integration with the DataMotion Server.

Drop message to directory: Typically, if the DataMotion Server is installed in your network, then this option is selected. Messages that are flagged by Policy rules for DataMotion delivery will be written as MIME messages to the designated directory. Since the DataMotion Server will poll this directory for messages to delivery securely, a Windows network share will be needed on the SMGW computer.

Relay via SMTP to DataMotion Server: This option is most commonly used for integration with your DataMotion Server corporate account, but will also allow secure messaging through any DataMotion Server appropriately configured. In the case of DataMotion SaaS integration, the DataMotion Server is not located in your network, but you have a corporate account on the DataMotion SaaS. Messages flagged for DataMotion delivery by the Policy rules will be delivered to the DataMotion SaaS via a secure SMTP connection using 128-bit TLS (SSL v3). These messages will then be processed by the DataMotion SaaS for secure delivery to their Internet recipients.

The following settings will be supplied by your DataMotion account administrator:

SMTP Server: The Internet domain name of the DataMotion SMTP server that will accept mail from your SMGW system.

Deliver Securely via TLS: Select this setting to create an encrypted communication link between your SMGW system and the SMTP server of the DataMotion SaaS site.

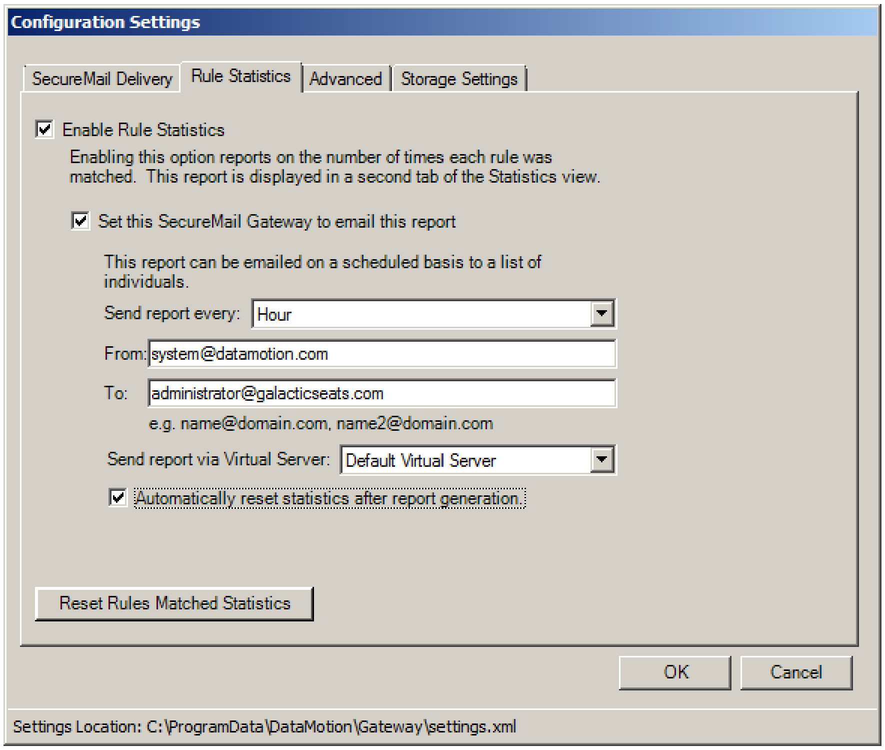
Company ID: A numeric value provided by your DataMotion administrator.

User Name: A login ID to access the DataMotion SMTP server.

Password: The password required to access the DataMotion SMTP server.

Tools | Settings: Rule Statistics

Figure 5 – Configuration Settings: Rule Statistics



☑ Enable Rule Statistics

Enabling this option reports on the number of times each rule was matched. This report is displayed in a second tab of the Statistics view.

☑ Set this SecureMail Gateway to email this report

This report can be emailed on a scheduled basis to a list of individuals.

Send report every: Hour

From: system@datamotion.com

To: administrator@galacticseats.com

e.g. name@domain.com, name2@domain.com

Send report via Virtual Server: Default Virtual Server

☑ Automatically reset statistics after report generation.

Settings Location: C:\ProgramData\DataMotion\Gateway\settings.xml

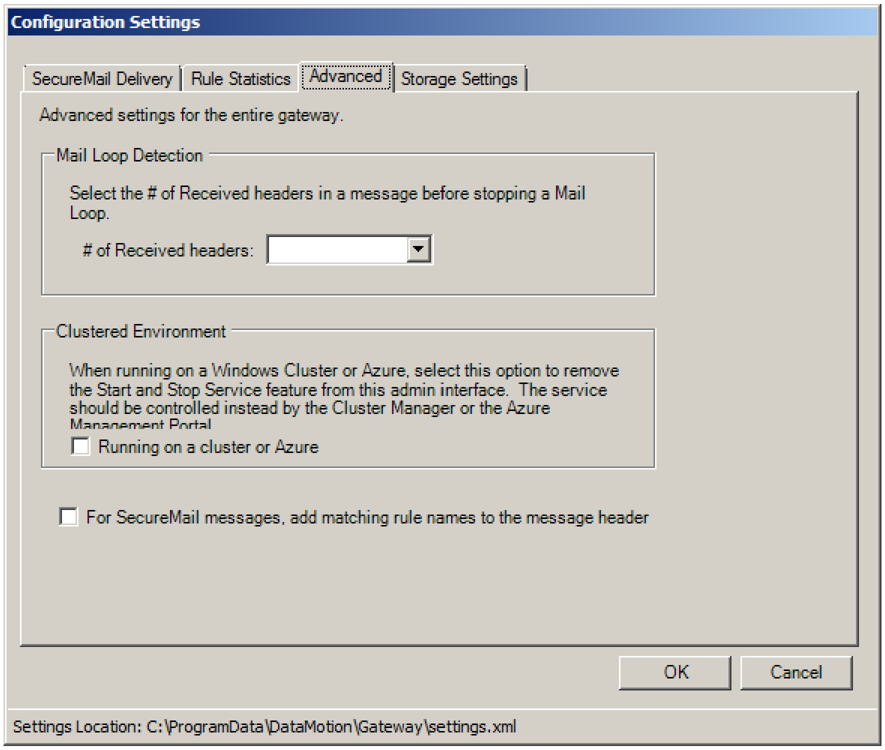
Enable Rules Matched Statistics: This will enable the statistics page with the number of times a rule was matched.

Set this SecureMail Gateway to email "Rules Matched Statistics" report: This option will email a rules matched report at predefined intervals from the specified Virtual Server.

Automatically reset Statistics after report generation: With this option, the report statistics will be reset after the report has been generated.

Tools | Settings: Advanced Tab

Figure 6 – Configuration Settings: Advanced Tab



Configuration Settings

Advanced settings for the entire gateway.

Mail Loop Detection

Select the # of Received headers in a message before stopping a Mail Loop.

# of Received headers:

Clustered Environment

When running on a Windows Cluster or Azure, select this option to remove the Start and Stop Service feature from this admin interface. The service should be controlled instead by the Cluster Manager or the Azure Management Portal

□ Running on a cluster or Azure

□ For SecureMail messages, add matching rule names to the message header

Settings Location: C:\ProgramData\DataMotion\Gateway\settings.xml

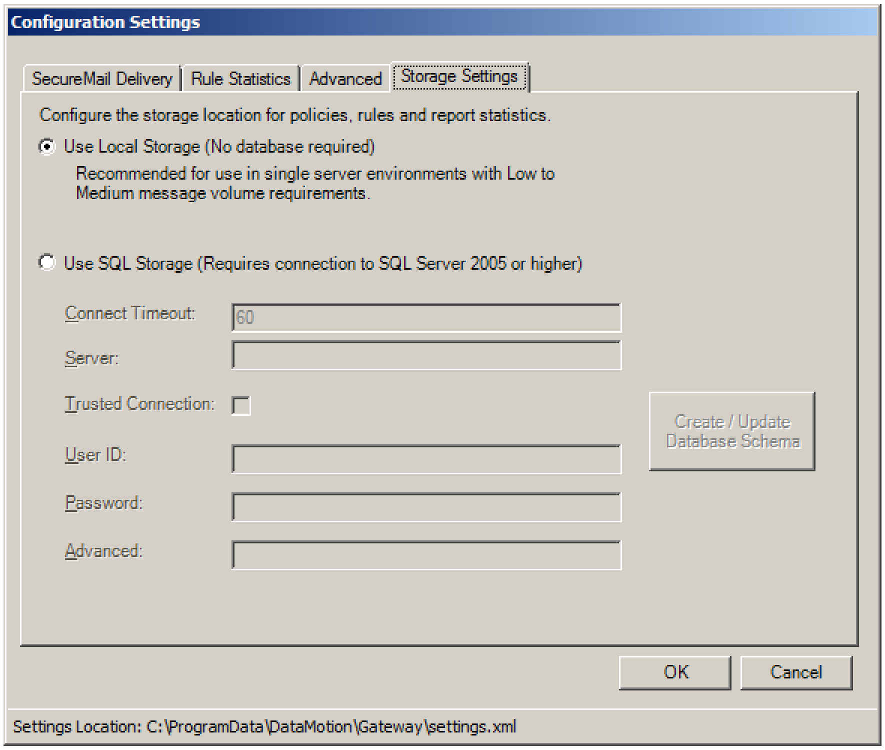
# of Received headers: This option specifies the number of received headers in a message that will trigger a detected mail loop for the message. Mail loop messages are then failed with appropriate notification.

Running of a cluster or Azure: This will remove the ability to stop and start the services inside the SMGW interface so they cannot be accidentally put into an invalid state.

For SecureMail messages, add matching rule name to the message header: When checked, the name of the policy filter will be added as a X-header into the message when it is sent to the DataMotion Server.

Tools | Settings: Storage Settings Tab

Figure 7 – Configuration Settings: Storage Settings



Configuration Settings

Configure the storage location for policies, rules and report statistics.

● Use Local Storage (No database required)

Recommended for use in single server environments with Low to Medium message volume requirements.

○ Use SQL Storage (Requires connection to SQL Server 2005 or higher)

Connect Timeout: 60

Server:

Trusted Connection: □

User ID:

Password:

Advanced:

Settings Location: C:\ProgramData\DataMotion\Gateway\settings.xml

SMGW can store its information in XML files or in a SQL database. The choice of storage is made when the application is first started, but can be changed later. The default is local storage which uses XML files to maintain the configuration data.

For enterprise installations where more than one SMGW is used in a load-balanced configuration, it may be desirable to store SMGW settings to a Microsoft SQL Server. With this configuration, each node in the SMGW cluster can be configured to use this common data store, and SecureMail Gateway settings will be utilized by all nodes in the cluster.

To utilize Microsoft SQL Server for the data store, the DataMotion SMGW database must be installed to an SQL Server as part of SMGW installation. Then, the following SQL Server connection options must be configured to attach to the SMGW SQL database:

Connect Timeout: The time in seconds to wait for the SQL Server to respond to requests. Default is 60 seconds.

Server: Select the SQL Server from the pull down list, or type in the name of the SQL Server where the database is located.

Trusted Connection: Place a check in this field to use the login name and password set in the Windows Service manager for the SMTP Engine. Uncheck this field to use the User ID and Password fields.

User ID: If not using Integrated Security, enter the SQL Server user name required to access the database.

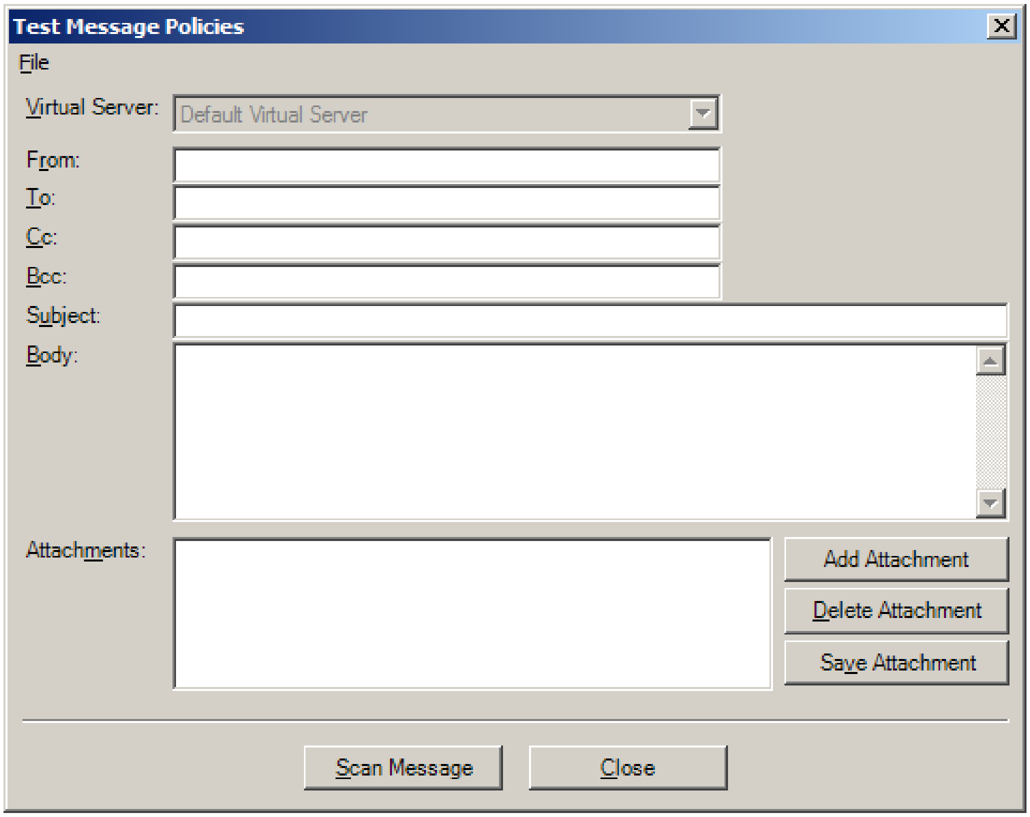
Password: If entering a User ID, enter the password required to connect to the database.

Advanced: Enter any additional SQL Server connection string parameters required to access the database. Typically, this field is left blank.

If multiple SMGW systems are used in a load balanced configuration, then the SQL database settings can be modified to point to a central database server. By doing this, SMGW settings made through the SecureMail Gateway will be utilized by all SMGW systems in the load balancing group without having to recreate the Policies for all systems.

Tools | Test Policies

Figure 8 – Test Message Policies



This feature is useful when you have defined at least one Policy containing at least one Rule. In this scenario, you can determine which Policy(s) and Rule(s) match a test email message.

To use this feature, enter information in one or more message fields. Attachments can be added, deleted and saved by selecting the corresponding button in the lower right portion of the window. Once the information and any attachments are provided, select the Scan Message button. Policies and Rules that match the message will be displayed.

If you have a MIME message on disk, you can use the File | Load from File menu to read its contents into the window. Other options under the File menu include Save, Reload Default, Save as Default, and Close.

A test email message can be created by many email client programs as long as it is saved to disk in MIME format with an EML file extension. A mail client such as Windows Live Mail or Mozilla Thunderbird can be used to save message in the MIME (EML) format.

One important aspect to note, however, is that a MIME message saved to disk by an email client often does not contain a sending computer's IP address. So if a Policy or Rule is triggered by IP address, this condition will not be matched. You can simulate an IP address by editing the EML message file with Notepad and adding a line at the top of the file as follows:

```
x-ipfrom:  123.234.123.234
```

where 123.234.123.234 should be replaced by an appropriate IP address of a computer that will be sending its messages through SMGW. When this new edited file is tested, any Policies or Rules that depend on this IP address will have this part of the matching condition met.

Tools | Event Viewer

SMGW writes various events such as error conditions to the Windows Event Log. This menu item provides convenient access to the Windows Event Viewer so that you can review this log of events.

HELP MENU

About Menu Item

Displays the version, copyright information and web URL information for SMGW.

4
Virtual Servers

CONFIGURING THE DATAMOTION SECUREMAIL GATEWAY SMTP ENGINE

SecureMail Gateway provides a high performance, multithreaded SMTP Engine that runs as a Windows background service. The SMTP Engine can be configured to act like one or more virtual SMTP servers, each with independent settings. This engine allows SMGW to provide SMTP receiving, scanning and delivery of messages, and its settings are managed through the SecureMail Gateway interface.

VIRTUAL SERVERS TREE ACTIONS

Various actions can be accessed off of the Virtual Servers tree item in the left window area. To access these actions, click on the appropriate icon in the toolbar, or right-click on the Virtual Servers tree item to display a popup menu with the following items.

New Virtual Server

Provides for the creation of a new Virtual Server with a unique set of properties.

Refresh

Queries the operational status of the SMGW Windows service and updates the display accordingly.

Start Service

Select this option to start the SMGW Windows service.

Stop Service

Select this option to stop the SMGW Windows service. With the service stopped, no messages will be received, content filtered, or delivered by the system.

Restart Service

Select this option to restart a running SMGW Windows service.

VIRTUAL SERVER ACTIONS

Various actions can be performed on each Virtual Server. These actions are accessed by highlighting the desired Virtual Server and then using the right-click popup menu or toolbar. The following options are available for the administrator to manage the selected virtual server.

PROPERTIES

Select Properties to manage operational characteristics of the SMTP Engine including IP address configuration, connection permissions, threads and queue paths. Information on each of these settings is covered in detail in the Virtual Server Properties section.

DELETE

Remove the highlighted Virtual Server from the system. This option is disabled for the first default Virtual Server.

VIEW LOG FILES

Opens Windows Explorer to the directory where log files are stored for this virtual server. These files are stored in standard comma delimited text format and can be opened with Windows Notepad or imported into programs such as Microsoft Excel.

VIEW QUEUES

Four submenu choices appear off of this choice: Pickup (received messages), Send (for delivery), Badmail and CMS (SecureMail) defined in menu Tools | Settings | SecureMail Delivery). Message files are stored in these directories as MIME messages with an EML file extension, and can be readily viewed using Windows Notepad or an email client such as Windows Live Mail, Mozilla Thunderbird or a recent version of Outlook.

NEW POILICY

Launches the New Policy wizard.

IMPORT ALL POLICIES

Allows you to import previously exported and saved settings, including policies and users. This option will overwrite all existing policies currently on the server.

EXPORT ALL POLICIES

Allows you to export the current settings and users for import on another server or as general backup. The files are stored as XML.

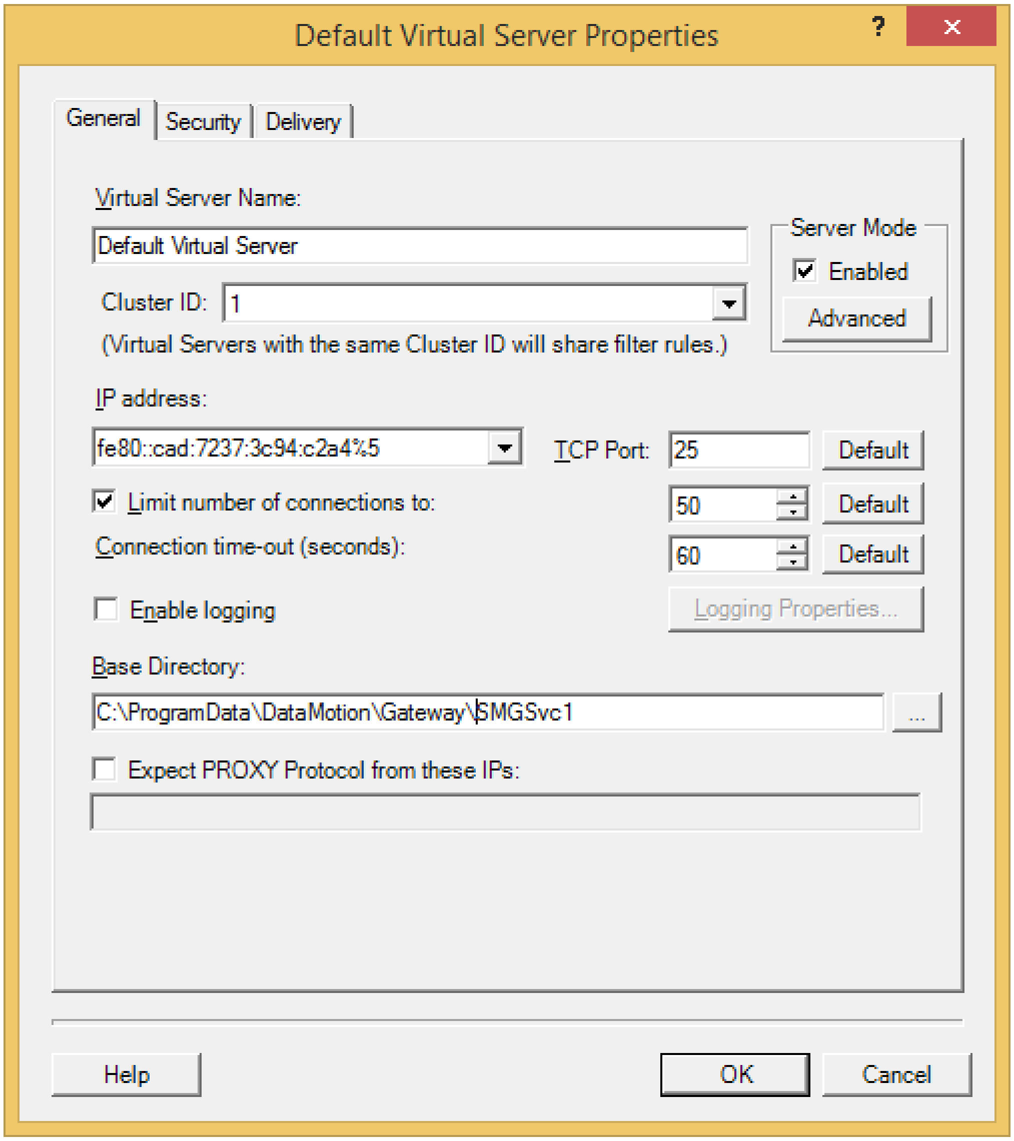
VIRTUAL SERVER PROPERTIES

When a particular Virtual Server is highlighted on the main window, and then the Properties action is selected, the Virtual Servers Properties screen will be displayed.

This screen is comprised of three tabs—General, Security and Delivery.

VIRTUAL SERVER: GENERAL TAB

Figure 9 – Virtual Server Properties: General Tab



Default Virtual Server Properties

Virtual Server Name: Default Virtual Server

Cluster ID: 1

(Virtual Servers with the same Cluster ID will share filter rules.)

Server Mode: ☑ Enabled

IP address: fe80::cad:7237:3c94:c2a4%5

TCP Port: 25

☑ Limit number of connections to: 50

Connection time-out (seconds): 60

☐ Enable logging

Base Directory: C:\ProgramData\DataMotion\Gateway\SMGSvc1

☐ Expect PROXY Protocol from these IPs:

For the selected Virtual Server, the General tab allows configuration of the following options:

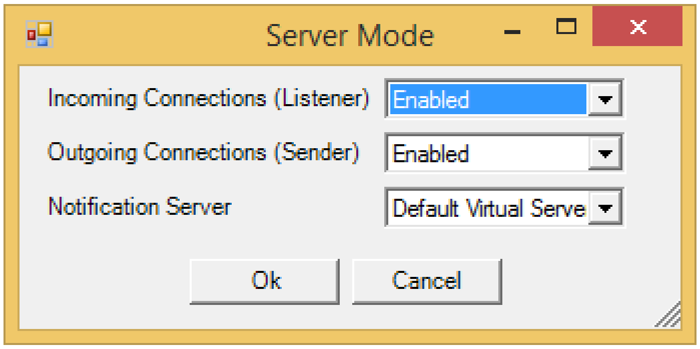
Virtual Server Name:

Type in a display name for the virtual server. This name will be listed in the list of virtual servers in the main window.

Server Mode

The Enabled checkbox controls whether the entire server is enabled if checked, or disabled if it is not checked.

The Advanced button will open a popup window containing additional options.



Incoming Connections (Listener): Enabled

Outgoing Connections (Sender): Enabled

Notification Server: Default Virtual Serve

- Incoming Connections (Listener): The available options for this field are Enabled, Disabled, or Force TLS (selecting this option will always enforce TLS on every Inbound connection).
- Outgoing Connections (Sender): The available options for this field are Enabled, Disabled, or Force TLS (selecting this option will always enforce TLS on every Outbound connection).
- Notification Server: The drop-down for this field will contain all of the Virtual Servers that you have on the Gateway. Only one option can be selected as the Notification Server for any particular Virtual Server on your system.

Cluster ID:

The Cluster ID is used to note virtual servers that will share filter rules.

IP address:

The SMTP listener thread will listen to incoming SMTP connections on the selected IP address.

TCP Port

Select the port that the SMTP Listener will monitor. The default port for SMTP services is 25. To prevent conflicts, the combination of IP address and port must not be used by any other process in the system.

Limit number of connections to

The SMTP listener can handle many simultaneous SMTP connections. Depending on the capabilities of your hardware and network, adjusting the number of connection threads may be desired. For most network and hardware configurations, however, the default setting of 50 simultaneous connections is usually effective.

Connection time-out (seconds)

Select the amount of seconds that should pass before an idle SMTP connection is closed. The default value is 60 seconds.

Enable Logging

SMGW can write its SMTP and content filtering activity to a log file. Select this option to enable logging. Then select the Logging Properties button described below to configure the log to your needs.

Note: Log files will be saved to the Logfiles directory under the Base Directory value set in the previous property.

Base Directory

Select a directory path that will serve as the base directory for SMGW Pickup, Send, Badmail and Logfiles subdirectories. The drive containing this directory should have sufficient free space to handle your email volume.

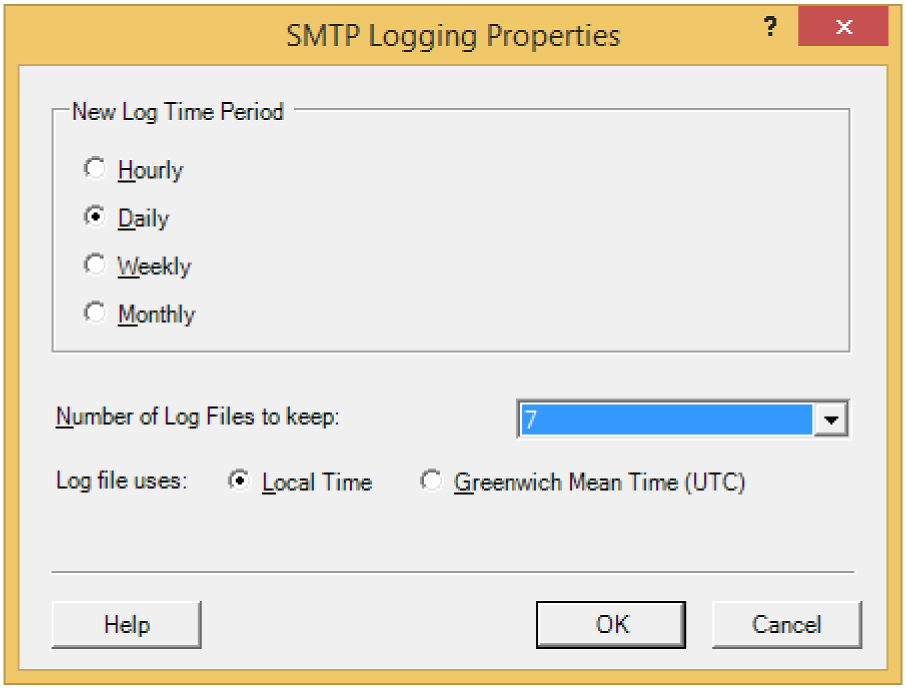
Expect PROXY Protocol from these IPs:

Selecting this checkbox will allow you to set one or multiple IP Addresses for Virtual Servers using a proxy, and expected to be using Proxy Protocol. This setting is required if you need to set IP whitelisting and blacklisting.

Logging Properties…

Select this button to display the following SMTP Logging Properties screen.

Figure 10 – Virtual Server Properties: SMTP Logging



SMTP Logging Properties

New Log Time Period

○ Hourly
● Daily
○ Weekly
○ Monthly

Number of Log Files to keep: 7

Log file uses: ● Local Time ○ Greenwich Mean Time (UTC)

New Log Time Period

Log file size can be controlled by selecting a time period to use before creating a new log file. When the time period has elapsed, the previous log file will be closed, and subsequent logging data will be written to a new file. Choose among time periods of Hourly, Daily, Weekly, or Monthly.

Number of Log Files to keep

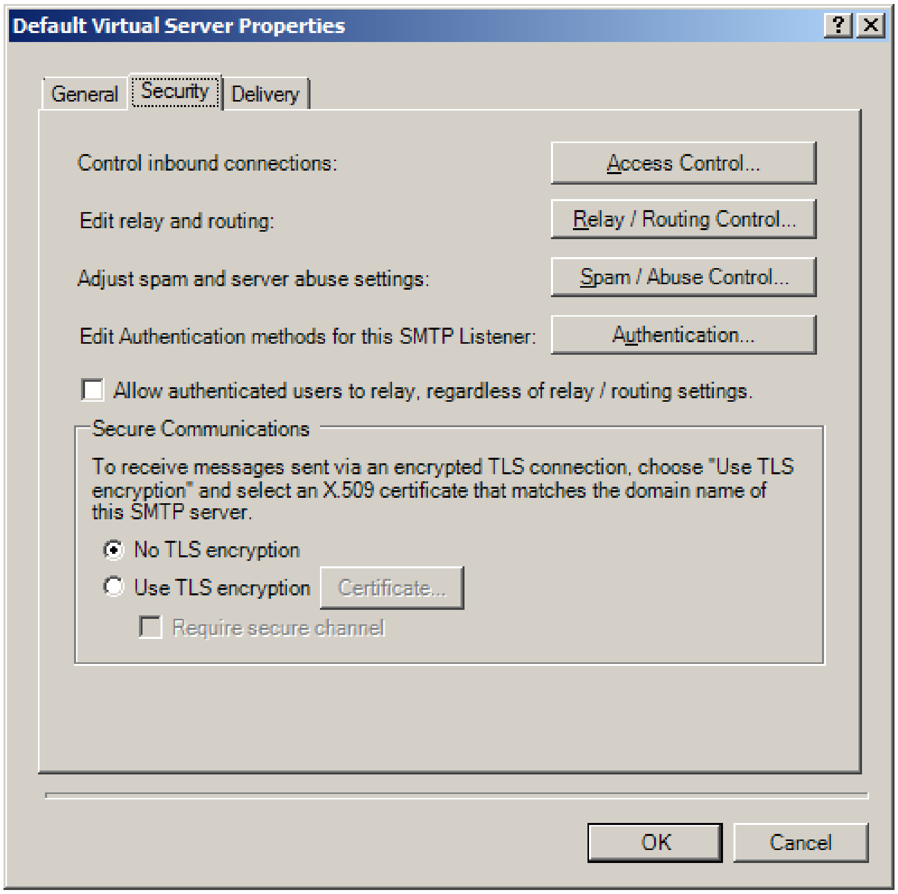
Select the maximum number of past log files to keep before deleting them. The list of log files will be sorted by date, and if the list is larger than this value, the oldest files will be deleted from disk.

Log file uses

Select Local Time or Greenwich Mean Time (UTC) as the date and time used to stamp each entry in the log file.

VIRTUAL SERVER: SECURITY TAB

Figure 11 – Virtual Server Properties: Security Tab



Default Virtual Server Properties

Control inbound connections: Access Control...

Edit relay and routing: Relay / Routing Control...

Adjust spam and server abuse settings: Spam / Abuse Control...

Edit Authentication methods for this SMTP Listener: Authentication...

☐ Allow authenticated users to relay, regardless of relay / routing settings.

Secure Communications

To receive messages sent via an encrypted TLS connection, choose "Use TLS encryption" and select an X.509 certificate that matches the domain name of this SMTP server.

● No TLS encryption

○ Use TLS encryption Certificate...

☐ Require secure channel

The Security Tab controls properties of the virtual server related to access, relay, limits, authentication and encrypted communication. The following options are available on this tab.

Allow Authenticated users to relay, regardless of relay / routing settings

When SMGW is configured to accept login credentials before sending a message, this option will allow authenticated users to relay messages even Relay / Routing Control settings would otherwise prevent them. This option is useful for DataMotion Server integration, since registered users of DataMotion Server can use SMGW for sending outbound email from their Internet email client.

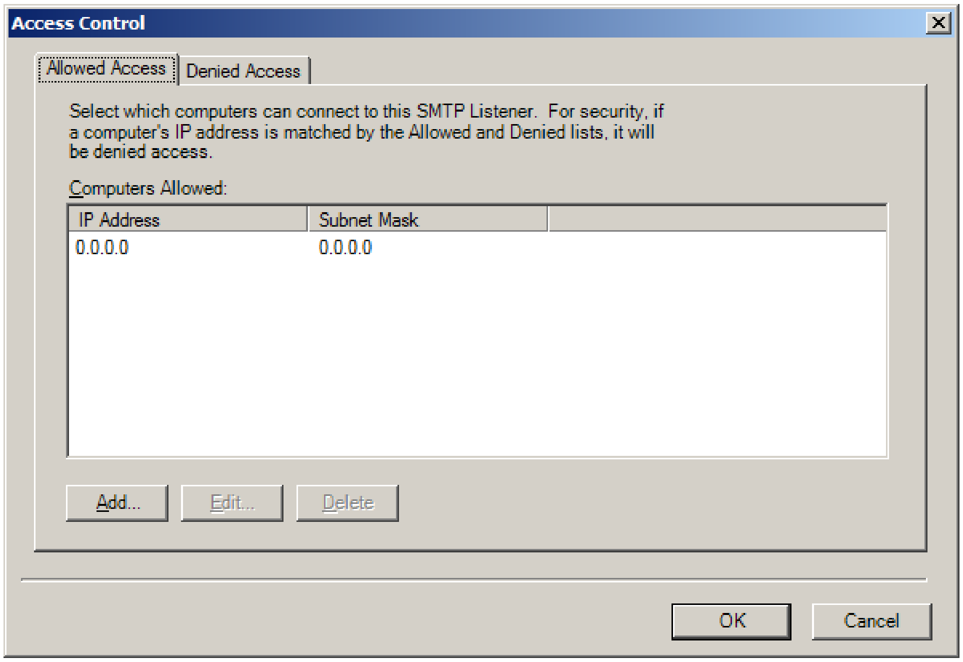
Secure Communications

By default, SMTP email is sent in plain text without benefit of encryption. This makes Internet email messages susceptible to eavesdropping and unintended disclosure. Setting the “No TLS encryption” option runs SMGW in this most basic way. By having an X.509 server certificate for the domain of this SMGW virtual server and selecting “Use TLS encryption", SMGW can receive TLS-encrypted messages from sending servers. When setting the "Use TLS encryption" option, SMGW can force a secure channel if a checkmark is placed in the "Require Secure Channel" field.

Security Tab: Access Control…

When the "Access Control" button is selected, the following window is displayed.

Figure 12 – Security Tab: Access Control



Select which computers can connect to this SMTP Listener. For security, if a computer's IP address is matched by the Allowed and Denied lists, it will be denied access.

Computers Allowed:

IP Address	Subnet Mask
0.0.0.0	0.0.0.0

When a computer makes a connection to a virtual server, its IP address is available for inspection. Before any data transfer takes place, the IP address will be examined. Based on the settings of the Access Control window, the connection will either be allowed to continue or immediately terminated.

ACCESS TABS – ALLOWED ACCESS AND DENIED ACCESS

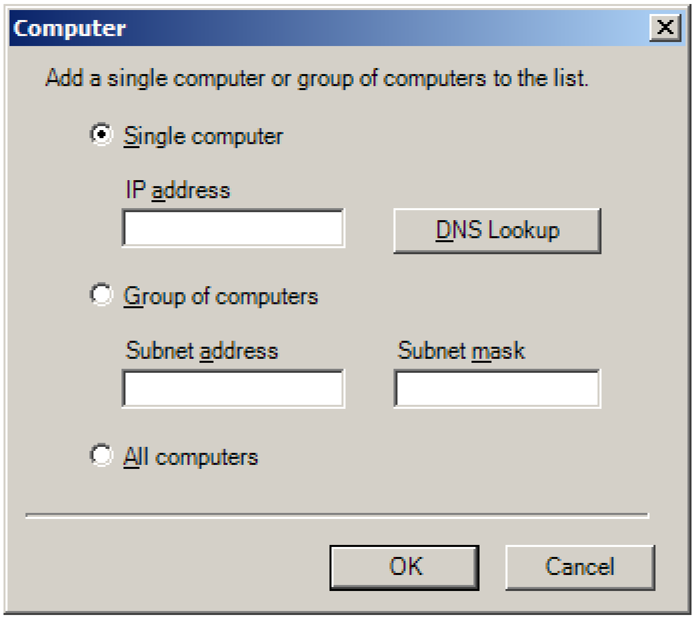
These tabs display the list of computers that are allowed and denied connection access to this virtual server. The Allowed Tab lists the IP addresses or networks that can send messages through this virtual service, and the Denied Tab lists entries that will be denied a connection. For security reasons, if an IP address is matched in the Allowed Access and Denied Access Tabs, then the connection will be denied. The only exception to this is if the IP address matches a network range on the Denied Access Tab, but is a "Single Computer" (see below) exact match on the Allowed Access Tab. In this case, the connection will be allowed.

Since the control of the Allowed and Denied Access lists is the same, the control options provided are described once below.

Add…

Allows the entry of a new computer or network range. Selecting this button displays the following screen.

Figure 13 – Access Tabs: Add Computer



Computer

Add a single computer or group of computers to the list.

● Single computer

IP address

○ Group of computers

Subnet address

Subnet mask

○ All computers

Single Computer

Select this radio button to define a single computer IP address to add to the Allowed or Denied list.

IP address

Type the IP address of the computer that will be Allowed or Denied access to relay messages to SMGW.

DNS Lookup

Since SMGW grants or denies connections based on IP address, you may wish to lookup the IP address of a particular computer by entering its domain name. Select the "DNS Lookup" button to enter a domain name and resolve it to an IP address.

Group of computers

Select this radio button to define a network of computers to add to the Allowed or Denied list.

Subnet address

Type the subnet address of the network of computers to add.

Subnet mask

Type the subnet mask of the network of computers to add.

All computers

Add all computers to the Allowed or Denied list.

Edit

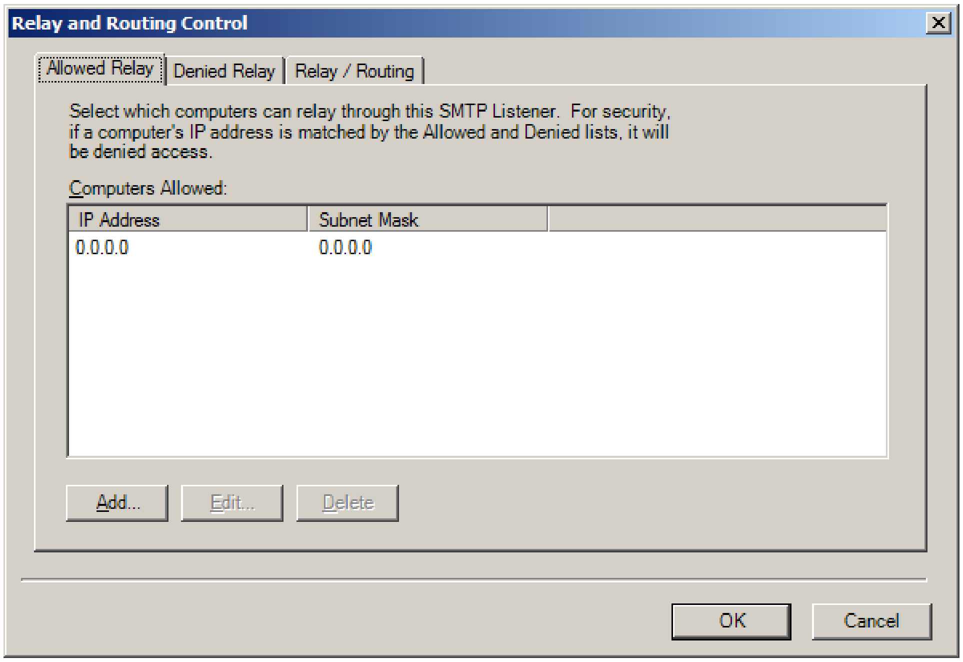
Allows the currently highlighted entry to be edited

Delete

Deletes the currently highlighted entry.

Security Tab: Relay / Routing Control…

Figure 14 – Security Tab: Relay / Routing Allowed Relay Tab



Select which computers can relay through this SMTP Listener. For security, if a computer's IP address is matched by the Allowed and Denied lists, it will be denied access.

Computers Allowed:

IP Address	Subnet Mask
0.0.0.0	0.0.0.0

The Relay and Routing window controls which computers can relay messages through the virtual server, special or custom delivery routes, and advanced delivery properties such as authentication and TLS encryption.

RELAY TABS – ALLOWED RELAY AND DENIED RELAY

These tabs display the list of computers that are allowed and denied to relay messages through this virtual server. The Allowed Tab lists the IP addresses or networks that can relay messages through this virtual service, and the Denied Tab lists entries that will be denied relay permissions. For security reasons, if an IP address is matched in the Allowed Access and

Denied Access Tabs, then relay privileges will be denied. The only exception to this is if the IP address matches a network range on the Denied Access Tab, but is a "Single Computer" (see below) exact match on the Allowed Access Tab. In this case, relay permissions will be allowed.

Since the control of the Allowed and Denied Access lists is the same, the control options provided are described once below.

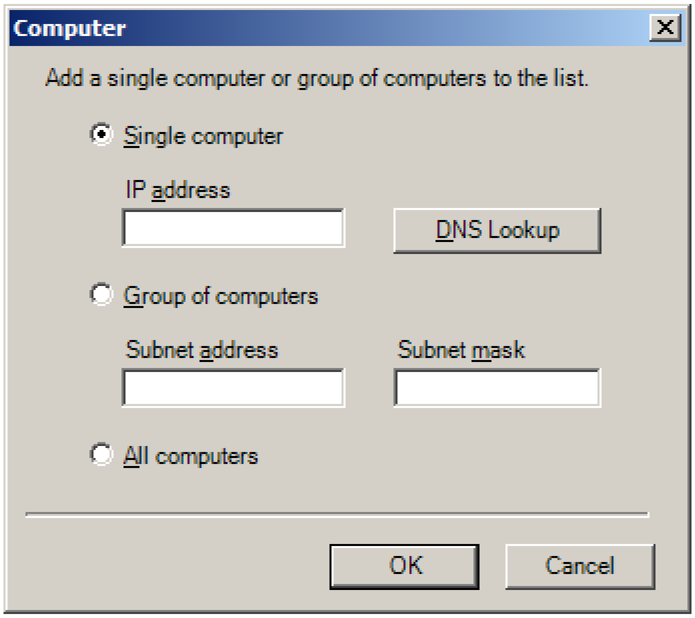
In most cases, these lists will contain the same entries as the Allowed Access and Denied Access lists described previously.

> **Note: Even if a computer's IP address is denied relay permissions, by using the features found under the Relay / Routing tab, it may still be able to send messages to certain message recipients. This allows the virtual server to operate in locked down manner, receiving messages only for a predefined set of recipients or recipient email address patterns. These protections are applied at the SMTP RCPT chitchat level before the actual message is sent. This provides a level of defense against SPAM dictionary attacks, and also minimizes the network traffic generated by SPAM messages. Further information about this feature is described in the Relay / Routing Tab section below.**

Add…

Allows the entry of a new computer or network range. Selecting this button displays the following screen.

Figure 15 – Relay Tabs: Add Computer



Computer

Add a single computer or group of computers to the list.

● Single computer

IP address:

○ Group of computers

Subnet address:

Subnet mask:

○ All computers

Single Computer

Select this radio button to define a single computer IP address to add to the Allowed Relay or Denied Relay list.

IP address

Type the IP address of the computer that will be Allowed or Denied access to relay messages to SMGW.

DNS Lookup

Since SMGW grants or denies connections based on IP address, you may wish to lookup the IP address of a particular computer by entering its domain name. Select the "DNS Lookup" button to enter a domain name and resolve it to an IP address.

Group of computers

Select this radio button to define a network of computers to add to the Allowed or Denied list.

Subnet address

Type the subnet address of the network of computers to add.

Subnet mask

Type the subnet mask of the network of computers to add.

All computers

Add all computers to the Allowed or Denied list.

Edit

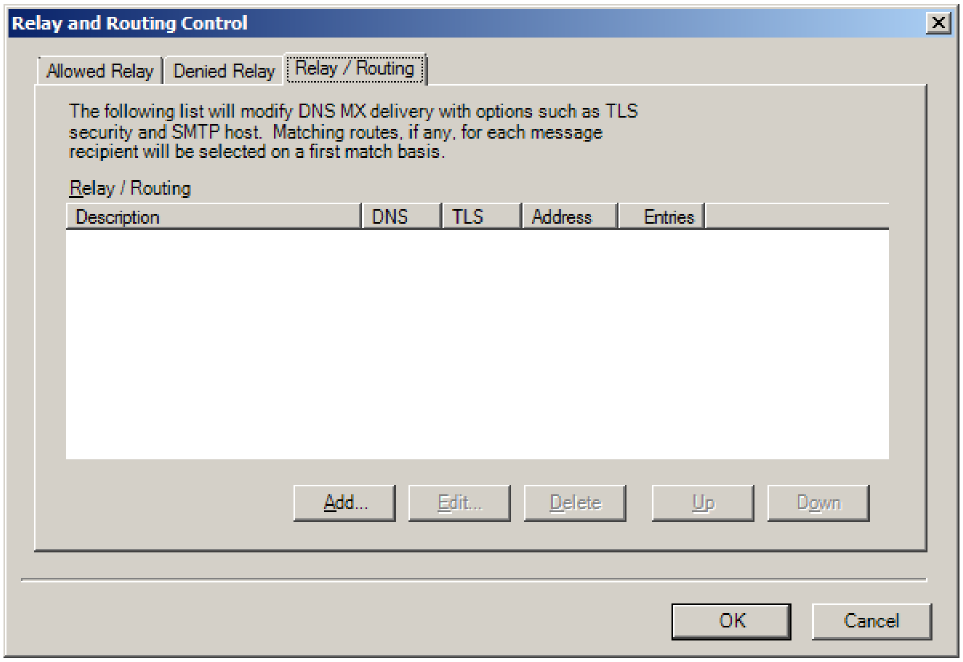
Allows the currently highlighted entry to be edited

Delete

Deletes the currently highlighted entry.

Relay / Routing Tab

Figure 16 – Security Tab: Relay / Routing Relay / Routing Tab



The following list will modify DNS MX delivery with options such as TLS security and SMTP host. Matching routes, if any, for each message recipient will be selected on a first match basis.

By default, messages will be delivered to recipient mail servers using standard DNS MX record methods. Delivery to mail servers, and parameter used to connect to these servers, can be modified through the Relay / Routing Tab. The list of routing overrides is displayed in the Relay / Routing list, and can be modified by selecting the appropriate command button below the list.

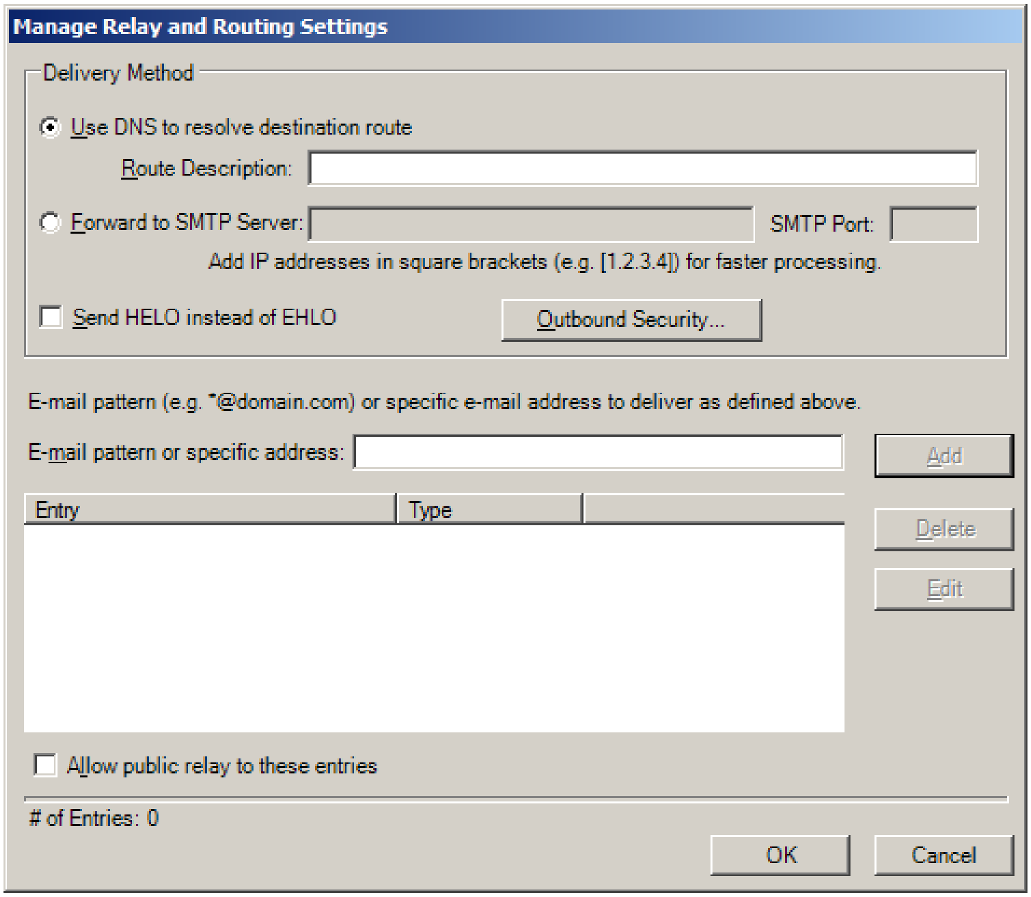
Entries in this list will be evaluated against message recipients in the order specified. As soon as the first matching entry is found, then the appropriate routing instructions will be followed. For this reason, entries are usually arranged in most specific to least specific order. Entries can be moved up and down in the list by highlighting an entry and using the Up and Down buttons. In addition, highlighted entries can be deleted by selecting the Delete button.

ADD / EDIT…

Manage Relay and Routing Settings

When the Add or Edit buttons are selected, the following screen will be displayed. The Add button allows a new entry to be added to the list, and the Edit button will edit a currently selected entry.

Figure 17 – Relay / Routing Tab: Manage Settings



Manage Relay and Routing Settings

Delivery Method

● Use DNS to resolve destination route

Route Description:

○ Forward to SMTP Server: SMTP Port:

Add IP addresses in square brackets (e.g. [1.2.3.4]) for faster processing.

□ Send HELO instead of EHLO

E-mail pattern (e.g. *@domain.com) or specific e-mail address to deliver as defined above.

E-mail pattern or specific address:

Entry	Type

□ Allow public relay to these entries

# of Entries: 0

Use DNS to resolve destination route

For recipients defined in the “Email pattern or specific address” list below, select this option to deliver messages by using standard DNS lookups to determine the mail server for recipients. When selecting this option, the Route Description also needs to be completed.

Route Description

When selecting the above DNS option, provide a description for this route. This description will appear in the first column of the list on the Relay / Routing tab.

Forward to SMTP Server

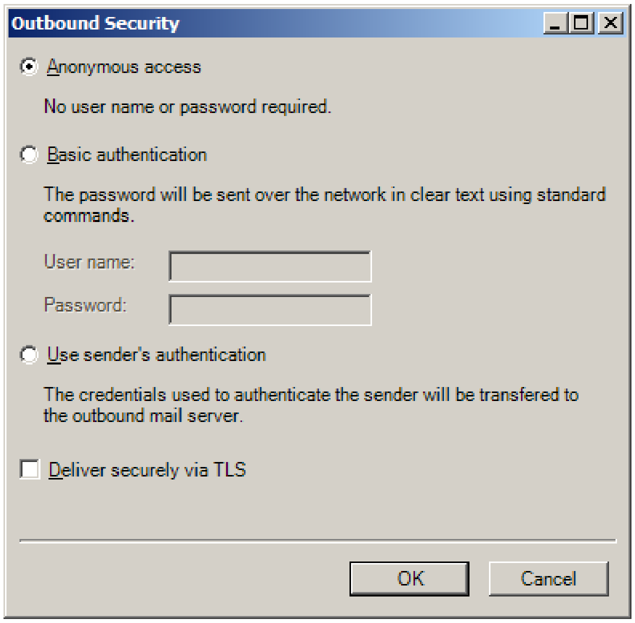
For recipients defined in the “Email pattern or specific address” list below, force their outbound SMTP messages to be delivered to a specific SMTP Server. This entry will override the typical DNS lookup delivery method, and is useful for pointing messages to an SMTP gateway for Internet delivery.

Send HELO instead of EHLO

SMGW will use Enhanced SMTP syntax when supported by a destination mail server. Select this option to override this behavior and default to standard SMTP.

Outbound Security…

Figure 18 – Relay / Routing Tab: Outbound Security



Outbound Security

● Anonymous access

No user name or password required.

○ Basic authentication

The password will be sent over the network in clear text using standard commands.

User name:

Password:

○ Use sender's authentication

The credentials used to authenticate the sender will be transfered to the outbound mail server.

□ Deliver securely via TLS

Certain mail servers may require authentication before accepting delivery of a message. For the destination server(s) specified by this route, select the type of authentication required from one of the following methods:

- Anonymous access – No authentication credentials will be supplied
- Basic authentication – Supply a User name and Password accepted by the server
- Use sender's authentication – Use the User name and Password provided on the incoming connection to authenticate to the destination mail server

Deliver securely via TLS

Use an encrypted TLS connection to deliver messages to this server.

Email pattern or specific address

For a route to take effect, the message recipient must be matched by one or more entries in the list. Matches can be made by specifying specific user email addresses (e.g. `johndoe@domain.com`), or by specifying an email address pattern such as `*@businesspartner1.com`. Standard DOS wildcards (e.g. `*` and `?`) are used for matching addresses, with a * matching one or more characters, and a ? matching any one character.

For example:

Pattern: `*@bp1.com` matches `joe@bp1.com` but not `joe@mail.bp1.com`

Pattern: `*@mail?.bp1.com` matches `joe@mail1.bp1.com` and `joe@mail2.bp1.com`

Allow public relay to these entries

If an computer's IP address is allowed to connect to SMGW to send messages (via the Access Control window described above), but its IP address is not allowed to relay messages (via the Relay and Routing Control window described above), you can still specify certain email addresses or patterns that can receive messages from this computer. To allow this functionality, place a checkmark in this option.

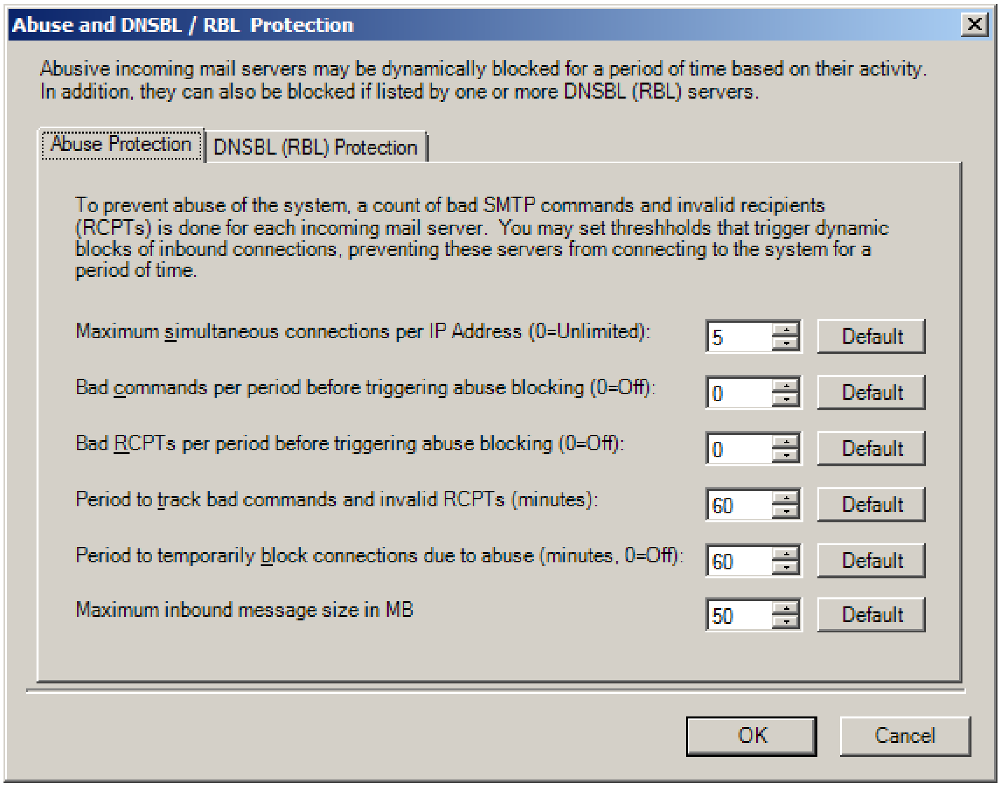
This feature can be used to prevent dictionary attacks which occur when a spammer's computer tries to send messages to randomly generated user names at your company's domain. At the RCPT TO chitchat level, before the message contents are delivered, recipients not in this allowed list will be denied, and an internal "abuse" counter associated with the offending computer will be incremented. By combining this feature with the Spam / Abuse Control feature described below, an abuse threshold can be set, allowing the connections of offending systems to be automatically terminated for a period of time, in effect, being placed on an automatic black list.

To add dictionary attack prevention to your system, follow these steps:

1. In Tools | Settings | Security | Access Control, allow all computers to connect to SMGW.
2. In Tools | Settings | Relay / Routing Control, prevent all computers except your internal mail server(s) to relay messages through SMGW.
3. Create a new entry in the Relay / Routing Tab and add a list of your employee email addresses.
4. Place a checkbox in "Allow public relay to these entries"
5. In Tools | Security | Spam Abuse Control, adjust the values to block out bad RCPTs for a period of time.

SECURITY TAB: SPAM / ABUSE CONTROL…

Figure 19 – Abuse and DNSBL / RBL Protection



Abuse and DNSBL / RBL Protection

Abusive incoming mail servers may be dynamically blocked for a period of time based on their activity. In addition, they can also be blocked if listed by one or more DNSBL (RBL) servers.

To prevent abuse of the system, a count of bad SMTP commands and invalid recipients (RCPTs) is done for each incoming mail server. You may set threshholds that trigger dynamic blocks of inbound connections, preventing these servers from connecting to the system for a period of time.

Maximum simultaneous connections per IP Address (0=Unlimited): 5

Bad commands per period before triggering abuse blocking (0=Off): 0

Bad RCPTs per period before triggering abuse blocking (0=Off): 0

Period to track bad commands and invalid RCPTs (minutes): 60

Period to temporarily block connections due to abuse (minutes, 0=Off): 60

Maximum inbound message size in MB 50

SMGW has several features that maximize system responsiveness and uptime, and allow it to server as an SMTP gateway server that protects your internal mail servers.

ABUSE PROTECTION TAB

Maximum simultaneous connections per IP Address

Mail servers may make more than one connection to SMGW to send messages. This is a useful technique that takes advantage of the multithreaded design of mail servers. However, the number of simultaneous connections in a system is finite, and a denial of service can occur if a mail server takes up too many simultaneous connections. Once the value specified in this option is reached, new connections from a particular computer will be denied until an existing connection is finished. Setting this value to 0 allows an unlimited number of simultaneous connections per IP address.

Bad commands per period before triggering abuse blocking

Normally, the SMTP chitchat between computers contains no bad commands or errors. However, a hacker may enter a combination of invalid commands to try to break the system. Provide a threshold value to surpass before triggering connection blocking for this

IP address. Setting this value to 0 allows an unlimited number of bad commands per IP address per period.

Bad RCPTs per period before triggering abuse blocking

If the allowed set of recipients is defined and public relay is disabled for a connecting computer's IP address, then SMGW will track the number of bad RCPT TO recipients during SMTP chitchat for each connecting IP address. If the entered threshold is exceeded, then the offending IP address will be prevented from making new connections to SMGW. This serves as a very strong method of dictionary attack prevention.

Details of the steps needed to fully enable this option can be found in the "Relay and Routing Control: Add / Edit…" section above.

Period to track bad commands and invalid RCPTs

For the bad commands per period and bad RCPTs per period options above, provide a value in minutes to track infractions for each IP address. This allows the system to keep track of all infractions from each IP address, even if they span across one or more connections. If the threshold to trigger abuse blocking is met, then new connections from the offending IP address will be blocked for a period of time specified in the option below. The tracking period starts when an offending IP address is first added to the bad RCPTs or bad command list, and ends when the specified tracking period in minutes has elapsed. Upon expiration, the offending IP address is removed from the tracking table until it issues another bad RCPT or bad command. Once the tracking period for an IP address expires, the IP address abuse record will be cleared from memory and new connections from the IP address will be allowed.

Period to temporarily block connections due to abuse

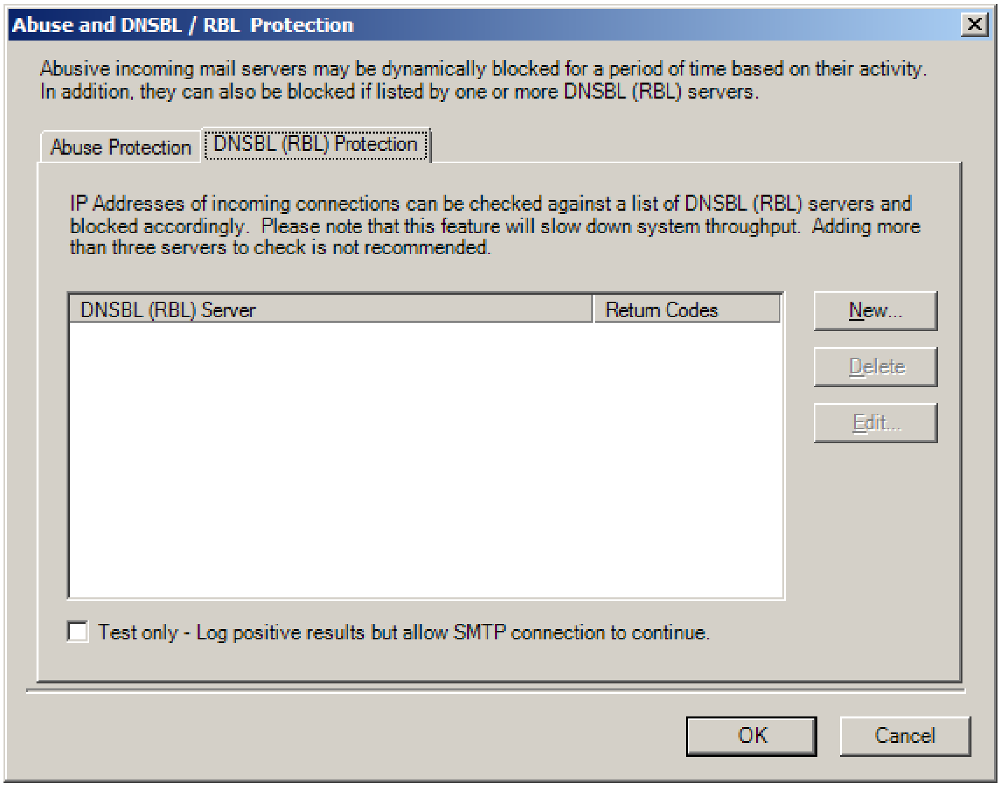
If an abuse threshold for bad RCPTs or bad commands per period is exceeded, specify in minutes that amount of time that must elapse before new connections will be allowed from this IP address.

Maximum inbound message size in MB

This setting specifies the maximum size of a message that will be evaluated. Larger messages will be rejected. Setting this value larger and then sending those larger messages will directly impact the amount of memory needed on the system to perform content scanning.

DNSBL (RBL) PROTECTION TAB

Figure 20 – DNSBL (RBL) Protection



Abuse and DNSBL / RBL Protection

Abusive incoming mail servers may be dynamically blocked for a period of time based on their activity. In addition, they can also be blocked if listed by one or more DNSBL (RBL) servers.

IP Addresses of incoming connections can be checked against a list of DNSBL (RBL) servers and blocked accordingly. Please note that this feature will slow down system throughput. Adding more than three servers to check is not recommended.

DNSBL (RBL) Server	Return Codes

☐ Test only - Log positive results but allow SMTP connection to continue.

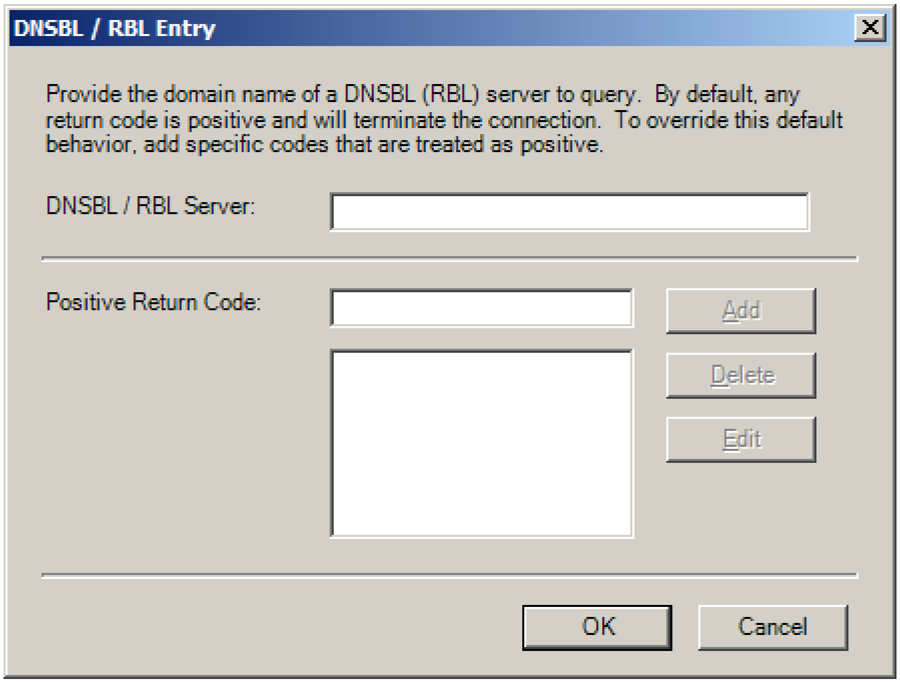
SMGW can check the IP address of each incoming connection against a list of DNSBL (RBL) servers. Those IP addresses that are found by this method can be blocked since they have been associated with spam activity.

Test Only

Check this box to log matches to the virtual server's SMTP log file, but still allow the connection to continue. This is useful when configuring the system to determine the result of adding one or more DNSBL (RBL) Servers.

New…

Figure 21 - DNSBL / RBL Entry



DNSBL / RBL Entry

Provide the domain name of a DNSBL (RBL) server to query. By default, any return code is positive and will terminate the connection. To override this default behavior, add specific codes that are treated as positive.

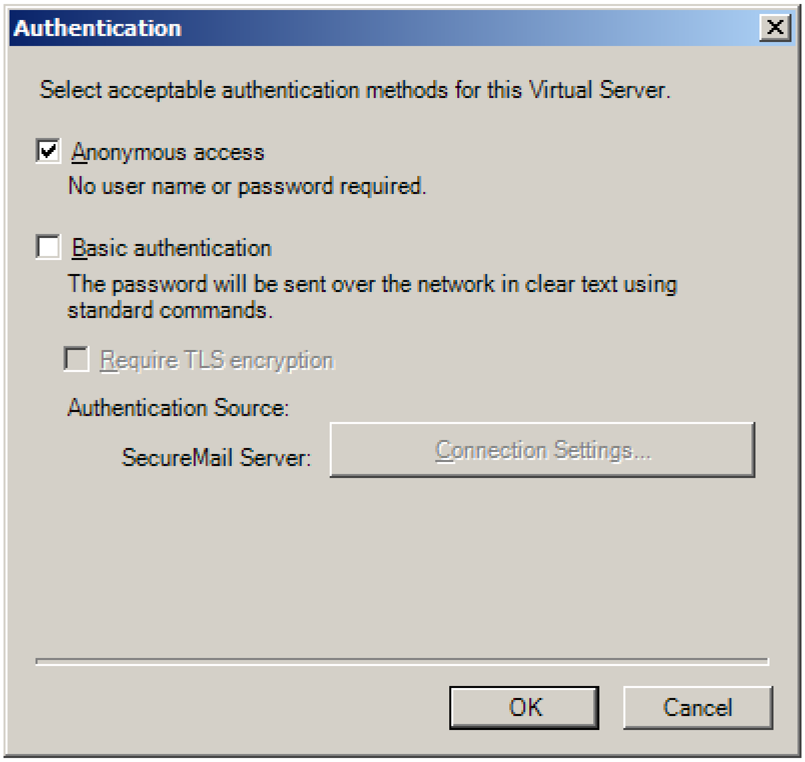
DNSBL / RBL Server:

Positive Return Code:

In the DNSBL / RBL Server field, enter the name of a server to submit queries. By default, any return code is positive and indicates that spam activity is associated with the submitted IP address. To override this behavior and trigger on only certain return codes, type them in the Positive Return Code field and click the Add button.

SECURITY TAB: AUTHENTICATION...

Figure 22 – Security Tab: Authentication



Authentication

Select acceptable authentication methods for this Virtual Server.

☑ Anonymous access
No user name or password required.

□ Basic authentication
The password will be sent over the network in clear text using standard commands.

□ Require TLS encryption

Authentication Source:

SecureMail Server:

SMGW can require valid authentication credentials from the sending computer before accepting an incoming message.

Anonymous access

No user name or password is required to send a message through SMGW. This is the default setting.

Basic authentication

By selecting “Basic authentication”, SMGW can integrate with a DataMotion Server to verify login credentials. This feature has been designed to allow DataMotion Server users to send secure DataMotion messages from their Internet email client without needing additional software or plug-ins. To accomplish this, the following high level steps should be taken:

1. Add a POP3 Internet mail profile to an email client
2. Set the outbound SMTP Server to the domain name of SMGW
3. Set the SMTP TLS option to encrypt messages sent via this profile.

4. Use their DataMotion Server username and password for outbound authentication.

Messages will then be sent through SMGW over an encrypted TLS link for subsequent secure delivery to any Internet recipient.

Require TLS encryption

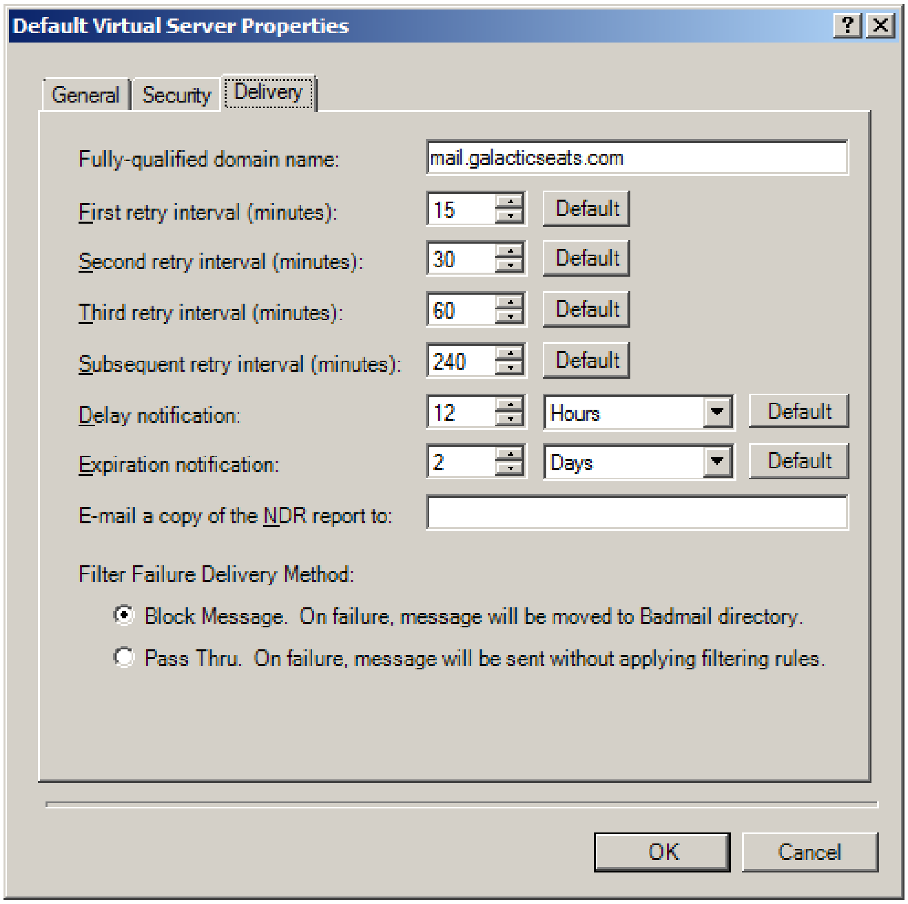
When selecting "Basic authentication", the login credentials are sent over a non-encrypted channel. Select this option to require an encrypted channel before accepting authentication data.

DataMotion Server: Connection Settings

Select the "Connection Settings…" button to display the Windows Data Link Properties window. Then provide the various parameters needed to make an SQL database connection from SMGW to your DataMotion Server.

VIRTUAL SERVER: DELIVERY TAB

Figure 23 – Virtual Server: Delivery Tab



Default Virtual Server Properties

Fully-qualified domain name: mail.galacticseats.com

First retry interval (minutes): 15 [Default]

Second retry interval (minutes): 30 [Default]

Third retry interval (minutes): 60 [Default]

Subsequent retry interval (minutes): 240 [Default]

Delay notification: 12 Hours [Default]

Expiration notification: 2 Days [Default]

E-mail a copy of the NDR report to:

Filter Failure Delivery Method:

● Block Message. On failure, message will be moved to Badmail directory.

○ Pass Thru. On failure, message will be sent without applying filtering rules.

Fully-qualified domain name

Set the display name that this SMGW virtual server will use to identify itself during SMTP transfers. If this field is left blank, the SMGW virtual server will perform a reverse DNS lookup on its IP address and use the name that is returned.

First retry interval

When a message cannot be delivered, the SMGW virtual server will wait for a period of time before attempting to send the message again. Set the value in minutes.

Second retry interval

Similar to the "First retry interval" above, set the value in minutes to wait before retrying message delivery after two unsuccessful delivery attempts.

Third retry interval

After three unsuccessful message delivery attempts, set the value in minutes to wait before trying to resend the message again.

Subsequent retry interval

Set the value in minutes to wait before trying to resend when message delivery has failed for more than three times.

Delay notification

SMGW will send the message sender a delay notification when a message has not been successfully delivered after a certain period of time. Set the time that must elapse before this delay notice is sent.

Expiration notification

After a defined period of time, SMGW will send the message sender a message expiration notice indicating that the message could not be sent. In addition, upon message expiration, no further attempts will be performed to deliver the message. Set the amount of time that must elapse before this expiration event occurs.

Email a copy of the NDR report to

When all delivery attempts have been exhausted for an email message, the message sender will receive an email message containing message expiration information. To have a second user such as a postmaster also receive a copy of this expiration message, add their email address to this field.

Filter Failure Delivery Method

When a message fails to be successfully scanned for any reason, this specifies what to do with the message. Block Message will cause the message to be placed into the Badmail folder and not be sent. Pass Thru will send the message directly as if there were no matches to any policies. The failures will be logged in either case.

5
User Groups

DEFINING AND MANAGING GROUPS OF USERS

A frequently used feature of the SMGW is User Groups. Through this feature, groups of users represented by their e mail addresses can be defined and then selected for use in Policies and Rules. Significant flexibility is provided for defining these groups, including:

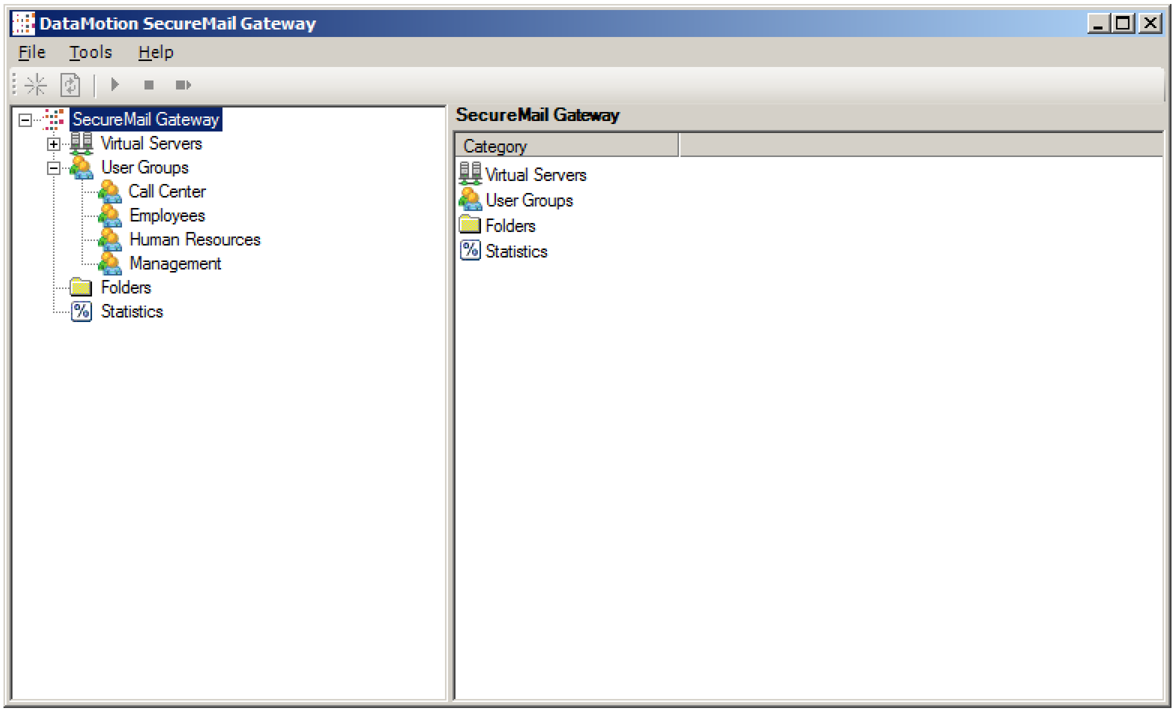
- manual entry of individual email addresses
- pattern matching of email addresses using wildcards and Regular Expressions
- bulk import of email addresses from an external file
- dynamic importing of email addresses from an external file with automatic background updating when the file is changed

In addition, groups can contain other groups, allowing for example, an Employees group to contain the Management, Call Center, Human Resources and Accounting groups.

When defining and managing User Groups, it is often beneficial to use its included drag and drop capabilities via the computer mouse. With drag and drop, users and groups can be quickly copied or moved between groups.

To work with User Groups, double click and expand the User Groups category in the left pane of the main window. (Note: If no User Groups have been defined, this category will not yet expand.) The following screen will be displayed (for illustration purposes, the image presented has several groups already defined):

Figure 24 – User Groups



User Groups that are defined appear in the tree under the User Groups category. In the pane at right, each individual User Group is displayed, along with the following columns:

Users – The number of user email address entries manually entered or imported into the group.

Groups – The number of other User Groups that this group contains.

Patterns – The number of wildcard or Regular Expression pattern matches that the group contains.

Files – The number of dynamic file links that the group contains.

Following are the actions that are available to administer User Groups:

NEW USER GROUP

When the User Groups category is highlighted in the tree list, select the New User Group icon ✳ from the toolbar to create a new User Group. This feature is also available through the right-click popup menu for this item. When this feature is selected, the User Group window will be displayed. The functionality of this window is described in the following section.

MANAGE USERS

Once a User Group is defined, you can manage its individual entries through the Manage User Group option. This option is available through the Properties toolbar icon ▤ and the right-click popup menu, and displays the Manage User Group Window. The Manage User Group Window section covers this feature in detail.

RENAME

Highlight the desired group to rename, and then display the popup menu by right-clicking on that item. Choose the Rename menu item to rename this User Group.

DELETE

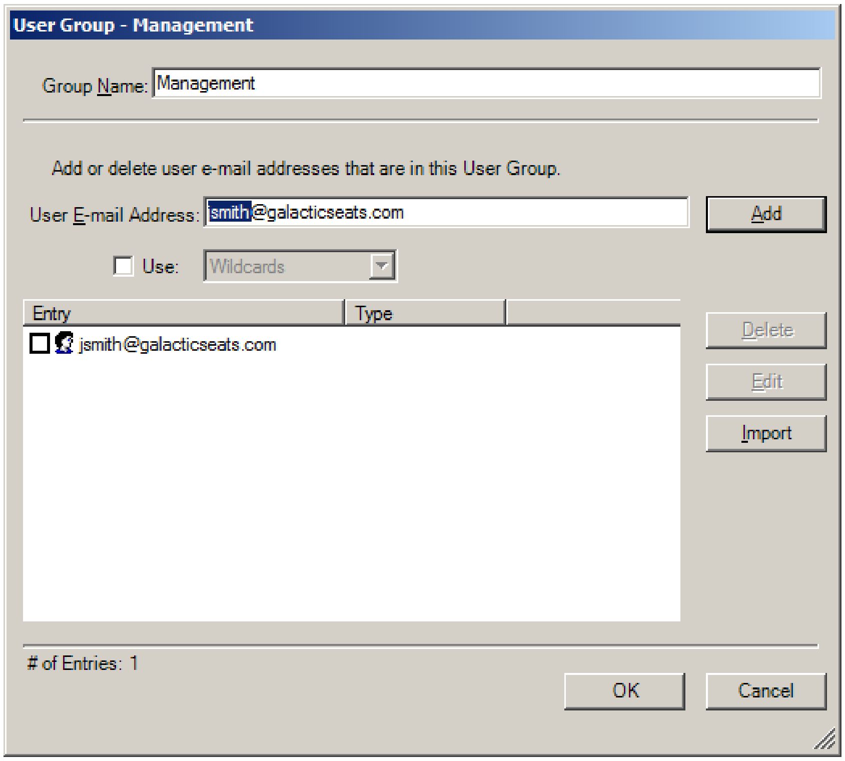
To delete a User Group, first highlight the group to be deleted. Specific User Groups are displayed by expanding the User Groups category in the tree in the left pane, or by highlighting the User Groups category and then selecting a User Group in the right pane. Once the desired User Group is highlighted, click the Delete toolbar icon ✕ or select the Delete menu item from the right-click popup menu.

A warning message will be displayed, displaying the group name and number of entries in the group. Select the 'Yes' button to delete the group, or 'No' to cancel the deletion.

MANAGE USER GROUP WINDOW

When selected, the User Group window will be displayed with the contents of the highlighted User Group:

Figure 25 – User Group Window



User Group - Management

Group Name: Management

Add or delete user e-mail addresses that are in this User Group.

User E-mail Address: jsmith@galacticseats.com

☐ Use: Wildcards

Entry	Type
☐ jsmith@galacticseats.com	

# of Entries: 1

The User Group window is comprised of the following items:

Group Name – Displays the name of the User Group. This is a required field.

User Email Address – Type in the email address to add to the entry list. Then click the Add button. As is shown in Figure 23, when the Add button is pressed, the prefix of the email address is highlighted and the focus returns to quickly enter a new address.

Wildcards and Regular Expressions – To match an email address pattern, check the "Use:" checkbox and choose between Wildcards or Regular Expressions. Then, in the User Email Address text box, type in the Wildcard or Regular Expression pattern to match. After the pattern has been entered, press the Add button.

Add button – Adds the entry in the User Email Address field to the list.

Delete button – Deletes all checked items in the list.

Edit button – Edits the currently highlighted item in the list.

Import button – Utilizes the contents of an external text file for inclusion into the list of email addresses in the group. When selected, the Import File window is displayed. Its use is described in the Import File Window section of Appendix A.

OK button – Accepts any changes and returns to the previous window.

Cancel button – Ignores any changes and returns to the previous window.

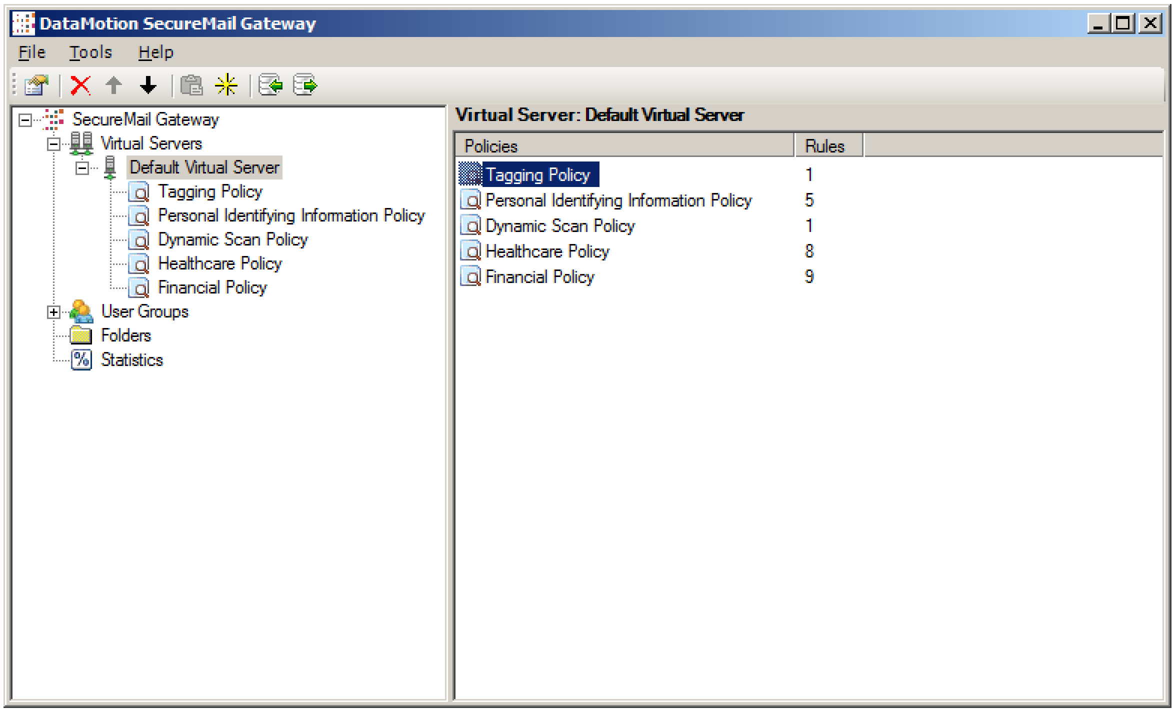
6
Policies

RULES AND ACTIONS FOR YOUR EMAIL TRAFFIC

The SMGW uses Policies to organize its filtering rules and actions. Each Policy has properties associated with it to determine if a message matches that Policy. If a match is found, then the message is examined by all of the Rules associated with the Policy. If a Rule matches the message, its Actions will then be performed. Policies are processed in the order that they are listed in the Rules Manager interface. For flexibility, an Action is available to skip the remaining Rules and Policies when an appropriate Rule is matched.

Policies are associated with Virtual Servers, and as such are grouped under the Virtual Server where its filters are applied. A number of policies are provided by default when the initial Virtual Server is created.

Figure 26 – Virtual Server Policies View



Virtual Server: Default Virtual Server

Policies	Rules
Tagging Policy	1
Personal Identifying Information Policy	5
Dynamic Scan Policy	1
Healthcare Policy	8
Financial Policy	9

For more information about the provided policies, see the *DataMotion SecureMail Gateway Quick Start Guide*.

Following are the actions available from the Policies category:

New Policy – Click on the New Policy toolbar icon ✳ or select New from the right-click popup menu.

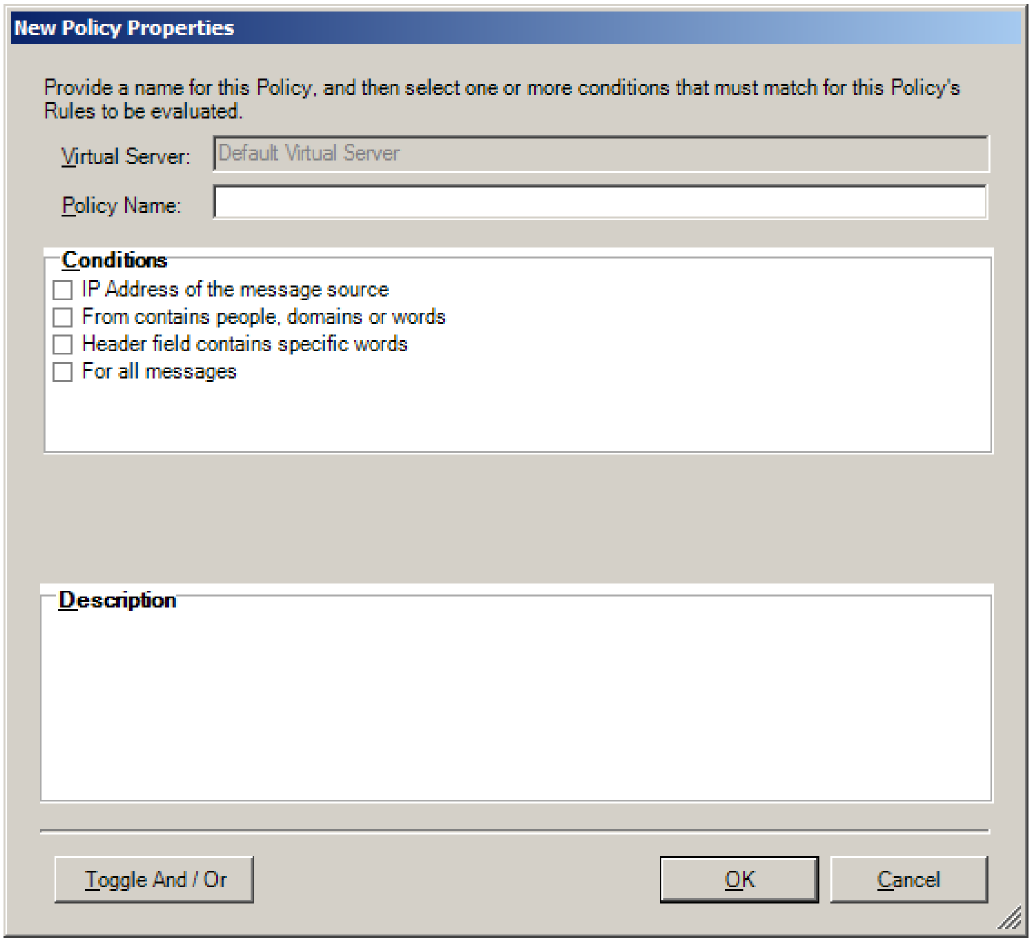
Import All Policies – Imports and overwrites the existing policies from a file via the Import toolbar icon or popup menu.

Export All Policies – Saves the results in the right pane to file via the Export toolbar icon or popup menu.

NEW POLICY

When creating a new policy, the following window will be displayed.

Figure 27 – New Policy Properties



New Policy Properties

Provide a name for this Policy, and then select one or more conditions that must match for this Policy's Rules to be evaluated.

Virtual Server: Default Virtual Server

Policy Name:

Conditions

□ IP Address of the message source
□ From contains people, domains or words
□ Header field contains specific words
□ For all messages

Description

Policy Name

Provide a display name for this policy.

Virtual Server

If more than one SMTP Virtual Server is defined, select the Virtual Server that this policy will apply to.

Conditions

To determine which Policies and their respective Rules and Actions are performed on a message, select one or more of the following policy conditions.

IP Address of the message source – To match the IP Address of the computers that will send messages through SMGW, enter a specific IP Address or range of IP Addresses. When selected, the IP Address Editor described in Appendix A will be used to edit this entry.

From contains people, domains or words – Provide one or more email addresses or wild pattern that must match to trigger this policy. The Email Address Entry Editor described in Appendix A will be used to edit this entry.

Header field contains specific words – Provide one or more values or wildcard patterns that, if found in the header field, will trigger this condition. The Text Entry Editor described in Appendix A will be used to edit this entry.

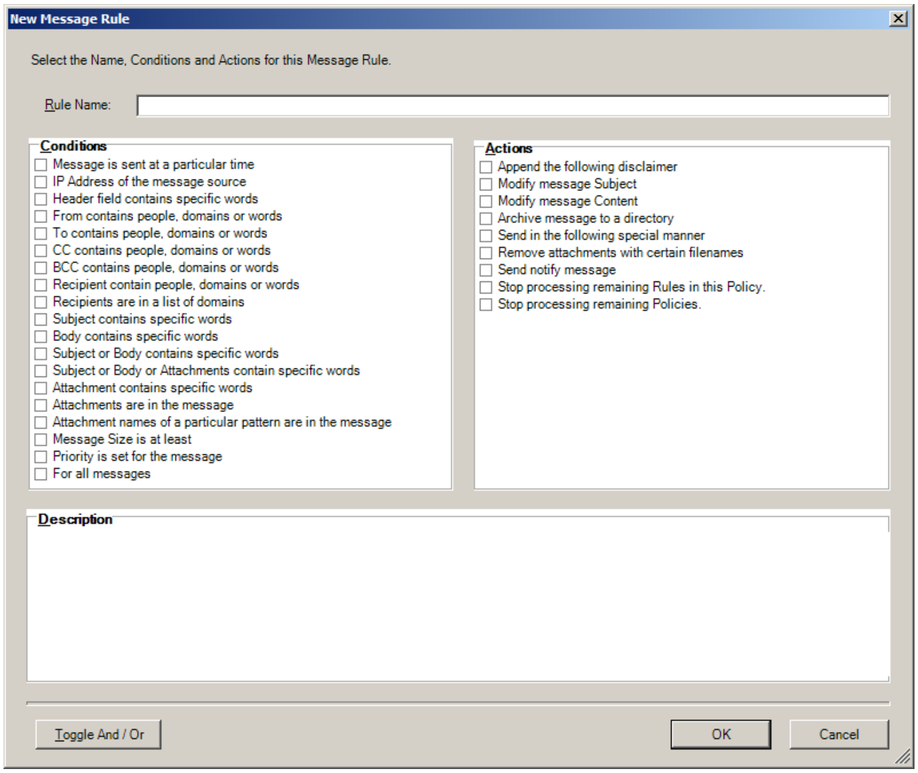
For all messages – This condition will be triggered for all messages going through this Virtual Server.

Toggle And / Or – By pressing this button, which resides in the bottom left corner of the window, the results of condition matches can be evaluated individually or in combination. "Or" logic will trigger the policy if any one condition matches, whereas "And" logic will trigger the policy if each defined condition matches.

OK – Select the OK button to accept the Policy conditions. If this is a newly defined Policy, no Rules or Actions will exist yet, and the SecureMail Gateway will display a dialog window prompting to create new Rules at this time.

RULE EDITOR

Figure 28 – Rule Editor



New Message Rule

Select the Name, Conditions and Actions for this Message Rule.

Rule Name:

Conditions

- □ Message is sent at a particular time
- □ IP Address of the message source
- □ Header field contains specific words
- □ From contains people, domains or words
- □ To contains people, domains or words
- □ CC contains people, domains or words
- □ BCC contains people, domains or words
- □ Recipient contain people, domains or words
- □ Recipients are in a list of domains
- □ Subject contains specific words
- □ Body contains specific words
- □ Subject or Body contains specific words
- □ Subject or Body or Attachments contain specific words
- □ Attachment contains specific words
- □ Attachments are in the message
- □ Attachment names of a particular pattern are in the message
- □ Message Size is at least
- □ Priority is set for the message
- □ For all messages

Actions

- □ Append the following disclaimer
- □ Modify message Subject
- □ Modify message Content
- □ Archive message to a directory
- □ Send in the following special manner
- □ Remove attachments with certain filenames
- □ Send notify message
- □ Stop processing remaining Rules in this Policy.
- □ Stop processing remaining Policies.

Description

The Rule Editor allows new rules to be created, and existing rules to be modified. Each rule is comprised of Conditions that must be met to trigger the rule, and Actions that will be carried out if the Conditions are met.

Rule Name

The Rule Name field contains the descriptive name of this rule.

Conditions

Similar to the Policy conditions described above, each rule must contain one or more conditions that a message must match before the actions associated with the rule will be implemented. The conditions provided by SMGW to examine a message are as follows.

Message is sent at a particular time – Select from among the various days of the week and hours of each day. These values will be used to match the message header Date field. If no Date field is present in the message, the time that the message was processed by SMGW will be used. The Time of Day Editor described in Appendix A will be used to edit the values of this field.

IP Address of the message source – When a computer connects to SMGW to send a message, its IP Address is recorded along with the message. Use this condition to set one or more IP Addresses or ranges of IP Addresses to match. The IP Address Editor described in Appendix A will be used to add and edit values for this condition.

Header field contains specific words – The message header contains many useful fields containing information about the origin, composition and for some third-party anti-spam systems, the spam score of the message. Use the Text Entry Editor described in Appendix A to define entries to be searched for in the header of the message.

From contains people, domains or words – Use the Email Address Entry Editor described in Appendix A to define entries to be searched for in the From field of the message.

To contains people, domains or words – Use the Email Address Entry Editor described in Appendix A to define entries to be searched for in the To field of the message.

CC contains people, domains or words – Use the Email Address Entry Editor described in Appendix A to define entries to be searched for in the CC field of the message.

BCC contains people, domains or words – While not displayed in the message itself, SMGW can determine BCC recipients through the SMTP chit chat session it had with the sending computer when it receives a message. Use the Email Address Entry Editor described in Appendix A to define BCC entries to be searched in the message.

Recipient contains people, domains or words – Recipient is any email address listed in the To, CC or BCC fields. This condition will search across these three fields to find a match. Use the Email Address Entry Editor described in Appendix A to define entries to be searched for among message recipients.

Subject contains specific words – The message subject is displayed by email clients when viewing a message. Use the Text Entry Editor described in Appendix A to define entries for this condition.

Body contains specific words – The message text and HTML body can be scanned for certain words or phrases. Use the Text Entry Editor described in Appendix A to define entries for this condition.

Subject or Body contains specific words – Scan the message subject, and the message text and HTML body for specific words or phrases. Use the Text Entry Editor described in Appendix A to define entries for this condition.

Attachment contains specific words – Many types of message attachments can be scanned for certain words or phrases. However, certain message attachments may be written in a format that does not contain plain text words, and as such, will not produce the desired matching results. To determine if an attachment type will be successfully scanned, open it up in Windows Notepad and browse through the document. If relevant words can be viewed, and they appear as contiguous letters with no extraneous symbols or spaces between them, then that attachment type can be scanned. In some cases, words may be split across an internal boundary within the file, and not appear through this method as being contiguous. SMGW will not be able to match these words.

The Text Entry Editor described in Appendix A will be used to define entries for this condition.

Attachments are in the message – SMGW can scan messages and count the number of document attachments contained in them. Select the number of attachments that a message must have to match this condition.

Attachment extensions of a particular type are in the message – The names of attached documents frequently have file extensions that identify them to the system. Use the Text Entry Editor described in Appendix A to define entries for this condition.

Message Size is at least – Provide a value in kilobytes (KB) that must be exceeded for this condition to be matched.

Priority is set for the message – Most email clients allow a message to be flagged with Low or High priority. Select from one of these two values to match this condition.

For all messages – When selected, all other conditions for this rule will be cleared, and all messages that are evaluated by this rule will have its actions implemented.

Toggle And / Or

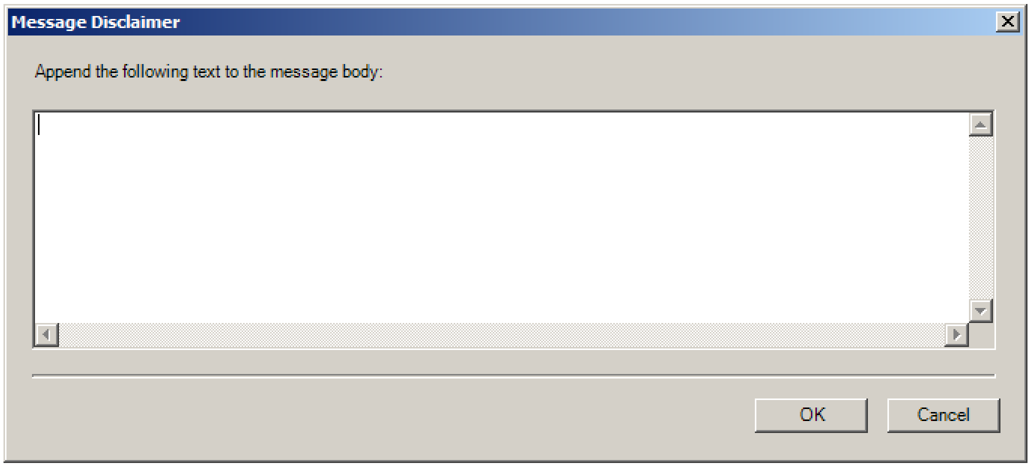
By default, a rule is considered matched when any one of its conditions is matched. When more than one condition is defined for a rule, the "Toggle And / Or" button will be enabled. By selecting this button, the matching criteria for this rule will be toggled between "any one condition must match", which maps into its "Or" logic, to "all conditions must match," which maps into its "And" logic.

Actions

When the conditions for a rule have been matched, the actions defined for that rule will be implemented. Following are the actions that are provided.

Append the following disclaimer – A message disclaimer can be appended to messages that match the conditions of a rule. This disclaimer will be appended to available text and HTML portions of the message. The following window will be displayed allowing a disclaimer to be provided.

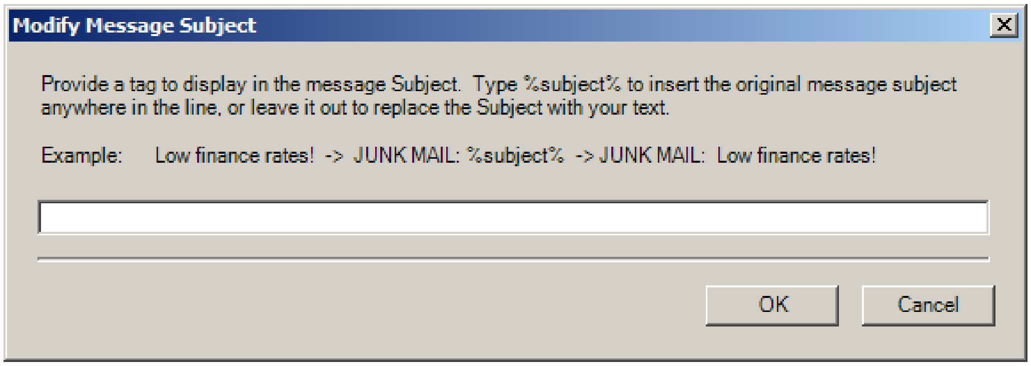
Figure 29 – Actions: Message Disclaimer



Append the following text to the message body:

Modify message Subject – Select this option to modify or replace the message Subject field. When selected, the following window will be displayed.

Figure 30 – Actions: Modify Message Subject



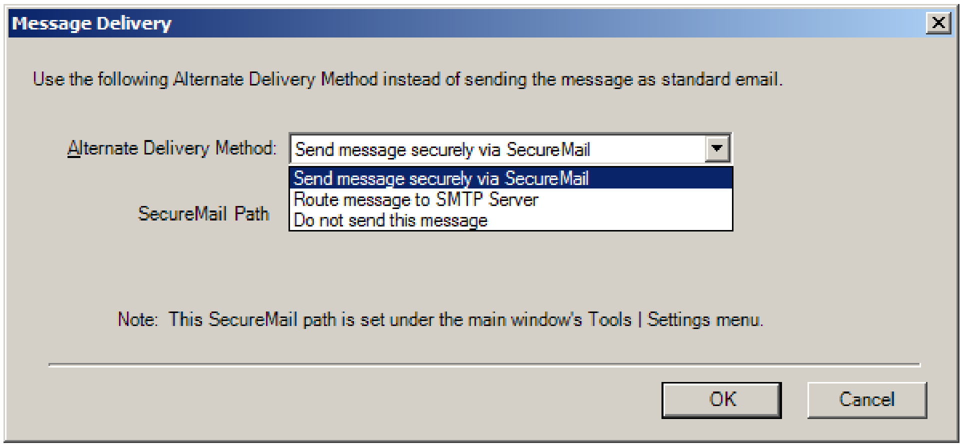
Provide a tag to display in the message Subject. Type %subject% to insert the original message subject anywhere in the line, or leave it out to replace the Subject with your text.

Example: Low finance rates! -> JUNK MAIL: %subject% -> JUNK MAIL: Low finance rates!

To replace the subject, type an alternate subject in the field provided. The text of the original subject can also be inserted into the new subject line by inserting a %subject% token into the new text.

Send in the following special manner – Message delivery can be altered in one of several ways.

Figure 31 – Actions: Send in the following special manner



Message Delivery

Use the following Alternate Delivery Method instead of sending the message as standard email.

Alternate Delivery Method: Send message securely via SecureMail

Send message securely via SecureMail
Route message to SMTP Server
Do not send this message

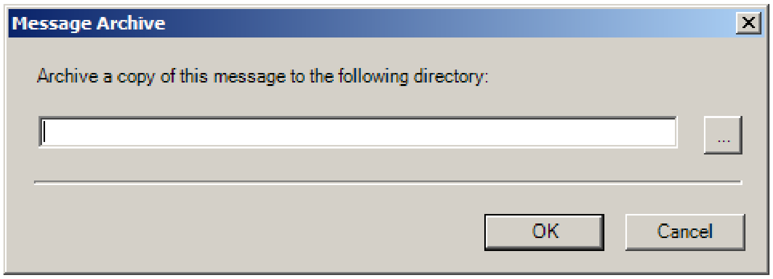
SecureMail Path

Note: This SecureMail path is set under the main window's Tools | Settings menu.

- **Send message securely via DataMotion** – Messages will be routed to your DataMotion Server or the DataMotion SaaS site for encrypted delivery with tracking to their Internet email recipients. The routing method is defined in the Email Address Entry Editor section.
- **Route message to SMTP Server –** This option will override DNS routing, and will also override any Routes that have been defined in the Relay / Routing Tab section.
- **Do not send this message** – Delivery of the message will not be attempted. This is useful, for example, when an unwanted message is detected and SMGW should not attempt delivery of that message.

Archive message to a directory – The message can be saved in MIME format to a directory for later review. Type in a directory path in the field provided.

Figure 32 – Actions: Archive message to a directory



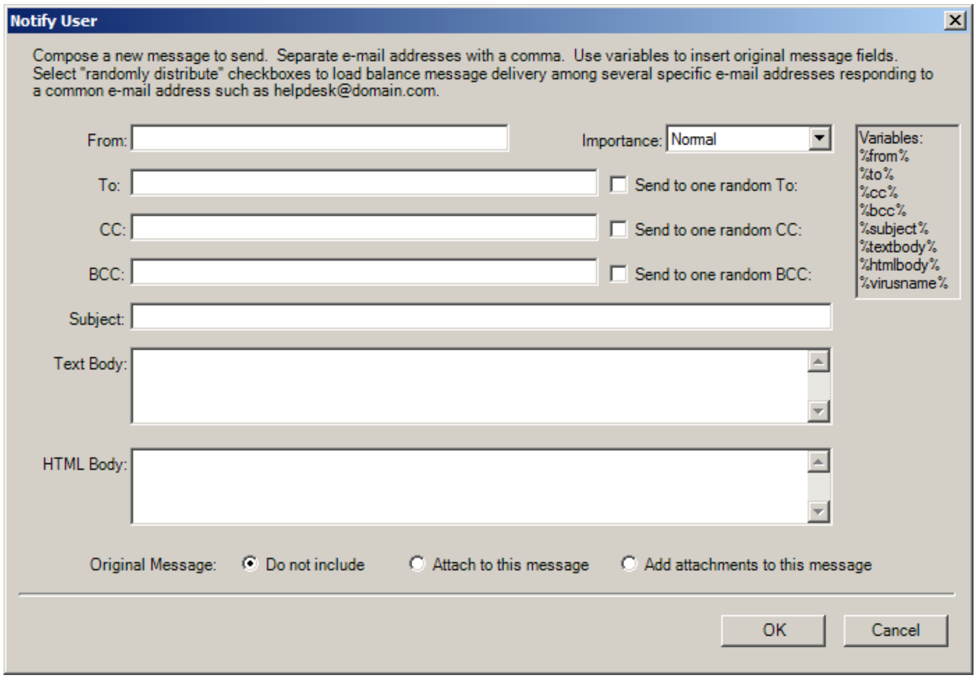
Message Archive

Archive a copy of this message to the following directory:

Remove attachments with certain extensions – Certain message attachments can be stripped from the message based on their filename. The Attachment Matching Condition window will be displayed, allowing filenames and patterns to be defined. This window is based on the Text Entry Editor described in Appendix A.

Send notify message – Based on a message matching your defined conditions, a new email message can be generated and sent by SMGW. This email message can be sent to one or more recipients, and for help desk or call center scenarios, to a random recipient specified in a list of users. A copy of the original message or just its attachments can also be sent in this new message.

Figure 33 – Actions: Send notify message



Notify User

Compose a new message to send. Separate e-mail addresses with a comma. Use variables to insert original message fields. Select "randomly distribute" checkboxes to load balance message delivery among several specific e-mail addresses responding to a common e-mail address such as helpdesk@domain.com.

From:
Importance: Normal
To: □ Send to one random To:
CC: □ Send to one random CC:
BCC: □ Send to one random BCC:
Subject:
Text Body:
HTML Body:

Variables:
%from%
%to%
%cc%
%bcc%
%subject%
%textbody%
%htmlbody%
%virusname%

Original Message: ● Do not include ○ Attach to this message ○ Add attachments to this message

OK Cancel

Various fields in the original message can be placed into the newly generated message. These fields are represented by the tokens that appear in the panel on the top right side of the window.

Stop processing remaining Rules in this Policy – A Policy can consist of many Rules executed in order from top to bottom as they appear in the Policy's Rules list. Select this option to prevent the remaining Rules in a Policy from being evaluated when a certain Rule match has occurred.

Stop processing remaining Policies – Similar to the above option, each Virtual Server can have more than one Policy applied to it. These Policies are also evaluated in top down order as they appear in the list. Select this option to prevent the remaining Policies from being evaluated when a certain Rule match has occurred.

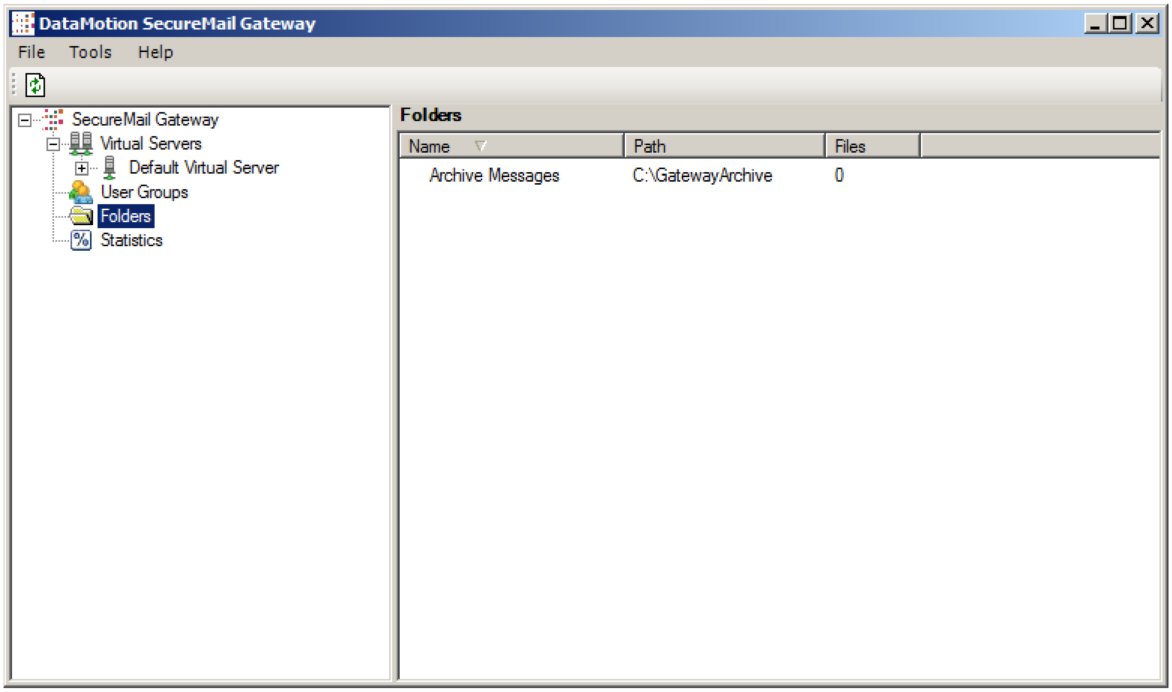
Description

As various Rule Conditions and Actions are selected, the Description panel of the Rule Editor will display a summary of all of the selections in effect. Blue underlined phrases in the description can be selected by mouse click to edit its corresponding action.

7
Folders

VIEW AND MANAGE ARCHIVED MESSAGES

Figure 34 – Folders

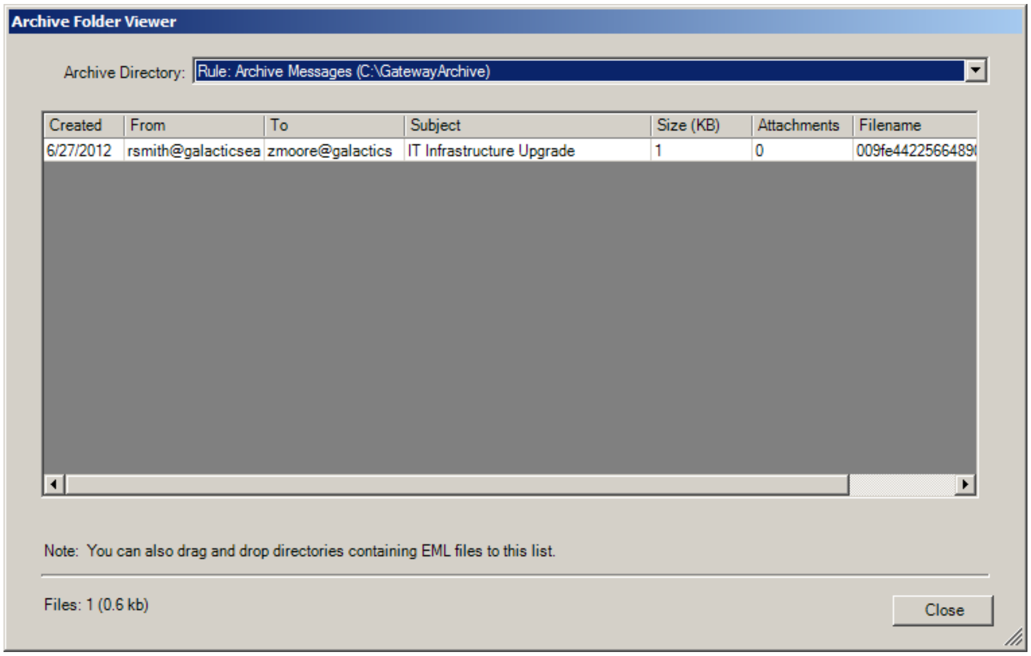


Name	Path	Files
Archive Messages	C:\GatewayArchive	0

The SecureMail Gateway Folders tree item displays information about all Rules that have an Action set to “Archive messages to a directory”. The columns displayed include the Rule Name, archive directory path, and number of files contained in the archive directory. By selecting a particular entry from the list, the following Archive Folder Viewer will be displayed for that directory.

ARCHIVE FOLDER VIEWER

Figure 35 – Archive Folder Viewer



Archive Folder Viewer

Archive Directory: Rule: Archive Messages (C:\GatewayArchive)

Created	From	To	Subject	Size (KB)	Attachments	Filename
6/27/2012	rsmith@galacticsea	zmoore@galactics	IT Infrastructure Upgrade	1	0	009fe4422566489

Note: You can also drag and drop directories containing EML files to this list.

Files: 1 (0.6 kb)

The Archive Folder Viewer shows information about each message contained in the archive directory, including their Date, From, To and Subject fields, each message size, number of attachments, and message filename.

Each of these columns can be sorted by clicking on their respective column header. Messages are stored in the archive directory as a MIME file containing an EML file extension. To view a particular message with an application associated with EML files (such as Windows Live Mail or Mozilla Thunderbird), highlight it and press Enter or double-click on it with the left mouse button. In addition, by right-clicking on an entry, a popup menu of additional options is available, including viewing the entry in Windows Notepad and deleting it.

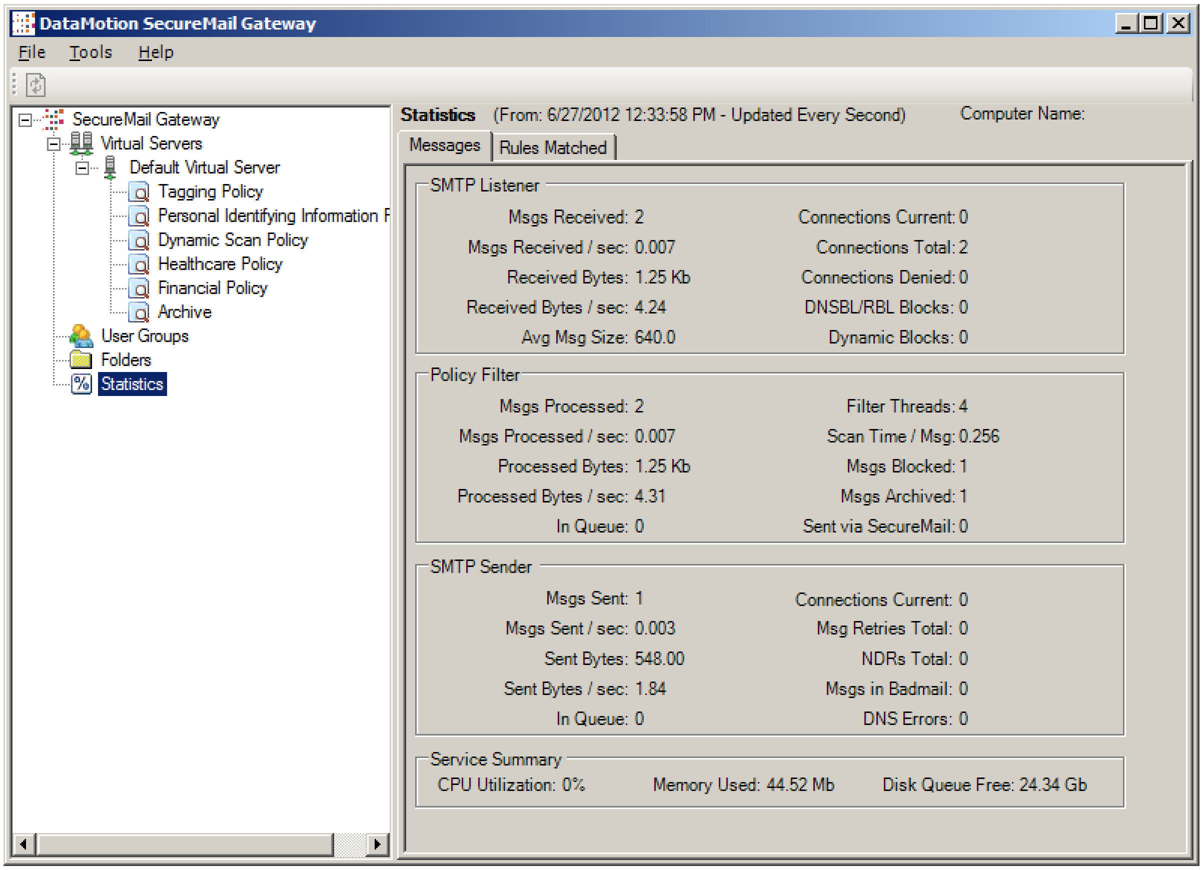
When the Archive Folder Viewer is loading its list of messages, a progress bar will be displayed indicating the proportion of messages that have been read into the list. SecureMail Gateway will cache the list information to disk, greatly decreasing the time that is required to reread information about previously displayed messages.

8
Statistics

MONITOR REAL TIME DATAMOTION SECUREMAIL GATEWAY STATISTICS

The SMGW SecureMail Gateway displays real-time statistics for the background SMTP Engine by selecting the Statistics tree item from its main menu. When selected, the following screen will be displayed.

Figure 36 - Statistics



Statistics (From: 6/27/2012 12:33:58 PM - Updated Every Second) Computer Name:

SMTP Listener

Msgs Received: 2 | Connections Current: 0
Msgs Received / sec: 0.007 | Connections Total: 2
Received Bytes: 1.25 Kb | Connections Denied: 0
Received Bytes / sec: 4.24 | DNSBL/RBL Blocks: 0
Avg Msg Size: 640.0 | Dynamic Blocks: 0

Policy Filter

Msgs Processed: 2 | Filter Threads: 4
Msgs Processed / sec: 0.007 | Scan Time / Msg: 0.256
Processed Bytes: 1.25 Kb | Msgs Blocked: 1
Processed Bytes / sec: 4.31 | Msgs Archived: 1
In Queue: 0 | Sent via SecureMail: 0

SMTP Sender

Msgs Sent: 1 | Connections Current: 0
Msgs Sent / sec: 0.003 | Msg Retries Total: 0
Sent Bytes: 548.00 | NDRs Total: 0
Sent Bytes / sec: 1.84 | Msgs in Badmail: 0
In Queue: 0 | DNS Errors: 0

Service Summary

CPU Utilization: 0% Memory Used: 44.52 Mb Disk Queue Free: 24.34 Gb

The Statistics display is updated once per second, and its values are reset each time the background SMTP Engine is restarted. So unless otherwise noted, each of the values indicated represent calculations made from the time it was last started. This time is noted at the top of the Statistics display.

Statistics are organized into four categories: SMTP Listener, Policy Filter, SMTP Sender and Service Summary.

SMTP LISTENER

Statistics related to messages being received by the SMTP Engine are displayed in the SMTP Listener section.

Msgs Received – The total number of successfully received messages.

Msgs Received / sec – The total number of successfully received messages divided by the total number of seconds that the service has been running. It may be possible to increase message throughput by increasing the number of simultaneous connections that the SMTP Listener component will accept. This value can be adjusted by referring to the "Limit number of connections to" section. After a certain number of simultaneous connections, however, the overhead of managing connections will increase to the point that the total message throughput on the system will decrease.

Received Bytes – The total number of bytes received by the service, including SMTP chit chat, and successful and aborted message deliveries.

Received Bytes / sec – The total number of received bytes divided by the total number of seconds that the service has been running.

Current Connections – The number of TCP connections currently in use to receive incoming messages.

Connections Total – The total number of connections accepted by the background service.

Connections Denied – Based on the properties defined in the Virtual Server Properties section, certain incoming connections may be denied. The number of connections denied is displayed by this entry.

DNSBL/RBL Blocks – When using DNSBL (RBL) Protection Tab to block incoming connections associated with spammers, this entry will display how many connections were blocked because of those settings.

Dynamic Blocks – The SMTP Engine can block incoming connections for a period of time based on connectivity activity defined to be abusive. This activity is defined in the Abuse Protection Tab section.

POLICY FILTER

Statistics related to Policies and Rules being processed by the SMTP Engine are displayed in the Policy Filter section.

Msgs Processed – Displays the total number of messages processed by the Policy Filter component of the SMTP Engine.

Msgs Processed / sec – Displays a calculation of the Msgs Processed value divided by the total number of seconds that have passed since the SMTP Engine service was last started.

Processed Bytes – The total size in bytes of all of the messages processed by the Policy Filter component of the SMTP Engine.

Processed Bytes / sec – A calculation of the Processed Bytes value divided by the total number of seconds that have elapsed since the SMTP Engine service was last started.

In Queue – Displays the total number of message files found in all Virtual Server Pickup directories. These message files are either waiting to be processed by the Policy Filter, or are currently in the process of being scanned for content filter rules. If this value grows over time, then the Policy Filter is not able to keep up with the pace of incoming messages into the system. To resolve this problem, either reduce the number of simultaneous connections that the SMTP Listener will accept, as defined in the "Limit number of connections to" section, reduce the number of Policies and Rules that must be processed, upgrade your system hardware, or consider installing an additional SMGW system in a load-balanced configuration.

Current Threads – The number of simultaneous messages that are currently being processed by the Policy Filter.

Scan Time / Msg – A calculation of the total number of seconds that the SMTP Engine has been running divided by the total Msgs Processed.

Msgs Blocked – The number of messages blocked from being sent. These messages were blocked by a message Rule that had one of its Actions set to "Send in the following special manner: Do not send this message."

Msgs Archived – The number of message copies written to an Archive directory. These messages were archived by a message Rule that had one of its Actions set to "Archive message to a directory."

Secure via DataMotion – The number of messages that were routed for secure delivery to a DataMotion Server or the DataMotion SaaS site. These messaged were routed by a message Rule that had one of its Actions set to "Send in the following special manner: Send message securely via DataMotion."

SMTP SENDER

Statistics related to messages being delivered by the SMTP Engine are displayed in the SMTP Sender section.

Msgs Sent – The number of messages successfully delivered to destination mail servers.

Msgs Sent / sec – A calculation of the Msgs Sent divided by the number of seconds that have elapsed since the SMTP Engine was started.

Sent bytes – The total number of bytes sent by the SMTP Engine while trying to delivery messages.

Sent bytes /sec – A calculation of the Sent bytes divided by the number of elapsed seconds since the SMTP Engine was started.

In Queue – The total number of message files awaiting delivery for the SMTP Engine. For each enabled Virtual Server, all files in their corresponding Send directory are counted.

Current Connections – The number of connections currently being used to deliver messages to destinations mail servers.

DNS Lookups – The total number of recipient email address resolved either by Internal Cache matches or external DNS Server lookups.

via Internal Cache – The number of recipient mail servers that were resolved by finding their DNS entry in internal cache memory. Entries are added to the cache each time a new, successful DNS domain lookup occurs. Entries are removed when their individual expiration times have elapsed.

via DNS Servers – The number of recipient mail servers that were resolved by making a query to external DNS servers.

Lookups not found – The number of recipient email addresses that could not be resolved by a query to external DNS servers.

SERVICE SUMMARY

Statistics related to the overall operation of the SMTP Engine service is displayed in the Service Summary section.

CPU Utilization – The percentage of CPU resources being used by the SMTP Engine service.

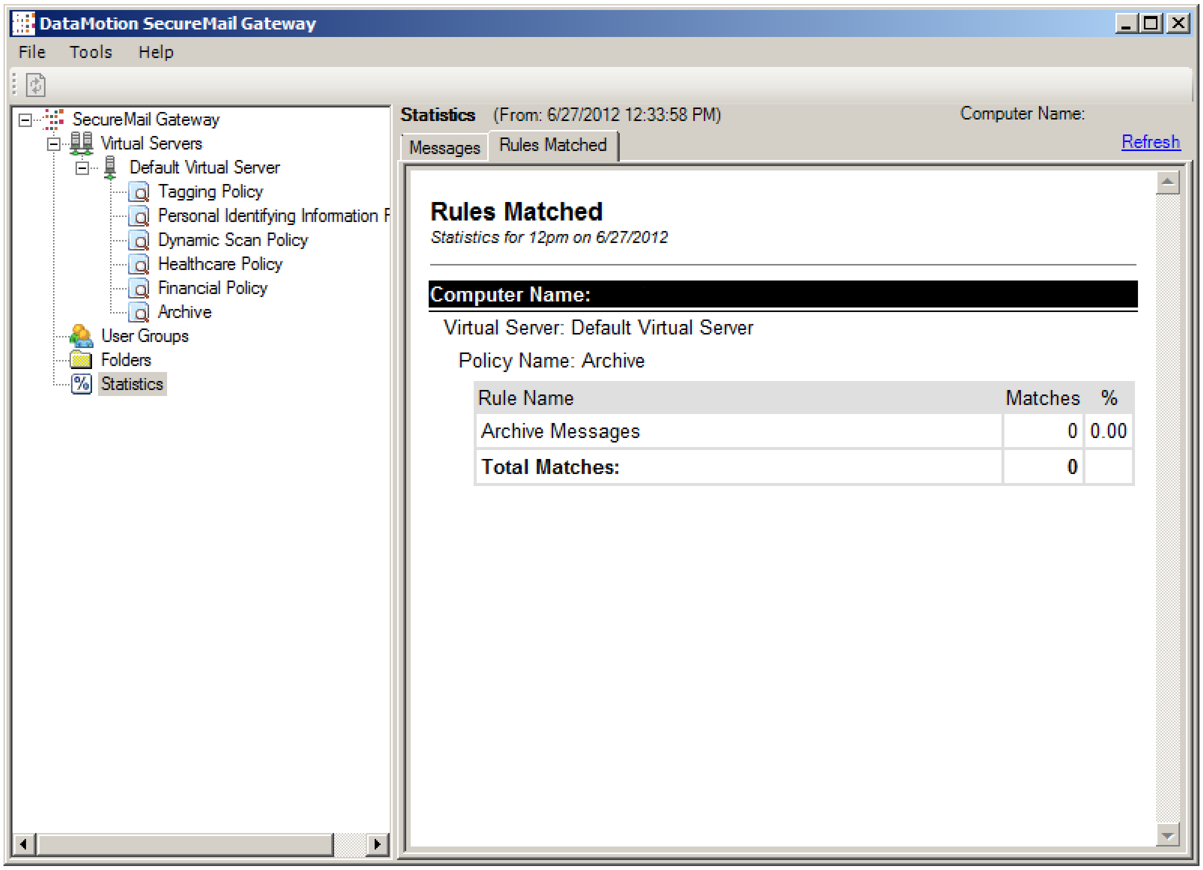
Memory Used – The amount of memory being used by the SMTP Engine service.

Disk Queue Free – The amount of free space on the hard drive where the SMTP Engine service is run. By default, message queue directories used by Virtual Servers are located on this drive. However, if a base directory relocated to a different drive, the free space on this drive will not be represented by this value.

MONITOR POLICY RULE MATCHES

When Rule Statistics have been enabled in the SMGW settings, a new tab appears in the Statistics area titles Rules Matched. This shows statistics about the policy rule matches on messages that have been sent through the SMGW.

Figure 37 – Rules Matched View



Statistics (From: 6/27/2012 12:33:58 PM) Computer Name:

Rules Matched

Statistics for 12pm on 6/27/2012

Computer Name:

Virtual Server: Default Virtual Server

Policy Name: Archive

Rule Name	Matches	%
Archive Messages	0	0.00
Total Matches:	**0**	

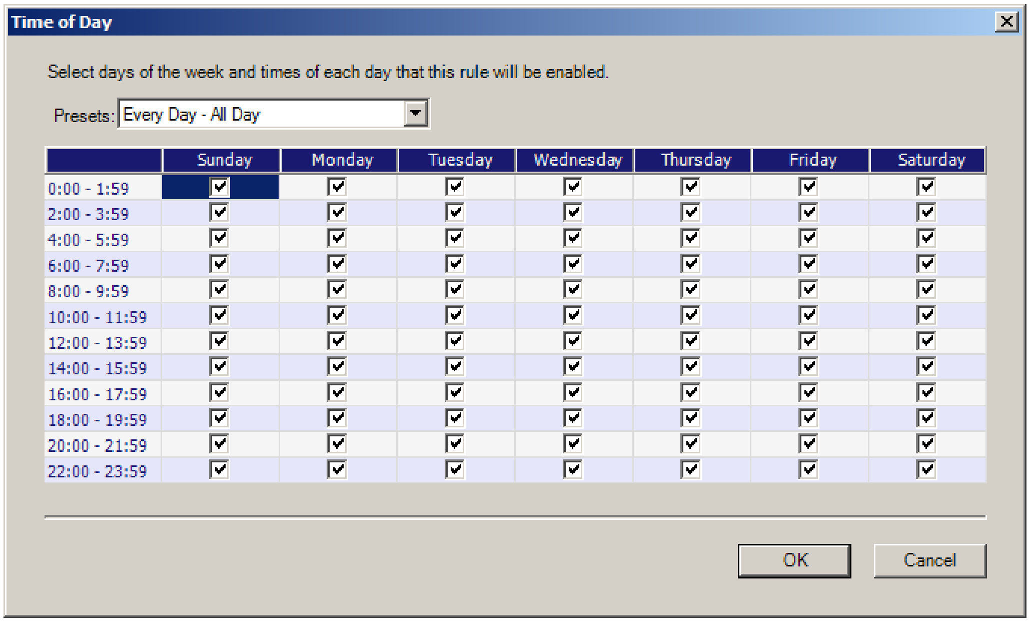
9
Appendix A: Gateway Editors

DIALOGS FOR ADDING SPECIAL DATA TYPES

TIME OF DAY EDITOR

For SMGW options that allow a time of day and day of week to be specified, the Time of Day editor will be displayed.

Figure 38 – Time of Day Editor



Time of Day

Select days of the week and times of each day that this rule will be enabled.

Presets: Every Day - All Day

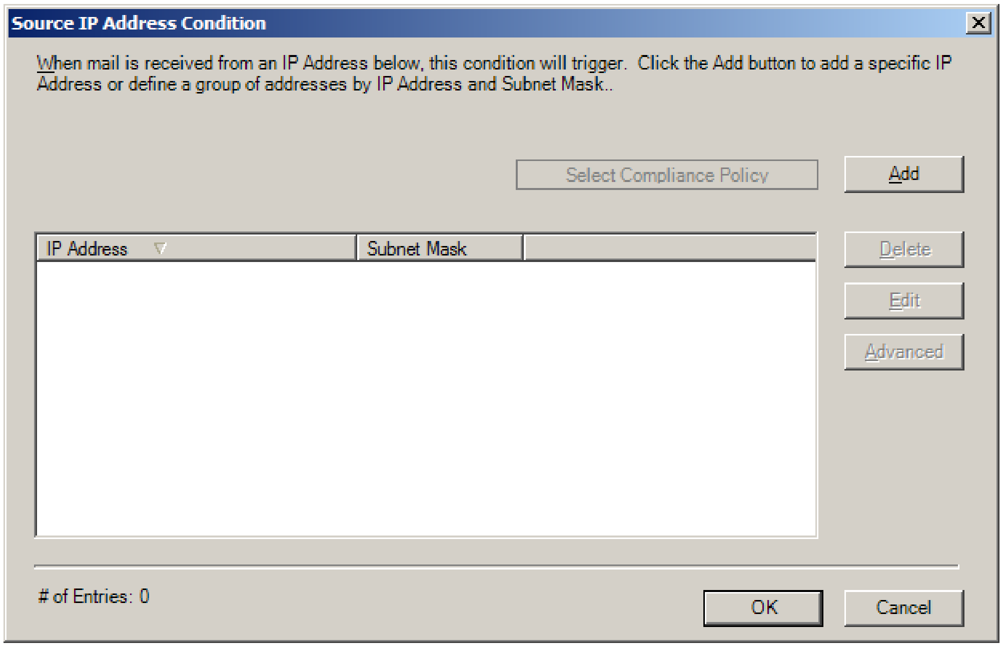
	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
0:00 - 1:59	☑	☑	☑	☑	☑	☑	☑
2:00 - 3:59	☑	☑	☑	☑	☑	☑	☑
4:00 - 5:59	☑	☑	☑	☑	☑	☑	☑
6:00 - 7:59	☑	☑	☑	☑	☑	☑	☑
8:00 - 9:59	☑	☑	☑	☑	☑	☑	☑
10:00 - 11:59	☑	☑	☑	☑	☑	☑	☑
12:00 - 13:59	☑	☑	☑	☑	☑	☑	☑
14:00 - 15:59	☑	☑	☑	☑	☑	☑	☑
16:00 - 17:59	☑	☑	☑	☑	☑	☑	☑
18:00 - 19:59	☑	☑	☑	☑	☑	☑	☑
20:00 - 21:59	☑	☑	☑	☑	☑	☑	☑
22:00 - 23:59	☑	☑	☑	☑	☑	☑	☑

Times of the day are listed down each row, and days of the week are listed across each column. A checkbox that intersects a time of day and day of week represents a particular time on a particular day. To enable an action to occur at a particular time and day, place a check in its corresponding checkmark.

Certain Presets are provided to allow one click selection of common time periods such as "Weekdays – All day" and "Every Day – Off peak."

IP ADDRESS EDITOR

Figure 39 – IP Address Editor



Source IP Address Condition

When mail is received from an IP Address below, this condition will trigger. Click the Add button to add a specific IP Address or define a group of addresses by IP Address and Subnet Mask..

IP Address	Subnet Mask

# of Entries: 0

When an option allows a list of IP Addresses to be entered, the IP Address Editor will be used. IP Address entries can contain specific addresses and ranges of IP Addresses using Subnet Mask syntax.

The following actions are provided by the IP Address Editor.

Add – Allows a new IP Address or range to be added. When selected, the dialog window described in Figure 12 will be displayed.

Delete – Deletes the currently highlighted IP Address entry in the list.

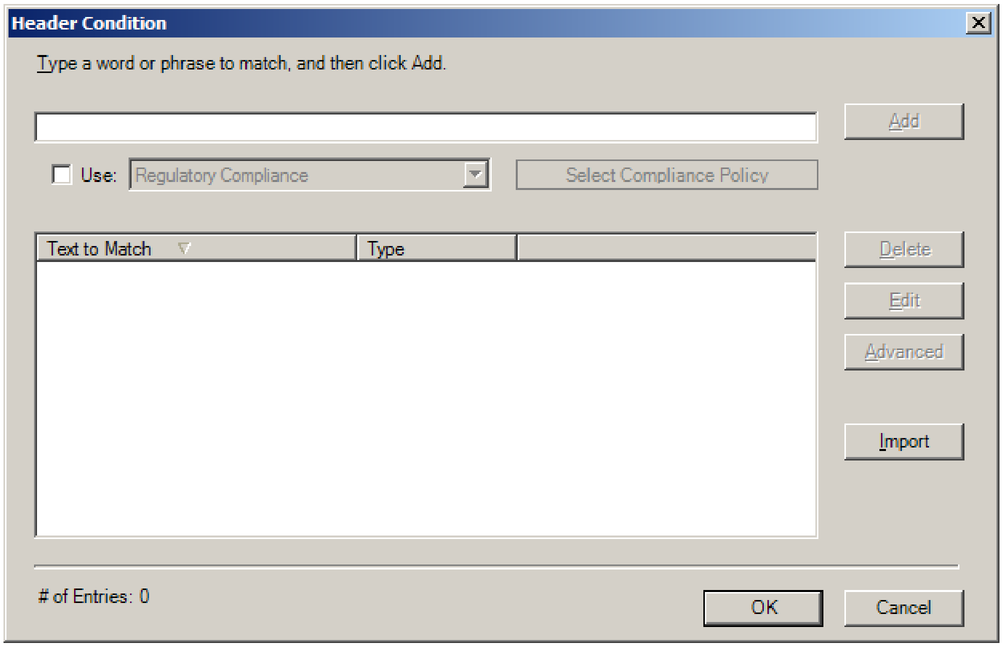
Edit – Edits the currently highlighted IP Address entry in the list by displaying the dialog window described in Figure 12.

Advanced – Allows selection of IP Addresses based on the following conditions:

- Contains any of the following
- Contains all of the following
- Does not contain any of the following
- Does not contain all of the following

TEXT ENTRY EDITOR

Figure 40 – Text Entry Editor



Header Condition

Type a word or phrase to match, and then click Add.

☐ Use: Regulatory Compliance

# of Entries: 0

When an option allows text entries to be defined, the Text Entry Editor will be used. This editor allows one or more text entries to be added to the list of entries to be matched. Each entry can include an exact text match, a wildcard match using simple wildcard patterns, a more powerful pattern matching algorithm based on Regular Expressions, or a reference to an external sorted text file containing entries to match.

The following actions are provided by the IP Address Editor.

Add – Allows a new text entry to be added to the list of entries.

Delete – Deletes the entry currently selected in the list.

Edit – Edits the entry currently selected in the list.

Advanced – Selects the type of match that must occur for the condition to evaluate as True or False.

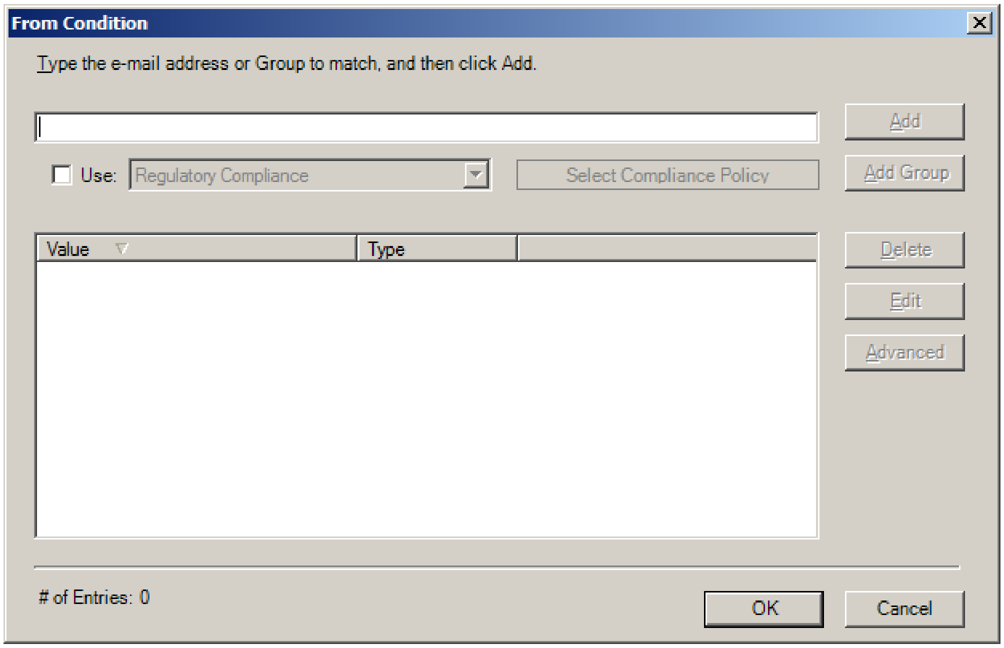
Available options include:

- Contains any of the following
- Contains all of the following
- Does not contain any of the following
- Does not contain all of the following

Import – Displays the Import File Window, allowing either a text file of entries to be imported into the list, or a dynamic reference to an external text file that will be reread by the SMTP Engine dynamically when it has changed.

EMAIL ADDRESS ENTRY EDITOR

Figure 41 – Email Address Entry Editor



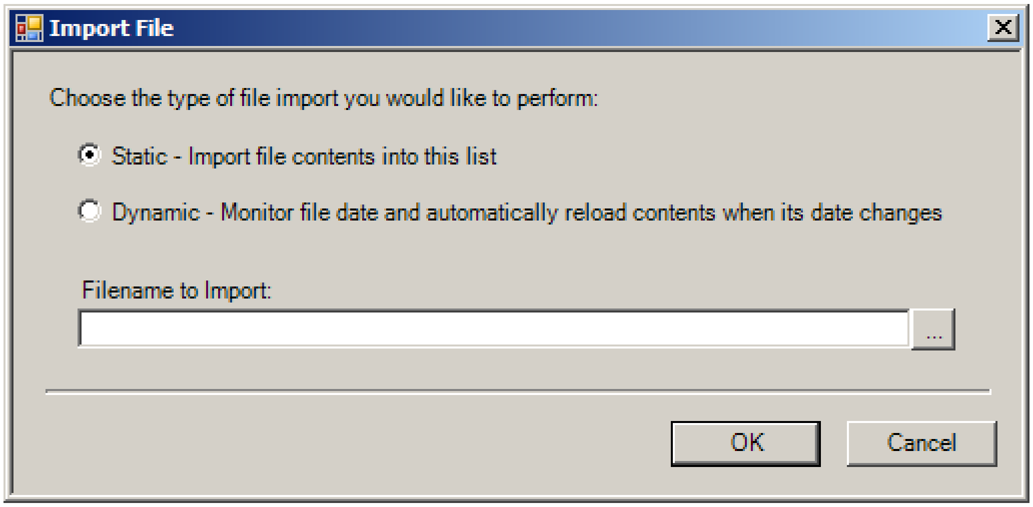
Similar to the Text Entry Editor described previously, the Email Address Entry Editor allows one or more email addresses, simple patterns, advanced Regular Expression matches, or dynamically updated external files with sorted email addresses to be added to a list. This list will be evaluated based on the condition defined under the Advanced button.

In addition to the buttons described in the Text Entry Editor, the Email Address Entry Editor also contains an Add Group button, allowing a group of users to be added to the list. This group is defined in the SecureMail Gateway – User Groups chapter.

IMPORT FILE WINDOW

Many email servers and directory systems allow email addresses to be exported to a file. As long as these addresses are written one address per line in a text file, SMGW is able to utilize them in its scanning process. By clicking the Import button, the following screen is displayed:

Figure 42 – File Import Window



Choose the type of file import you would like to perform:

● Static - Import file contents into this list

○ Dynamic - Monitor file date and automatically reload contents when its date changes

Filename to Import:

SMGW uses external text files in one of two ways:

Static – imports the text file contents into your current list of entries without having to manually enter the contents

Dynamic – uses the text file entries for matching along with any other list entries, and also dynamically rereads the file contents when its file date has changed. This is especially useful for integrating with a batch process that updates the file on a periodic basis. As an example, with Dynamic linking, a utility program can be run against a directory on your mainframe, LDAP or Active Directory, and periodically, write the latest list of user email addresses in a department to file department.txt. Upon update, SMGW will automatically use the latest list of department users for its content scanning.

External Import File Format

The SMGW can import and utilize the contents of an external text file as long as it follows the following criteria:

1. It is saved in ASCII text file format.
2. It is comprised of one word or phrase per line.

Each line is delimited with a Carriage Return and Line Feed (chr(13) + chr(10))

* * *

This represents the end of the *DataMotion SecureMail Gateway Administration Guide*.