

UserGate Mail Server 1.x

Administrator Manual

Table of Contents

Introduction	3
System Requirements	3
Installation	3
Update and Uninstallation	3
Quick Setup	4
Server Settings	4
Connection Setup	4
Assign connection password	5
Server Setup	5
Services	7
Delivery Routes	9
Domains	11
LDAP synchronization	13
Web Mail Properties	13
Setting backup UserGate Mail Server	14
Recovery UserGate Mail Server from backup	15
SMTP Server	15
Domain Settings	17
Remote Accounts	20
Distribution Lists	21
Message Rules	22
Antispam Modules	25
Antivirus Modules	26
Message Queue	27
Message History	27
Server Log	28

Introduction

UserGate Mail Server is a full function mail server with POP3, IMAP4, SMTP, HTTP, HTTPS, and SSL support. UserGate Mail Server major features include domains local and remote accounts support, distribution lists support, LDAP and Webmail directory services synchronization, integrated antivirus and anti-spam modules as well as a powerful and flexible rules system.

Mail security in UserGate Mail Server is provided by two integrated antivirus modules from Kaspersky Lab and Panda Security. Both antivirus modules are intended for mail traffic scanning and can be used separately or jointly for successive message scanning.

For antispam protection, in addition to the standard filtering features (a white list and a black list), UserGate Mail Server uses two full function modules from Commtouch and SpamAssassin. The Commtouch module is built with a unique filter, based on a proprietary RPD (Recurrent-Pattern Detection) algorithm that identifies spam by its primary feature - frequency of occurrence. Unlike other antispam filter vendors, Commtouch does not provide filter updates based on a typical content definitions database: its product scans mail traffic for spam patterns.

The SpamAssassin antispam module is an extendable mail filter used for spam identification. The module filters messages by successively passing them through a series of tests. Each test has a certain "value." If a message passes a test, the value is added to the total score. The value may be both positive and negative; all positive values are called "spam." The message passes all tests, after which the module calculates the total score. Higher scores mean higher possibility that the message is spam.

System Requirements

We recommend installation of UserGate Mail Server on computers with Windows 2000, XP, 2003/2008 Server, Vista operating systems with minimum 360 mb RAM. If you are planning to use your mail server with external networks, the computer with a UserGate Mail Server must have an Internet connection.

Installation

To install UserGate Mail Server, run setup file and select the required options in the installation wizard. The installation will include all the selected components and an additional MS Visual C++ Redistributable package. All system services will be installed automatically, and the mail server will be launched after installation. The mail server default installation directory is "%Program files%\Entensys\UserGate Mail Server" (hereinafter, %UserGate Mail%).

If the mail server does not respond to primary services (SMTP, POP3 or IMAP) connection requests, check the administrator console port settings. By default, the mail server uses TCP port 2222 to communicate with the administrator console. .

Update and Uninstallation

We recommend you uninstall the previous version of UserGate Mail Server before installing the new one. If necessary, you can save server settings file "%UserGate

Mail%\settings.xml" and statistics database. The backup copies of the statistics database are located in the "%UserGate Mail%\Backup" folder.

To uninstall UserGate, go to Start - Applications and select Uninstall in the application program directory. You may also uninstall the application from Add/Remove Programs menu in Control Panel. UserGate Mail Server will be removed, but server settings file (settings.xml), copies of the statistics database (Backup folder) and some other files will not be deleted from the program folder.

Quick Setup

1. Open the administrator console and connect to the server.
2. Go to Server Settings - domains, right-click on an empty area and select "Add domain."
3. Specify domain settings, full domain name (e.g. esafeline.net), domain alias and signature (e.g. your company signature) if required and save changes.
4. Add several user accounts. Go to domain Settings - local accounts. Specify names that will be used in mail addresses before the @ symbol and their passwords.
5. The quick setup is completed. Default spam protection includes a DNSBL spam blacklist (sorbs.net, spamhouse.org). Antivirus modules and spam analysis modules (Commtouch module and free SpamAssassin module) are also running. So most spam messages will be stopped before they reach the destination mailboxes.
6. For remote access to your mailbox via web-interface, type the IP address of the computer with Mail Server and extension for port 5555 in your browser window: for example, <http://192.168.0.1:5555>.
7. Setting up your mail client is a simple task. To set up POP3 and SMTP servers, specify the IP address of the computer with UserGate Mail Server (e.g. 192.168.0.1 like in the example above), account name and password. If your account name is testuser and the domain name is esafeline.net, the user name may be specified with the @ symbol and the domain name (testuser@esafeline.net) or without them (testuser).

Server Settings

Connection Setup

When you start the administrator console for the first time, it will open on Connections page. This page contains the single connection with the UserGate Mail Server, working through interface 127.0.0.1 for the *Administrator*. To establish connection between the administrator console and the server, double-click the connection line or click "Connect" in the control panel. You can create more than one connection on the Connections page if the administrator console is to work with multiple mail servers. Specify the following parameters in the connection properties:

- Server name - connection name.
- User name - account name for server connection.
- Server address - domain name or UserGate server IP address.
- Port - TCP port used for server connection (port 2222 by default).

- Password - connection password.

Assign connection password

To assign UserGate Mail Server connection password, go to the "Server Settings - Remote Admin" page in "Advanced Security Settings" menu. You can also assign TCP port for server connection in this menu. New settings will be enabled immediately after application; you do not need to restart the server.

Server Setup

Basic settings

In Basic Settings, specify the required parameters for UserGate Mail Server database access. Default settings presuppose that the database server is located on the same computer where UserGate Mail Server is installed, so the database address will be specified as localhost. The mail server works with the database through the ugmiluser account.

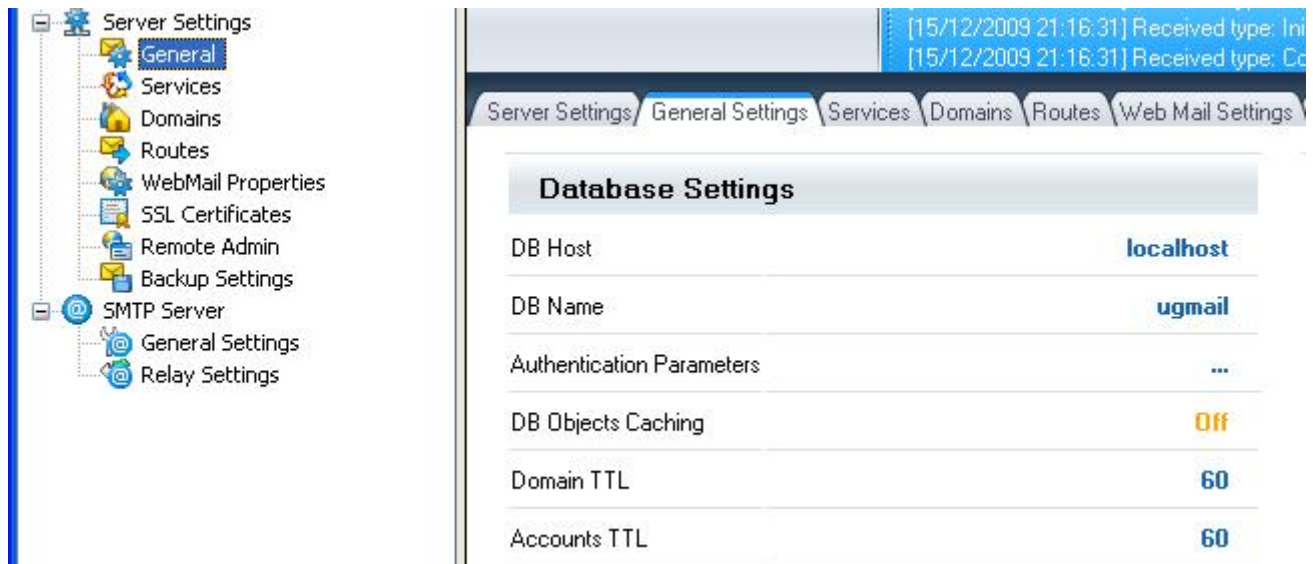


Fig. 1. Basic Settings

You can make a heavy loaded server working with several domains work faster by enabling database object caching. The mail server will then cache all mail domain and account data, which helps to minimize database requests. In cache settings, specify the cache record time-to-live (TTL). The default TTL is 60 seconds.

Mail messages are processed in several threads. The administrator may specify the required number of threads processing the mail delivery (Max. Delivery Threads) and the maximum number of threads (Max. TCP threads), as well as assign a priority to different threads (Thread Priority).

Threading	
Max TCP Threads	15
Max Delivery Threads	3
Thread Priority	Normal <input type="button" value="v"/>

Fig. 2. Setting Up Threads and Priorities

Caution: We do not recommend increasing the total number of threads to the maximum value or set the highest priority to them unless necessary, as this may increase the memory usage by UGMail.exe process and the processing time.

Setting message store location

The folder (Message Store) where the mail server will store all incoming messages is specified in General Settings. By default, all incoming mail will be placed in folder %UserGate Mail Server%\Mail. The folder %UserGate Mail Server%\Tmp is used to store temporary files during a virus scan of incoming messages.

Directories	
Messages Storage	C:\Program Files\Entensys\UserGate Mail Se
Temporary Directory	C:\Program Files\Entensys\UserGate Mail Se

Fig. 3. Mail Store Settings

Server settings

If your mail server works with more than one domain, the administrator can specify a Default domain. In this event, if the user specifies only a part of email address (without the domain name) during the authorization, the mail server will automatically add Default domain.

Shadow email

With UserGate Mail Server you can copy all incoming mail to the specified email address (Shadow Mail). Any existing email address can be used for Shadow Mail. Incoming mail will be copied regardless of any further processing of mail by antispam or antivirus modules and regardless of user mail processing rules.

Creating server messages templates

An administrator can create templates for mail server service messages in Server Messages Setup. There are preset scripts for certain types of messages that help make message text more detailed. For example, %_ATTACHMENT_% macro denotes the name of the attachment. When creating a service message, the mail server will replace the macro with the name of attachment.



Fig. 4 and 5. Creating Server Messages Templates. Server Settings.

Services

Mail protocols are processed by a number of services. The services are listed on the Services page of the UserGate Mail Server administrator console. You can specify the list of interfaces and ports for each service, set the maximum of simultaneous connections and limit the range of IP addresses to which connection will be allowed. By default, mail servers process all the available server network interfaces. Also, in default settings, connection to mail services is allowed from any IP address (from 0.0.0.0 to 255.255.255.255).

The administrator can also create the so-called Welcome Message for each service in addition to network settings.

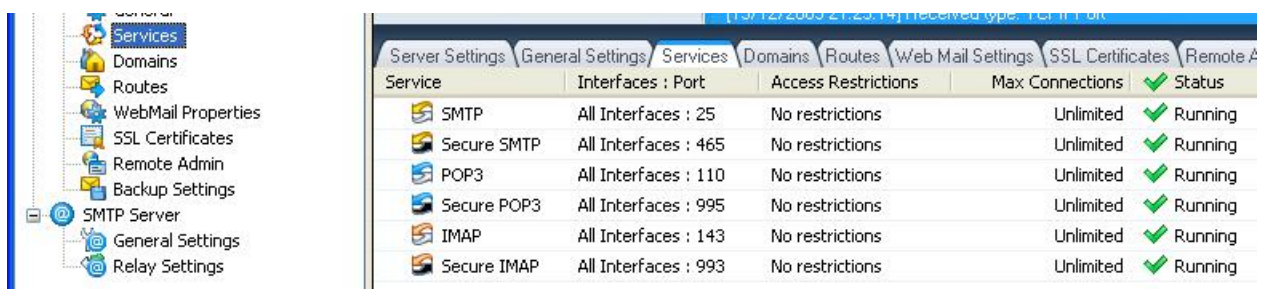



Fig. 1. Services

IMAP: General [Close]

Shutdown IMAP service [1] [2] [3]

Setup interfaces 

Interface	Port
<input checked="" type="checkbox"/> All interfaces	143
<input type="checkbox"/> 93.92.216.34	143
<input type="checkbox"/> 192.168.0.1	143

Hint
Services Hint

[OK] [Previous] [Next] [Cancel]

IMAP: Restrictions [Close]

Shutdown IMAP service [1] [2] [3]

Specify addresses     

IP Addresses	Action	Comment
0.0.0.0 - 255.255.255.255	Allow	

[OK] [Previous] [Next] [Cancel]

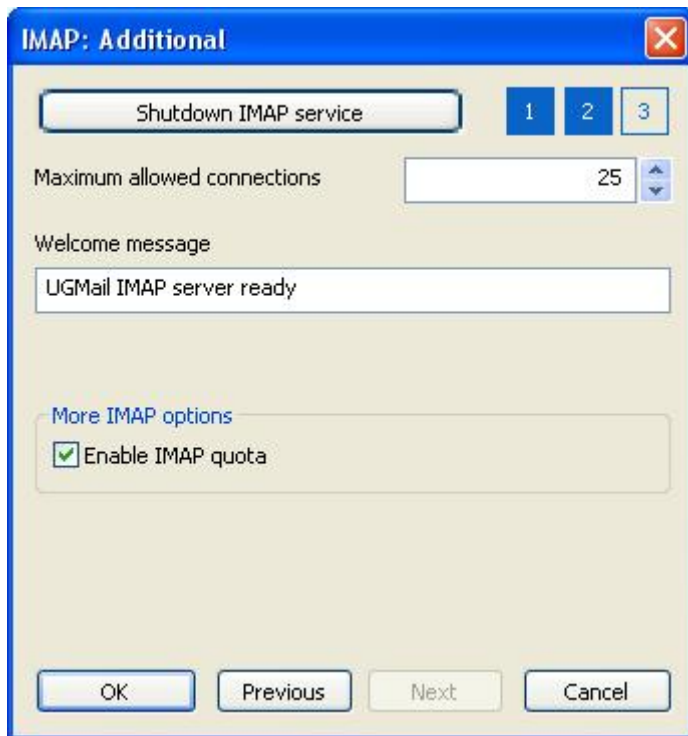


Fig. 2,3,4. IMAP Service Settings

Delivery Routes

You can specify incoming mail delivery routes for each domain on the administrator console's Routes page. The following parameters should be specified in the route settings:

- Mail domain name
- Remote SMTP server address and port
- Maximum delivery attempts
- Repeated delivery timeout (the interval of time after which the server will attempt a repeated delivery if the previous delivery fails)
- Authorization parameters for a remote SMTP server.

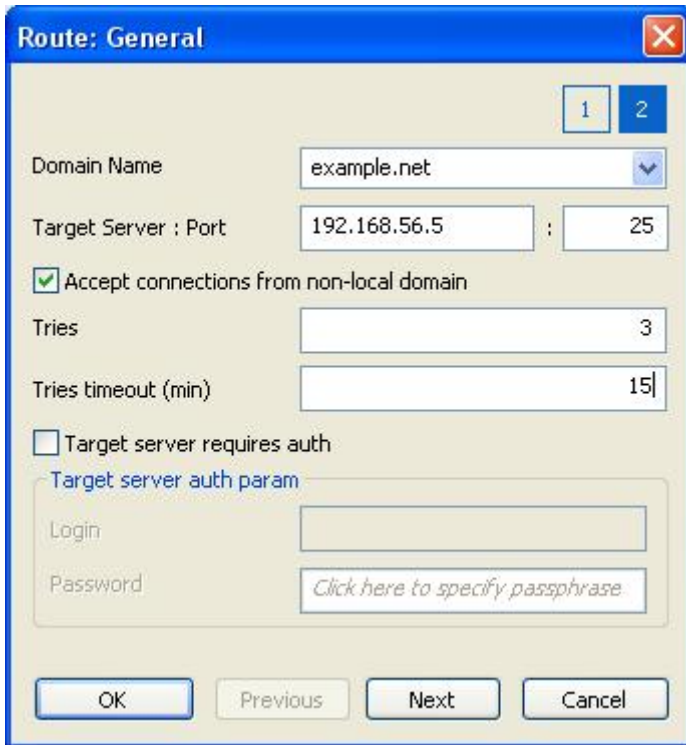


Fig. 1. Server Routes

You can also specify the accounts in the route parameters to which the route will apply. A set route will apply to all domain accounts by default.

If the "Address as local" option is enabled, the domain specified in the route will be considered local and the administrator does not have to set the applicable permissions in Relay Settings.

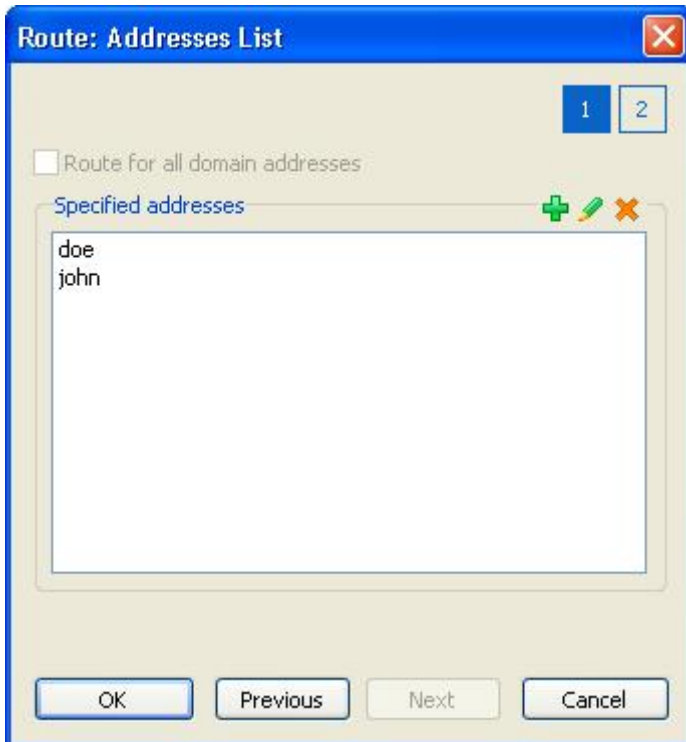
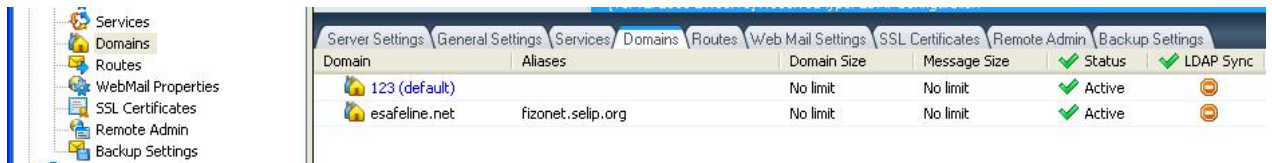


Fig. 2. Route parameters

Domains

The domain name is the key setting for the mail server. An administrator can specify the domains to be processed by the mail server in the administrator console's domain page. The following information should be specified for each domain:

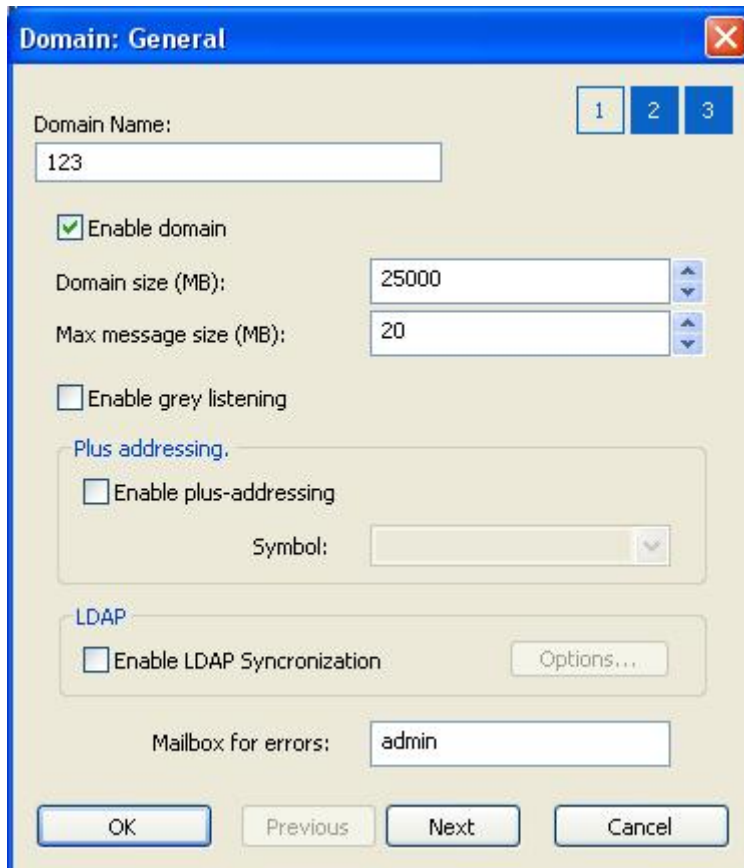
- domain name (in FQDN, Fully Qualified domain Name format)
- Maximum domain size
- Grey Listing mode (one of spam protection methods)
- Plus Addressing mode
- Email address for error messages.



Domain	Aliases	Domain Size	Message Size	Status	LDAP Sync
123 (default)		No limit	No limit	Active	Active
esafeline.net	fizonet.selp.org	No limit	No limit	Active	Active

Fig. 1. domains

The domain size is calculated as the total size of accounts in the domain. If the total size of accounts in the domain exceeds the maximum domain size, the main server will stop processing incoming mail for that domain.



Domain: General

Domain Name: 123

Enable domain

Domain size (MB): 25000

Max message size (MB): 20

Enable grey listening

Plus addressing:

Enable plus-addressing

Symbol: [Dropdown]

LDAP

Enable LDAP Synchronization [Options...]

Mailbox for errors: admin

OK Previous Next Cancel

Fig. 2. domain Settings

In the domain settings, the administrator can also specify domain Signature and signature attachment rules and set one or more alternative domain names (alias).

Domain: Signature ✕

Domain Name: 1 2 3
123

Enable domain signature

Edit signature
123 signature

Signature usage: Set if not specified in account. ▾

Add when reply
 Add when local message

OK Previous Next Cancel

Domain: Aliases ✕

Domain Name: 1 2 3
123

Domain aliases + ✎ ✕

Alias
321
231
132
111

OK Previous Next Cancel

Fig. 3 and 4. domain Signature. Aliases

The LDAP Sync option in mail domain settings can be used to synchronize accounts with an LDAP directory, such as the MS Active Directory.

LDAP synchronization

In addition to the local database of mail domain accounts, UserGate Mail Server supports LDAP directories accounts import. This allows centralized accounts management, reduces possible errors and simplifies the administration process. The procedure of LDAP synchronization is described below:

- Enable LDAP Sync in Mail domain Settings - Server Settings
- Specify LDAP name (e.g. Active Directory domain name)
- Specify login and password for the user to connect to the LDAP directory.

You can make additional settings on the Advanced page, such as the name of subdirectory from which the mail server will start browsing through the LDAP directory structure. When synchronizing, the mail server will browse all inferior subdirectories of the LDAP directory.

When addressing the LDAP directory, the mail server will select all accounts that have email addresses in their properties. Directory will be accessed via LDAP protocol. Safe protocol is not currently supported. The timeout for a new request (2 minutes) cannot be changed.

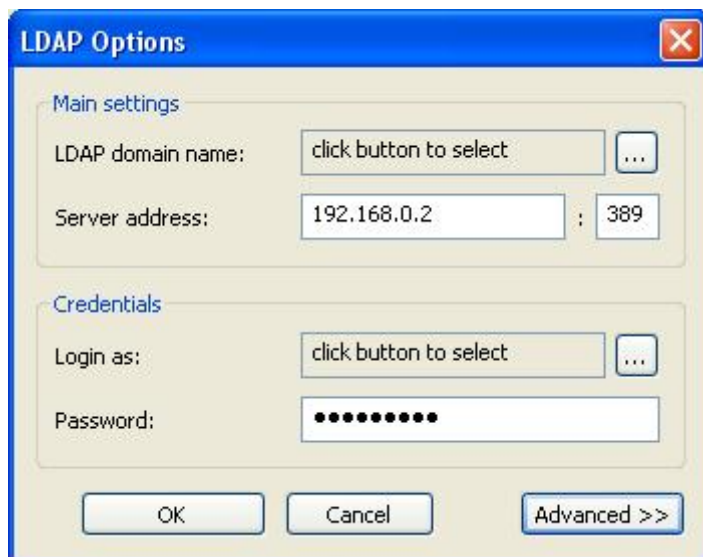


Fig. 5. LDAP Synchronization Parameters

Web Mail Properties

On this page, the administrator can set UserGate Webmail properties, including "Company Name," welcome message text, system locale and company logo. IMAP sorting can also be enabled on this page. UserGate Webmail uses port 5555 and can be accessed at <http://ugmail:5555/webmail> by default, where ugmail is the address of the server on which the UserGate Mail Server is installed.

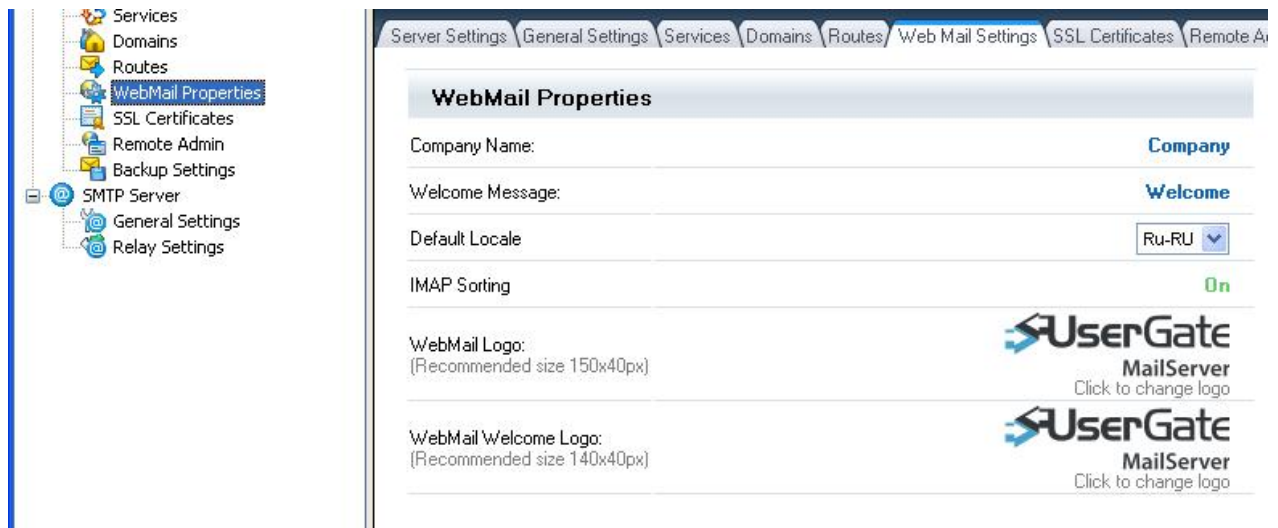


Fig. 1. Web Mail Settings

Setting backup UserGate Mail Server

In UserGate Mail Server backup the following parameters should be specified:

- Directory for containing backup files. The default directory is %UGMail%\Backup.
- Maximum number of backup files that you want to save. Earlier copies of backup files will be deleted automatically.
- Interval for performing a full backup.
- Interval for performing a differential backup. It is recommended to choose the value of this interval smaller than the corresponding parameter for full backup.
- Backup start time.

Optionally, UserGate Mail Server administrator can back up the current state of UserGate Mail Server through "Manual Backup" item. Let us suppose that we have specified: backup start time (T_{start}), full backup creation interval (P_{full}) and differential backup creation interval (P_{diff}). Then the time for creation of subsequent full and differential backup files could be defined as follows:

$$T_{full}(i) = T_{start} + (i - 1) * P_{full}, \text{ where } i = 1, \dots, N.$$

$$T_{diff}(j) = T_{full}(i) + j * P_{diff}, \text{ where } j = 1, \dots, M$$

During backing up UserGate Mail Server saves the contents of the mail directory (default %UGMail%\Mail), server's settings file (%UGMail%\settings.xml) and creates a dump of the mail database. UserGate Mail Server database ("ugmail") contains some server's settings and information about processed mail messages.

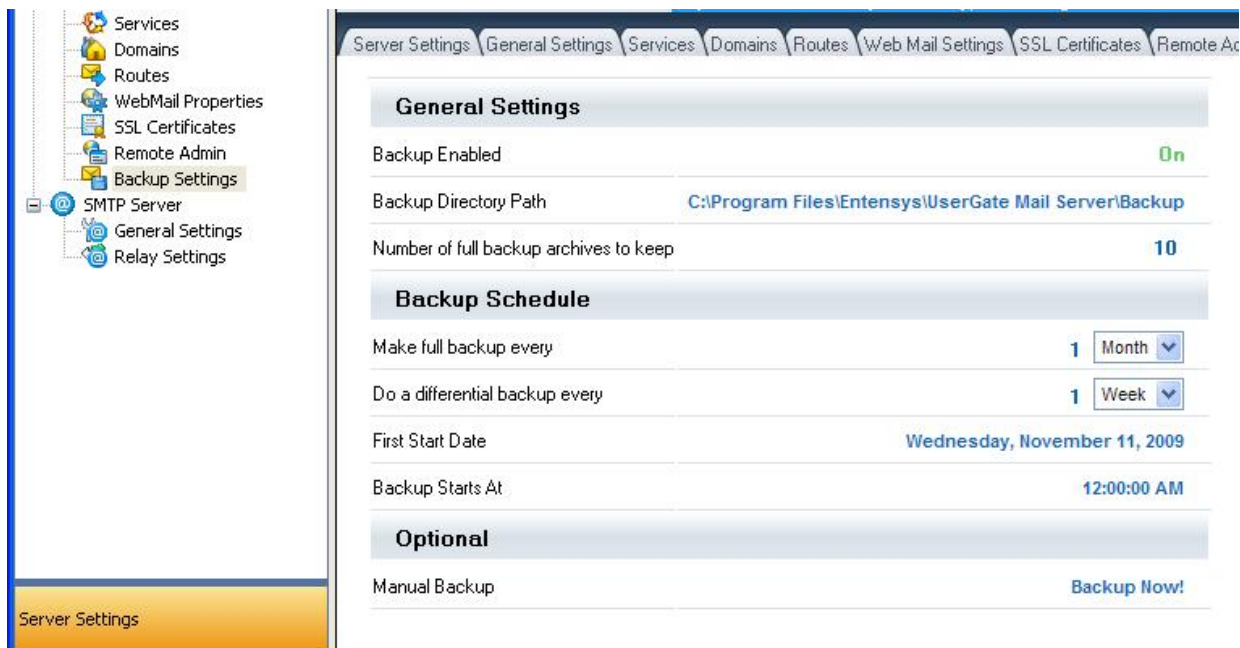


Fig. 1. Backup Settings

Recovery UserGate Mail Server from backup

Recovery from backup is performed in two stages. At the first stage, a set of differential backup files and an initial full backup is used to form a resulting backup. It is performed with BackupPrepare command line tool, located in the %UGMail%\Backup directory. The latest differential backup file (*.zip) name is used as a command line argument. Start of BackupPrepare tool might look like this:

```
BackupPrepare.exe "2010.01.01 09.01.00 diff1.zip"
```

During work BackupPrepare tool pass through the whole chain of intermediate differential backup files, up to the first full backup. If it succeeds a directory containing final full backup will be created. In the example shown above, you will get a directory "2010.01.01 09.01.00". At the second stage the obtained full backup directory name is used as a command line argument passed to RestoreBackup.bat tool. This tool is also located in %UGMail%\Backup directory. Before starting RestoreBackup.bat tool you must stop UserGate Mail Server and close any applications that might have access to mail database. Starting RestoreBackup.bat might look as follows:

```
RestoreBackup.bat "2010.01.01 09.01.00"
```

RestoreBackup tool will remove the current mail directory, the current server's settings file and mail database by replacing them with files taken from the backup directory.

SMTP Server

Basic settings

SMTP server basic settings include mail delivery parameters, delivery schedule, restrictions applied to mail protocols under RFC requirements, and some other parameters.

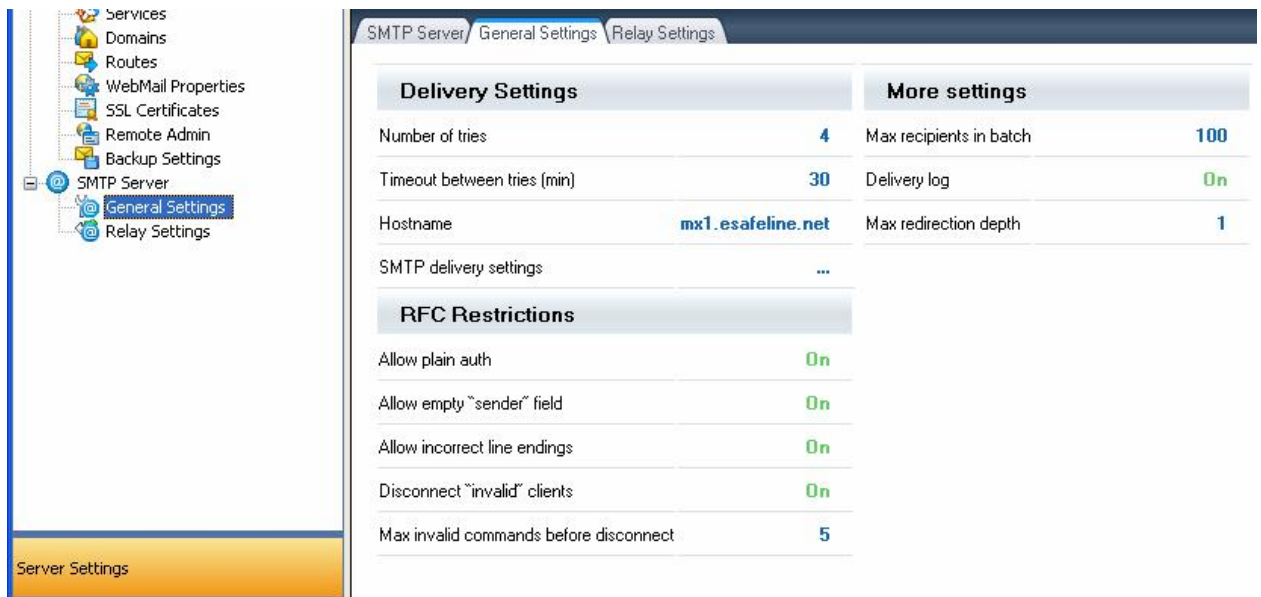


Fig. 1. SMTP Server Settings

Delivery queue parameters are the main parameters of SMTP settings.

These parameters specify how long a message will be queued for processing and how mail will be delivered. Queue parameters include:

- Maximum delivery attempts
- Repeated delivery timeout.

Hostname parameter will be used by the mail server for connection to other mail servers to deliver mail messages.

By default, the SMTP server uses the so-called MX delivery mode when each message is delivered to the server that is responsible for the recipient's domain. Still, an administrator may specify a relay server in SMTP Delivery Settings. Login and password can be set in the Relay Server settings if the server requires authorization.

The SMTP server can be set to block incoming mail addressed to more than one recipient. The maximum number of recipients is set by the parameter Maximum Recipients. In addition, a delivery log is available that allows detailed logging of the sending process.

Mail processing may loop as it is a non-linear process due to user policies and the antivirus and antispam modules. This situation is very unlikely, but settings include the parameter "Maximum relay depth" to prevent looping.

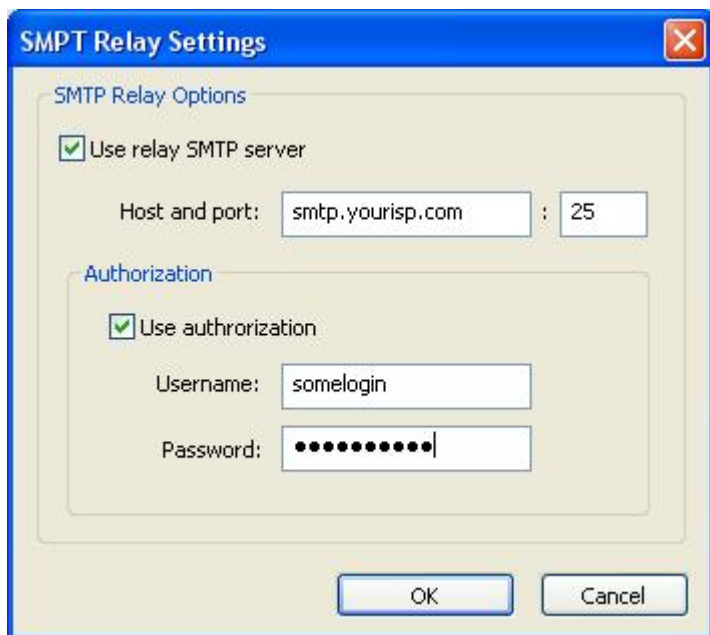


Fig. 2. Relay Settings

Relay parameters

The mail server administrator may allow or deny certain types of mail processing for particular a IP addresses or a range of addresses. The relay settings should specify:

- First and last IP address in the range
- Relay options
- Comments.

In relay options, you can allow mail relay within your mail domain (Local - Local), sending mail to remotedomains from your local domain (Local - Remote) and receipt of mail addressed to your domain from remote domains (Remote - Local).

If the Remote - Remote option is enabled, your UserGate Mail Server will be used as a relay server. We strongly recommend you do not enable this option because open relays are invalid configurations for mail servers according to the Internet Society. Never enable this option if the server can be accessed from the Internet.

Caution: Do not enable "Remote - Remote" option for the entire IP range if your server works with remote mail servers. This will make your server an open relay.

Policies in Relay Settings will be processed according to the set priorities.



Fig. 3. Setting Relay Permissions

Domain Settings

Local user accounts

Create user accounts on Local Accounts page for each domain. User account parameters are set as follows:

- Login
- Mail domain name
- Administrator console access level
- Password
- User name
- Personal message size limit
- One or more alternative names (alias)
- Re-direct email address.

User authorization via LDAP

Specify password in account settings to enable authorization at the mail server. There is no need to specify password if the mail server is installed on the computer included in the Active Directory domain and LDAP Sync option is enabled in the mail domain properties. The domain password will be used for authorization.

Account: General ✕


Account login: 1 2 3
test1

Enable Account

Domain: esafeline.net

Passphrase: ●●●●

Account max size (MB): 0

 Person name:

Override message size for this account.

Override domain settings
Account message size (KB): 0

OK Previous Next Cancel

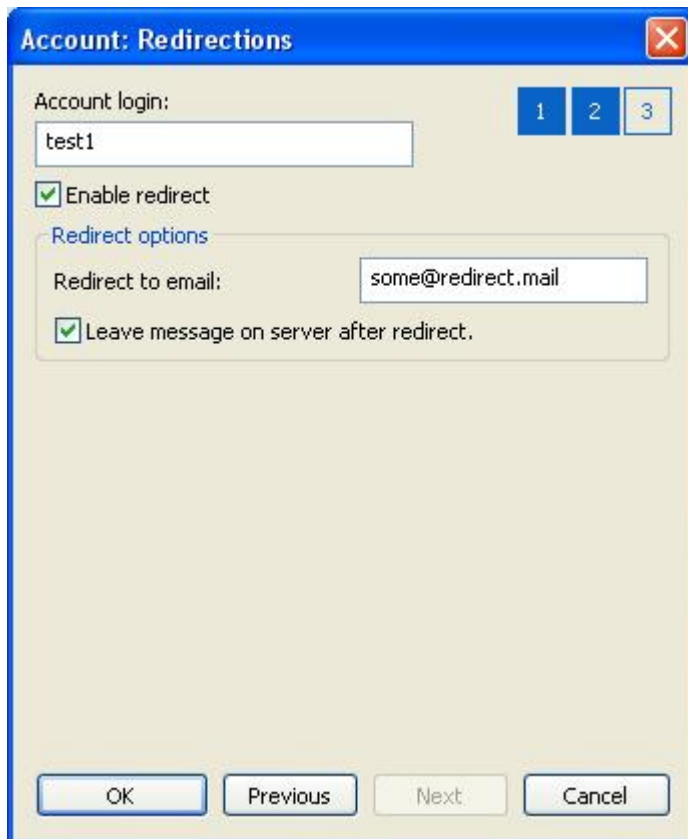
Account: Aliases ✕

Account login: 1 2 3
test1

Account Aliases + ✎ ✕

- doe@esafeline.net
- john1@esafeline.net
- john2@esafeline.net

OK Previous Next Cancel



Figures 1, 2 and 3. User Account Settings

Remote Accounts

You can associate each local account in UserGate Mail Server with a remote account. A remote account is used for occasional requests to a remote mailbox. If there are new messages in the remote mailbox, they will be automatically downloaded to a local account and, depending on the settings, may be deleted from the remote mailbox. If the local account or associated domain is inactive, mail will not be downloaded from remote accounts. Remote account settings should be set as follows:

- Email address
- Remote server address
- Login and password for POP3 authorization
- local accounts that receive mail from the remote account.

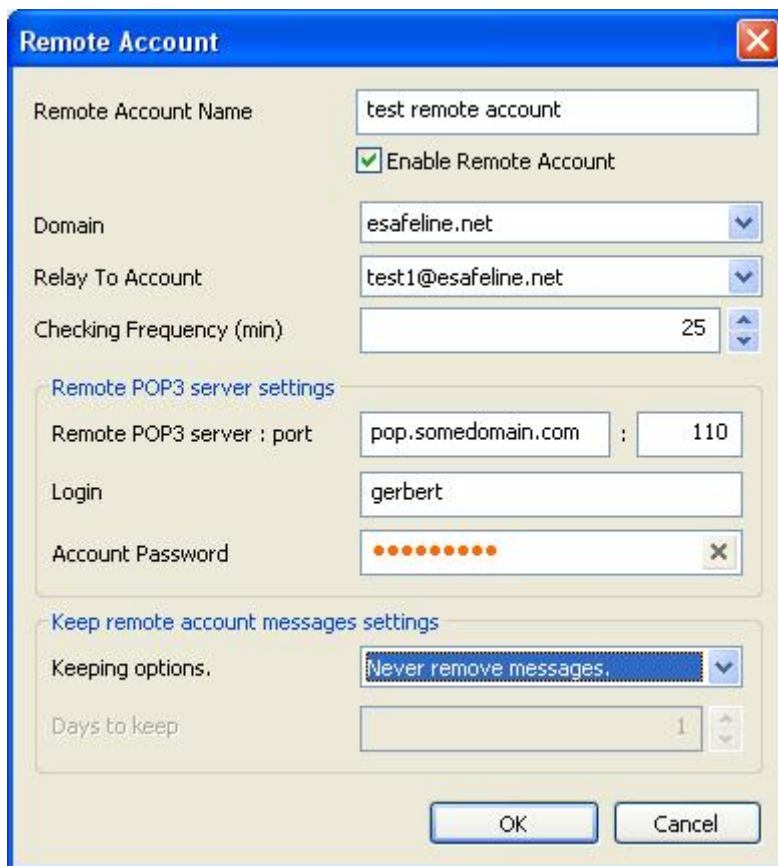


Fig. 1. Setting Remote Accounts

Distribution Lists

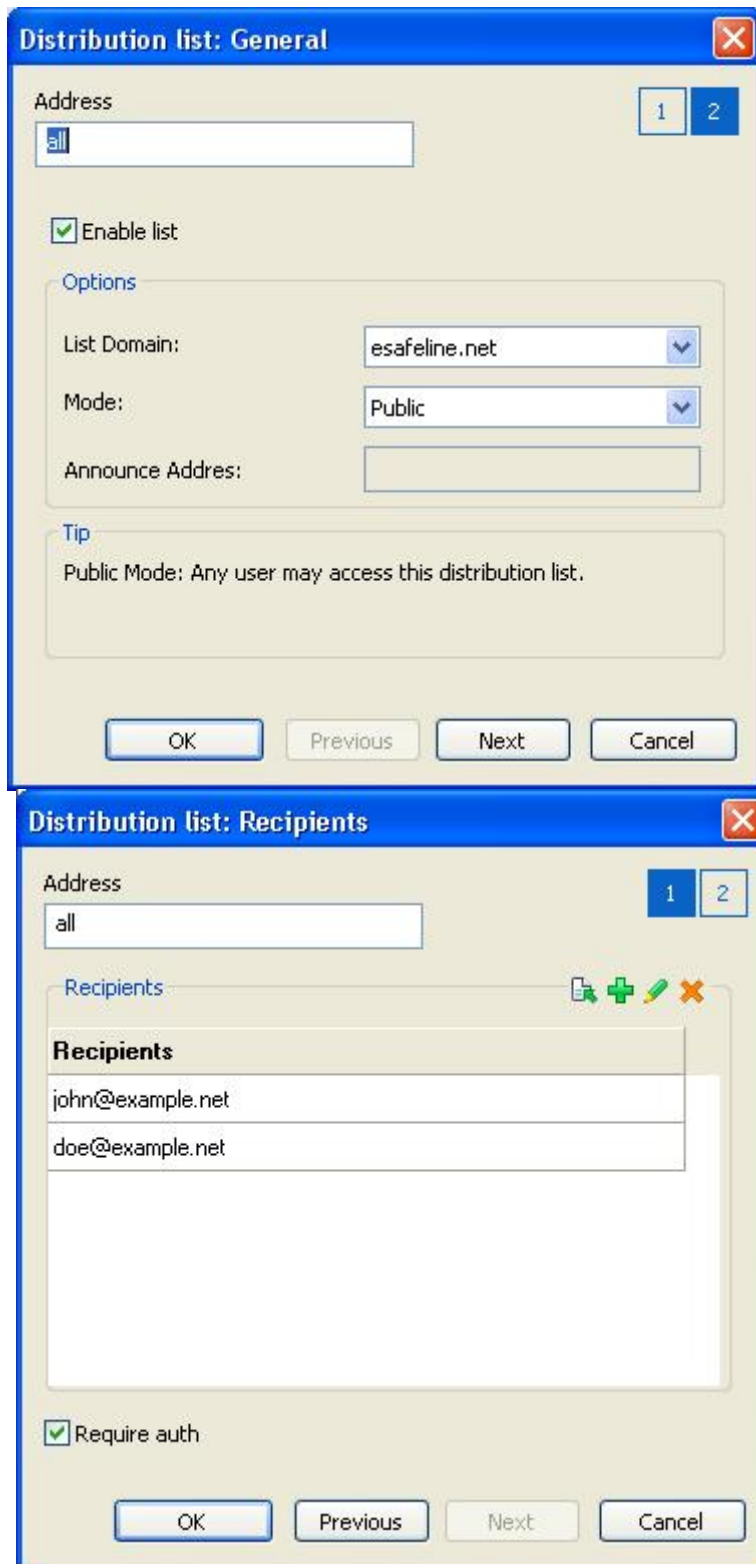
You can send the same message to a group of email addresses included in a particular distribution list. A distribution list is an address from which your message is copied to all addresses on the list. Distribution list settings should be set as follows:

- Distribution address
- Mode to determine the addresses that are allowed to use a given distribution list
- Email addresses for distribution.

UserGate Mail Server supports three distribution modes. General mode is a common distribution mode in which distribution messages can be sent from any address.

In Group mode, only users listed in the distribution properties can send messages to a distribution group. Messages sent from other accounts will be replied by the mail server with the following notification: *"550 Not authorized."*

Information mode is used when a certain account needs to send messages to all addresses on the distribution list. Messages sent from other accounts will be replied by the mail server with the following notification: *"550 Not authorized."*

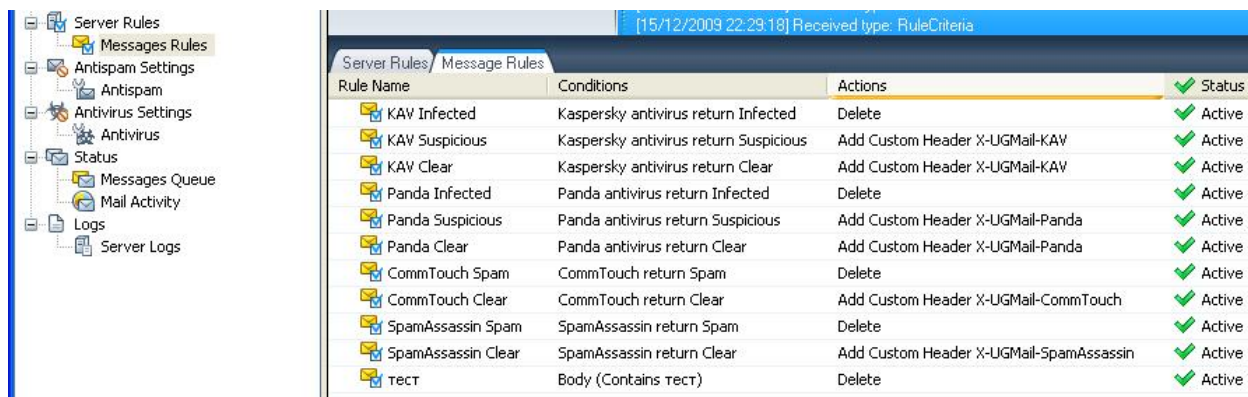


Figures 1 and 2. Distribution lists

Message Rules

All messages in UserGate Mail Server are processed according to message rules. Rules are the combination of conditions with AND/OR operators and one or more actions that should be processed if the condition is true. Rules are implemented in a

top-down sequence, which means that each message can be matched to several rules. For non-linear message processing, you can select the "Stop Processing" option to disregard downstream rules or "Jump to Rule" to jump to a certain downstream rule.



Rule Name	Conditions	Actions	Status
KAV Infected	Kaspersky antivirus return Infected	Delete	Active
KAV Suspicious	Kaspersky antivirus return Suspicious	Add Custom Header X-UGMail-KAV	Active
KAV Clear	Kaspersky antivirus return Clear	Add Custom Header X-UGMail-KAV	Active
Panda Infected	Panda antivirus return Infected	Delete	Active
Panda Suspicious	Panda antivirus return Suspicious	Add Custom Header X-UGMail-Panda	Active
Panda Clear	Panda antivirus return Clear	Add Custom Header X-UGMail-Panda	Active
CommTouch Spam	CommTouch return Spam	Delete	Active
CommTouch Clear	CommTouch return Clear	Add Custom Header X-UGMail-CommTouch	Active
SpamAssassin Spam	SpamAssassin return Spam	Delete	Active
SpamAssassin Clear	SpamAssassin return Clear	Add Custom Header X-UGMail-SpamAssassin	Active
TECT	Body (Contains tect)	Delete	Active

Fig. 1. Message Rules

You can select the following options:

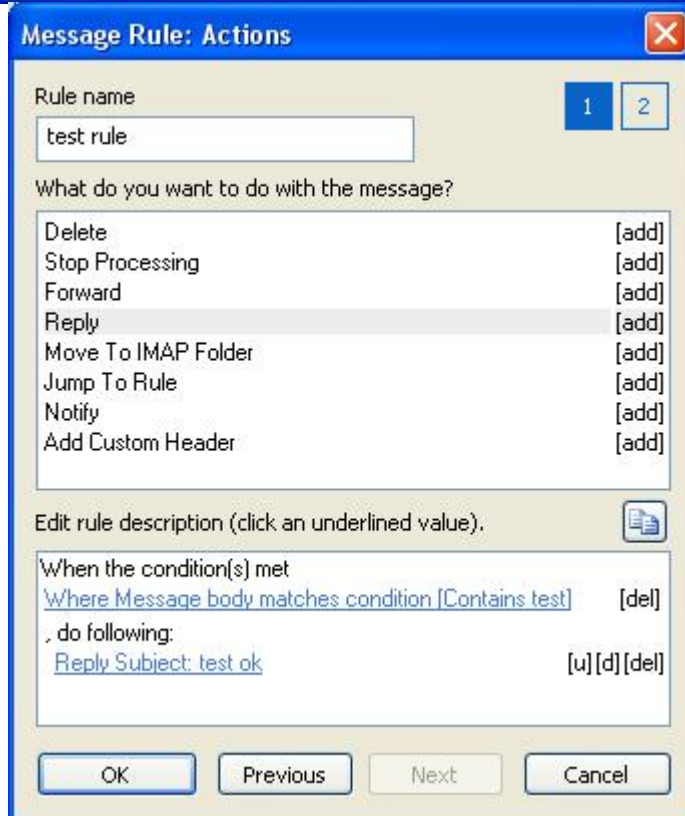
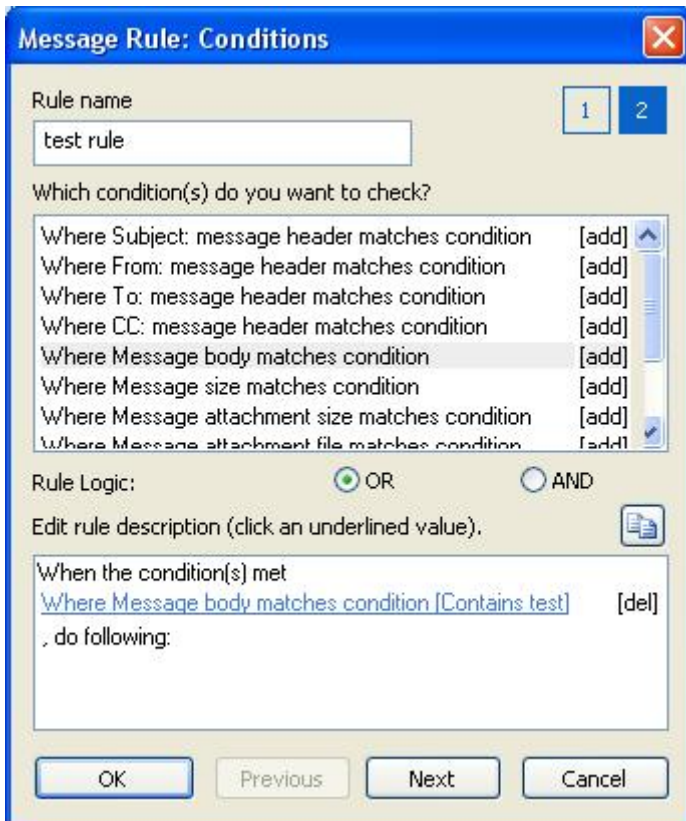
- Subject field [Equals, Contains, RegEx, Not Contains, Not Equals]
- From field [Contains, RegEx, Not Contains]
- To field [Contains, RegEx, Not Contains]
- CC field [Contains, RegEx, Not Contains]
- Message Body [Contains, RegEx, Not Contains]
- Message Size [Less than, Greater than]
- Message attachment [Equals, Contains, RegEx, Not Contains, Not Equals]
- SURBL check [Clear, Spam]
- SpamAssassin check [Clear, Spam]
- CommTouch check [Clear, Spam]
- Kaspersky check [Clear, Suspicious, Infected]
- Panda check [Clear, Suspicious, Infected]

The following actions can be selected:

- Delete
- Stop processing
- Forward
- Reply
- Move to IMAP folder
- Jump to rule
- Notify
- Add Custom header

- Remove attachment

Mail filtering by Custom Header is not supported. This function is performed primarily by a mail client. You can apply rules to all or selected domain accounts.



Figures 2 and 3. Rules

Antispam Modules

UserGate Mail Server supports several spam protection technologies that include DNSBL (DNS blacklist), SURBL (Spam URI blacklist), Greylisting and Tarpitting.

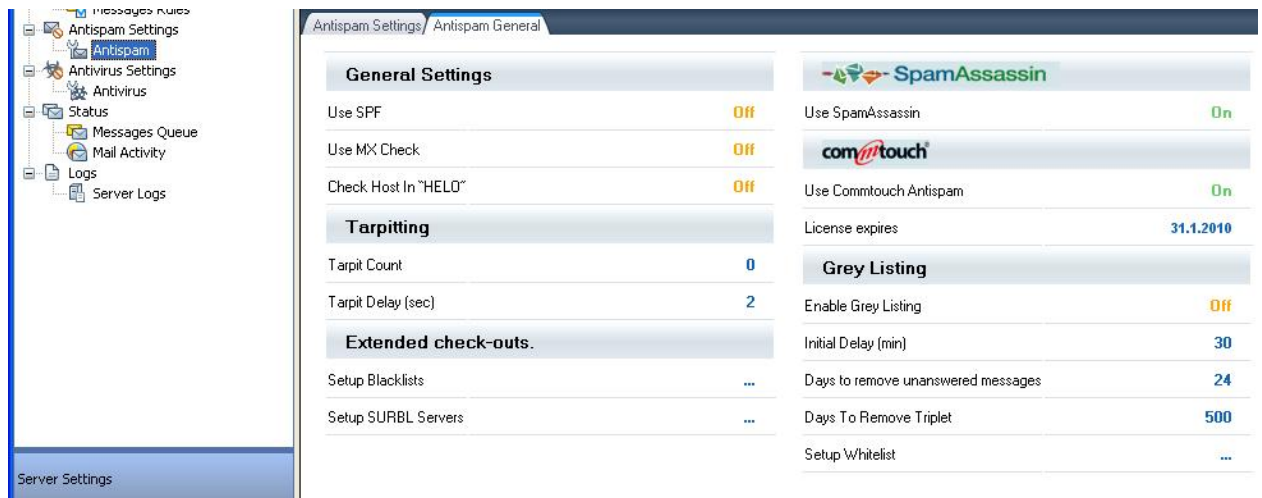


Fig. 1. Antispam

Greylisting

Greylisting is a tool to delay mail delivery. An incoming message is not delivered immediately, and the sender receives a message requesting to retry sending the message later. The data triplet (information about the sender, recipient and destination) remains unchanged. If the triplet of the incoming message matches one of the triplets in the list, the message is delivered immediately (this means the sender is trying to send the message again). This helps filter spammers, because they usually do not retry sending messages to the same addresses.

Blacklists (DNSBL)

Dynamic blacklist is a network service offered by blacklist providers. The providers track IP addresses (sometimes domain names) compromised by spammers. Mail filters with a dynamic blacklist support submit a request to a blacklist provider that contains the sender address and addresses of mail servers the message passed in route to the recipient. If the request shows that the address is on the black list, it means the message most likely contains spam. Along with maintaining spammer lists, some blacklist providers track outgoing addresses of viruses, trojans, worms, applications allowing unauthorized remote control and other malicious content. Dynamic blacklist services are requested via a DNS service to check if the spammer lists contain the IP addresses listed in the message heading (in the Sender field or mail relay server addresses in the Received fields: character domain names can be used along with IP addresses).

Tarpitting

This is a method of delaying delivery of mail from a remote server suspected of spam distribution. A server may become suspicious due to a large number of recipients of the same letter. If this number exceeds a set limit, tarpitting will apply to all further messages from that server.

SURBL filtering

SURBL filtering is used to detect spam by URL contained in the message text (verification against blacklists). The module extracts the domain component (level 2 or 3) for each URL found in the message, adds a SURBL name suffix and sends a DNS request to the SURBL server(s) address. For example:

URL (<http://some.test.ru/index.html>) -> test.ru + (insecure-bl.rambler.ru) -> resolutetest.ru.insecure-bl.rambler.ru -> 127.0.0.1 -> add symbol

A separate list (2tld file) is used for domains in which three levels instead of two should be checked. This may be applicable to virtual hosting services or special areas for Level 3 domains, such as org.ru orpp.ru.

SpamAssassin module

SpamAssassin is an expandable spam mail filter. The module filters incoming mail by consecutively passing them through a series of tests. Each test has a certain "value." If a message passes a test successfully, the value is added to the total score. The value may be both positive and negative; all positive values are called "spam" and negative values - "ham." The message passes all tests, after which the module calculates the total score. Higher scores mean higher possibility that the message contains spam.

SpamAssassin has an adjustable limit. If the message exceeds the limit, it is classified as spam. As a rule, the limit should be set to let a spam message match more than one criteria. Matching just one test is not enough to exceed the limit.

Commtouch module

Commtouch Anti-Spam Gateway is a patented spam protection solution for mail servers and SMTP gates. Commtouch module is uses a unique filter based on proprietary RPD (Recurrent-Pattern Detection) algorithm that helps identify spam by its main feature - frequency of occurrence. Unlike other antispam filter vendors, Commtouch does not provide filter updates based on a typical content definitions database: its product scans mail traffic for spam patterns.

When the Anti-Spam Enterprise gate receives an e-mail, it looks for the relevant rule in the local policies that applies either to the company in general or to the particular users. If the message does not match any of the rules, Commtouch module starts looking through local cache with previous responses by the Anti-Spam Detection Center. If it still cannot find a rule for the message, the gate module sends a request to the Anti-Spam Detection Center located at Commtouch. If the Center is unavailable, the message is delivered to the user's inbox.

If a message is classified as spam, the gate module acts according to its configuration settings. A legitimate message is delivered to the user mailbox.

Antivirus Modules

UserGate Mail Server has two integrated antivirus modules from Kaspersky Lab and Panda Security. Both modules scan SMTP traffic. The antivirus modules can be configured on Antivirus page of administration console. An administrator may specify the maximum size of messages scanned by antivirus modules and action on virus detection, as well as enable notification of message sender and recipient.

Before you start the antivirus modules, proceed with update of virus definitions. With default settings, virus definition updates are downloaded from Kaspersky Lab website for Kaspersky Antivirus and from special entensys site for Panda Antivirus.

UserGate Mail Server can simultaneously work with two antivirus modules. The sequence of scanning is defined by the Message Rules set by the UserGate Mail Server Administrator.

Message Queue

The Message Queue page indicates the queue of messages on the mail server. The mail server administrator can remove messages from the queue, stop the queue or resume message queue. By default, message queue lists the 20 last messages processed by the mail server.



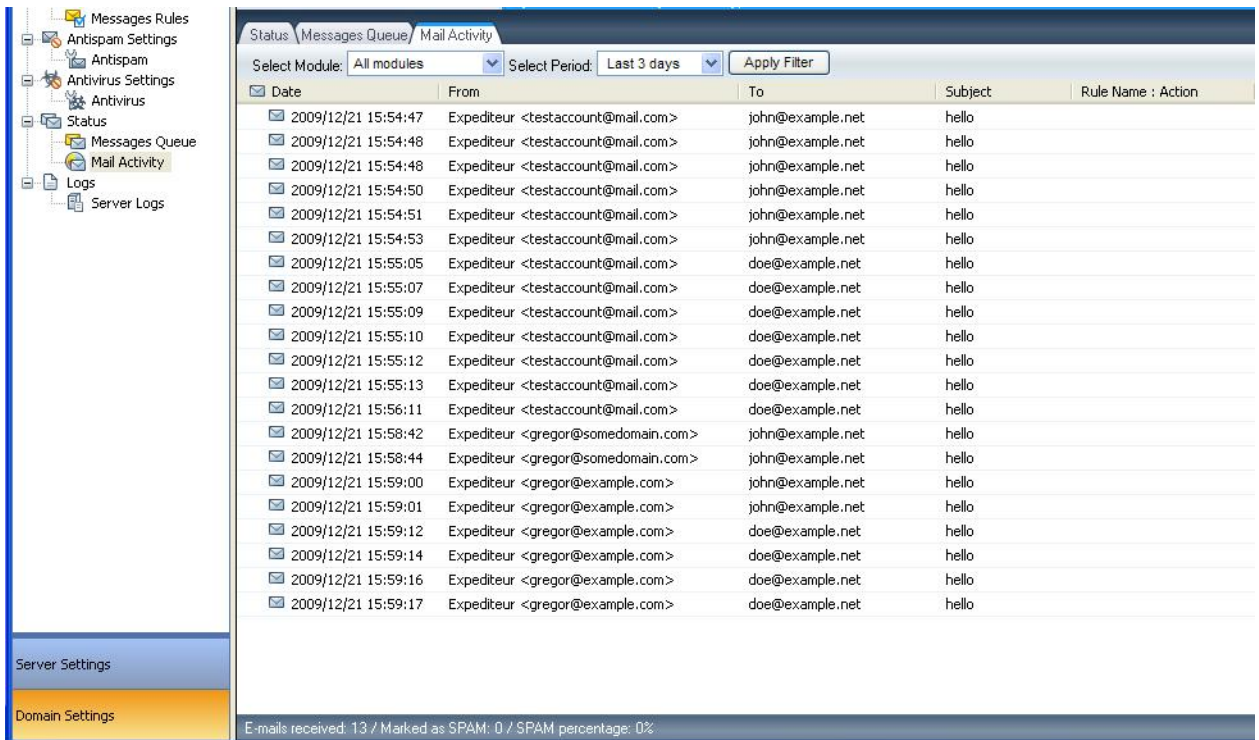
Fig. 1. Message Queue

Message History

Message history summarizes the work of the mail server. The Message History page contains all the valuable information about the messages processed by the mail server. This page also contains some information about the integrated antivirus and antispam modules' activity. You can check the time when a message was processed, its To and From fields and which modules processed the message.

Information can be sorted by Date, Source, Destination, Subject or a module (antispam or antivirus). It also contains information about the activated message rules: if a message was processed by a rule, it will be indicated on the Message History page.

The Message History page was intended as the principal source of help and the source of information about the messages processed by the mail server. It helps resolve mail delivery problems. There are several actions that can apply to each message: it can be either delivered to its recipient or added to the white address list (in the next version) if one of the antispam modules classified the message as spam by mistake.



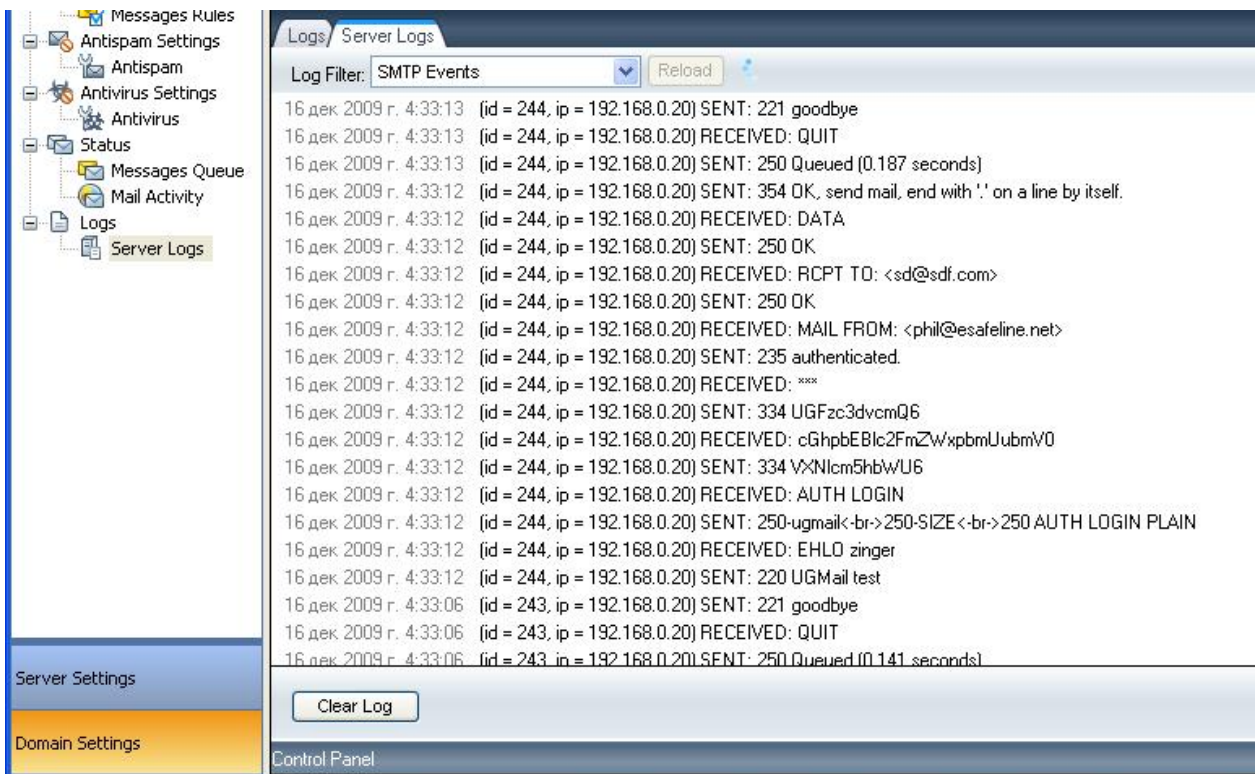
The screenshot shows the 'Message History' page in the UserGate Mail Server interface. The left sidebar contains navigation options: Messages Rules, Antispam Settings, Antispam, Antivirus Settings, Antivirus, Status, Messages Queue, Mail Activity, Logs, and Server Logs. The main content area displays a table of message history with columns for Date, From, To, Subject, and Rule Name : Action. The table shows messages received on 2009/12/21 from 'Expeditur <testaccount@mail.com>' and 'Expeditur <gregor@somedomain.com>' to recipients like 'john@example.net' and 'doe@example.net'. At the bottom, a status bar indicates 'E-mails received: 13 / Marked as SPAM: 0 / SPAM percentage: 0%'.

Date	From	To	Subject	Rule Name : Action
2009/12/21 15:54:47	Expeditur <testaccount@mail.com>	john@example.net	hello	
2009/12/21 15:54:48	Expeditur <testaccount@mail.com>	john@example.net	hello	
2009/12/21 15:54:48	Expeditur <testaccount@mail.com>	john@example.net	hello	
2009/12/21 15:54:50	Expeditur <testaccount@mail.com>	john@example.net	hello	
2009/12/21 15:54:51	Expeditur <testaccount@mail.com>	john@example.net	hello	
2009/12/21 15:54:53	Expeditur <testaccount@mail.com>	john@example.net	hello	
2009/12/21 15:55:05	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:55:07	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:55:09	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:55:10	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:55:12	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:55:13	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:56:11	Expeditur <testaccount@mail.com>	doe@example.net	hello	
2009/12/21 15:58:42	Expeditur <gregor@somedomain.com>	john@example.net	hello	
2009/12/21 15:58:44	Expeditur <gregor@somedomain.com>	john@example.net	hello	
2009/12/21 15:59:00	Expeditur <gregor@example.com>	john@example.net	hello	
2009/12/21 15:59:01	Expeditur <gregor@example.com>	john@example.net	hello	
2009/12/21 15:59:12	Expeditur <gregor@example.com>	doe@example.net	hello	
2009/12/21 15:59:14	Expeditur <gregor@example.com>	doe@example.net	hello	
2009/12/21 15:59:16	Expeditur <gregor@example.com>	doe@example.net	hello	
2009/12/21 15:59:17	Expeditur <gregor@example.com>	doe@example.net	hello	

Fig. 1. Message History

Server Log

Server Log page contains a processing log for mail server modules and can be browsed with filtering by different parameters. Mail server administrator may browse logs for each individual module of UserGate Mail Server.



The screenshot shows the 'Server Logs' page in the UserGate Mail Server interface. The left sidebar contains navigation options: Messages Rules, Antispam Settings, Antispam, Antivirus Settings, Antivirus, Status, Messages Queue, Mail Activity, Logs, and Server Logs. The main content area displays a log of SMTP events with a 'Log Filter' set to 'SMTP Events'. The log entries show various SMTP transactions, including 'SENT: 221 goodbye', 'RECEIVED: QUIT', 'SENT: 250 Queued (0.187 seconds)', 'SENT: 354 OK, send mail, end with '.' on a line by itself.', 'RECEIVED: DATA', 'SENT: 250 OK', 'RECEIVED: RCPT TO: <sd@sdf.com>', 'SENT: 250 OK', 'RECEIVED: MAIL FROM: <phil@esafeline.net>', 'SENT: 235 authenticated.', 'RECEIVED: ****', 'SENT: 334 UGFzc3dvcmQ6', 'RECEIVED: cGhpbEBlc2FmZWxpbnUubmV0', 'SENT: 334 VxNlcm5hbWU6', 'RECEIVED: AUTH LOGIN', 'SENT: 250-ugmail
250-SIZE
250 AUTH LOGIN PLAIN', 'RECEIVED: EHLO zinger', 'SENT: 220 UGMail test', 'SENT: 221 goodbye', 'RECEIVED: QUIT', and 'SENT: 250 Queued (0.141 seconds)'. A 'Clear Log' button is visible at the bottom of the log area.

Fig. 1. Server Log