UserGate MAIL SERVER

UserGate Mail Server 2.X
Administrator's Manual

Table of Contents

Introduction

UserGate Mail Server is a powerful mail gateway solution with integrated spam filtering and antivirus modules. In addition to filtering, UserGate Mail Server features message backup, rules-based message processing, POP3 messages downloading, archiving and “automatic reply.” The product is built from multiple modules, which makes it more failsafe and allows running the server on a distributed system. UserGate Mail Server supports all the leading spam filtering technologies and features Entensys Cloud Antispam and Antivirus and Bayesian statistical spam filtering solution designed by Entensys.

System Requirements

We recommend to install UserGate Mail Server on servers, running MS Windows XP/2003/Vista/7/2008 (32 or 64 bit) with a live Internet connection. The minimum recommended RAM is 512 MB for systems running Windows XP and 1 GB for servers with Windows Vista or later versions. Free disk space requirements are subject to the number of e-mail accounts and archiving requirements. The application will need some 40 MB of free disk space for installation.

UserGate Mail Server Installation and Removal

Before you install the application, make sure the required server ports (TCP 25, TCP 80 and TCP 443) are not assigned to other applications or services and connection to these ports are allowed by the firewall.

To install UserGate Mail Server, run the setup file and follow the installation wizard's instructions. The installation wizard will prompt you to specify the UserGate Mail Server administrator’s log-in, password, Email address, mail server name and select network interfaces for SMTP, HTTP and HTTPS servers. By default, UserGate Mail Server’s network services monitor all network interfaces available to the server. Mail server name will be used for processing incoming and outgoing messages (SMTP, POP3, IMAP) and normally it should be the same as MX record for your mail domain. The default installation folder is “%Program files%\Entensys\CSE” (further referred to as %CSE%).

When installation is completed, a special CSETray module's icon will appear in the system tray. You may use the tray agent's pop-up menu to launch and stop UserGate Mail Server modules and monitor their status. The agent's icon will show an exclamation mark if any of the application's modules is not running.

UserGate Mail Server is administered from a web-based administrator console at http://localhost or https://localhost.

Unless you have assigned a login and password, the default login will be "Admin" and the default password remains empty. Note that login and password are case-sensitive, i.e. the default system administrator login is Admin, started with capital A.

You may remove UserGate Mail Server from the main menu "Programs — UserGate Mail Server 2.x — Remove or Modify UserGate Mail Server 2.x," or from "Control Panel – Install and Remove Programs," or (in Windows 7/2008) from "Control Panel – Programs and Features."

UserGate Mail Server Registration

To register your UserGate Mail Server, open the administrator console in your web browser application, go to "UserGate Mail Server – Licenses" and press "Register." The registration dialog has three options: enter pin code, register free 5-account version, or obtain demo key. If you enter the pin code, you will receive a valid license trial key. Regardless of the option you select, you will need a live Internet connection over HTTPS to register the product. If you are connected to the Internet via an upstream proxy server, you can specify server settings in the registration window.

When you complete the registration process, you can view information on registered UserGate Mail Server modules and license expiry date in the administrator console. Besides, you may use the console to check for UserGate Mail Server updates. Update request is submitted to the vendor's website (http://www.entensys.com). If an update is available, your UserGate Mail Server will not be reinstalled automatically. Only a system administrator can reinstall the server application.

License Policy

UserGate Mail Server includes built-in antivirus modules from Kaspersky Lab and

Panda Software, as well as the “Cloud Antispam” and “Cloud Antivirus” modules. These modules require additional licenses to be acquired (usually 1 year). To activate a module, register your UserGate Mail Server using a special pin code (enter it to the same field where you entered regular PIN-code). The license for the UserGate Mail Server application has no expiry period.

You can use a full-featured trial version of UserGate Mail Server for 30 days. The built-in antivirus modules also have a 30-day trial period.

The number of email accounts to be filtered by UserGate Mail Server depends on the product’s license. The list of filtered email addresses will be automatically generated during the forwarding process. You can view the list on the “Processed Addresses” page in “UserGate Mail Server” section. If you have a 10-user license, the product will filter spam and complete virus checks only for the first ten addresses on the list. You can only place valid email addresses on the Processed Addresses list; no additional addresses will be processed. Addresses that are not processed are highlighted in red on the list.

MPORTANT! UserGate Mail Server licensing policy does not distinguish between an email account and an alias, which means that each alias used for any mailbox will be treated as an additional mailbox and will require license.

Spam Filtering Methods

UserGate Mail Server supports several spam filtering methods, including DNS filtering (DNSBL, RHSBL, Backscatter, MX, SPF, SURBL), “Cloud Antispam” and statistical filtering (Bayesian filtering method designed by Entensys). In addition, UserGate Mail Server supports SMTP monitoring (ensures the commands comply with RFC), allows to set maximum message size, maximum number of addressees, etc.

Spam filtering modules can be configured in a separate section of the administrator console. When installed, UserGate Mail Server already preconfigured with the most popular servers for spam check (DNSBL, SURBL).

UserGate Mail Server Quick Setup

All UserGate Mail Server modules will run automatically upon installation. To quickly configure the server, complete the following minimum setup:

- Acquire UserGate Mail Server license key;
- Create one or more mail domains;
- Create mail accounts;
- Check DNS settings;
- Check mail delivery to destinations on a remote domain (Internet).

NOTE! The default assumption is that your DNS server has the corresponding MX record for your mail domain. The MX record should be pointed to the external IP address of the computer where your UserGate Mail Server is installed. UseGate Mail Server should be accessible over SMTP (TCP port 25) protocol from the Internet.

To enable the spam filtering modules to perform properly, the network settings of the computer on which your UserGate Mail Server is installed must have correct address of the DNS server configured for domain resolution. By default, UserGate Mail Server will use the DNS server specified in the computer's network settings. However, you can list one or more additional DNS server addresses on the "UserGate Mail Server –Settings" page of the administrator console.

UserGate Mail Server Structure

UserGate Mail Server is a modular server. Each module is designed for a specific task. The modules interface via a special coordination module (CSERouter) over an RPC protocol. A web server module with XML-RPC support is used for administrator interface. The modules and their functions are outlined below.

Monitoring Agent (CSETray)

Monitoring Agent allows you to manage (enable, disable and restart) all UserGate Mail Server modules. You can use shortcut menu to control the agent. UserGate Mail Server can be controlled remotely. To enable remote control, enter the IP address of the server where CSERouter process is running in the command prompt when launching CSETray. Because CSERouter is the main module of UserGate Mail

Server, you will not be able to control this process from CSETray. To launch Administrator console double-click on CSETray agent.

Coordinator (CSERouter)

Coordinator is the main module of your UserGate Mail Server. CSERouter enables and disables other server modules, registers the modules and coordinates message exchange. Modules exchange messages over the RPC protocol.

SMTP Server (CSESmtp)

This module implements SMTP protocol and is used to process incoming mail. SMTP Client receives incoming messages, applies certain spam filtering methods (DNSBL, RHSBL, SPF, RFC restrictions, Greylisting, Tarpiting, white/black lists) and backs up the incoming messages as *.qeml files to the incoming queue folder "%CSE%\mail\queue\inc" for further processing by other modules.

Message Processing Coordinator (CSETosser)

This module coordinates message processing. CSETosser scans the outgoing message queue "%CSE%\mail\queue\out" and generates tasks for CSEProcessor module.

Message Processor (CSEProcessor)

Features of this module include spam filtering (SURBL, Cloud Antispam), virus scanning (Cloud Antivirus, Kaspersky, Panda) and message processing with rules created by UserGate Mail Server administrator or user. When processed, a message (*.xeml file) is placed into the outgoing queue "%CSE%\mail\queue\out" or quarantine folder "%CSE%\mail\quarantine" depending on the processing result. A file with delivery status information (*.dlvr) is additionally generated for messages placed into the outgoing queue.

In addition, CSEProcessor generates statistics reports on spam messages for each processed address. Information on spam messages (date, time, sender address and subject) is recorded in statistics files "%CSE%\mail\statistics\users*.stat."

Message Delivery Manager (CSEDM)

Delivery Manager module (CSEDM) monitors the outgoing queue "%CSE

%\mail\queue\out" and delivers messages across the specified routes. Besides, CSEDM monitors folder "%CSE%\mail\queue\import" containing messages incorrectly identified as spam.

Messages that cannot be immediately delivered to the addressee are placed in folder "%CSE%\mail\queue\out\try" for delivery retry. You can set the number of delivery retries and intervals between such retries in Delivery Settings section of "Communication Server – Settings" page.

Statistics Module (CSEStat)

This module records mail processing statistics. All statistical information (date, time, source and destination addresses, UserGate Mail Server modules used for processing and the processing result) is recorded in the built-in SQLite3 database. Database file is located in %CSE%\mail\statistics\stat.csdb folder.

IMAP Client (CSEImapC)

IMAP client manages IMAP folders located on a remote mail server. CSEImapC supports MS Exchange 2003 and Lotus Domino R7 and is used to create a special IMAP folder structure on a remote mail server and process messages in such folders.

In addition, CSEImapC downloads messages from remote IMAP mailboxes.

POP3 Client (CSEPop3c)

Mail server client over POP3 protocol. Downloads mail from remote POP3 accounts. All critical data, such as download date and status and message unique identifiers are stored in a special folder – %CSE%\mail\pop3c.

IMAP-server (CSEImap)

IMAP-server processes mail transmitted via IMAP/IMAPs protocol. It performs as a mail server via IMAP/IMAPs protocol between server and clients.

POP3 Server (CSEPop3)

IMAP-server processes mail transmitted POP3/POP3s protocol. It performs as a mail server via IMAP/IMAPs protocol between server and clients.

Scheduler (CSECron)

The Scheduler module is used to update virus definitions of the antivirus modules and distribute UserGate Mail Server statistics.

Scheduler supports daily, weekly, monthly and custom schedules. CRONTAB line is used to create a custom schedule. The line includes six segments divided by spaces (or tabs). Each segment sets time as follows:

(minute:0-59) (hour:0-23) (day:0-31) (month:0-12) (week day:0-6, 0-Sunday)

Each of the first five segments may have the following settings:

- Asterix (*) sets the full range (from the first to the last element);
- Dash (-) sets a specific range; for example, “5-7” means 5, 6 and 7;
- Lists – numbers (or range of numbers) divided by commas; for example, “1,5,10,11” or “1-11,19-23;”
- Incremented asterix or range is used to set increments in a given range of numbers. The increment is set with a slash. For example, “2-10/2” means “2,4,6,8,10”, and “*/2” in the “hours” segment means “every two hours”.

Mail Backup Utility (CSESync)

CSESync periodically copies all mail into a backup folder (specified in administration console) and, if necessary, restores the latest version of a message and mail server settings from the backup copy.

Web Server (CSEHTTP)

The web server is used to administer UserGate Mail Server.

Web Server API (CSESrvCtrl)

This module implements API for the XML-RPC interface of the web server (CSEHTTP).

Message Processing

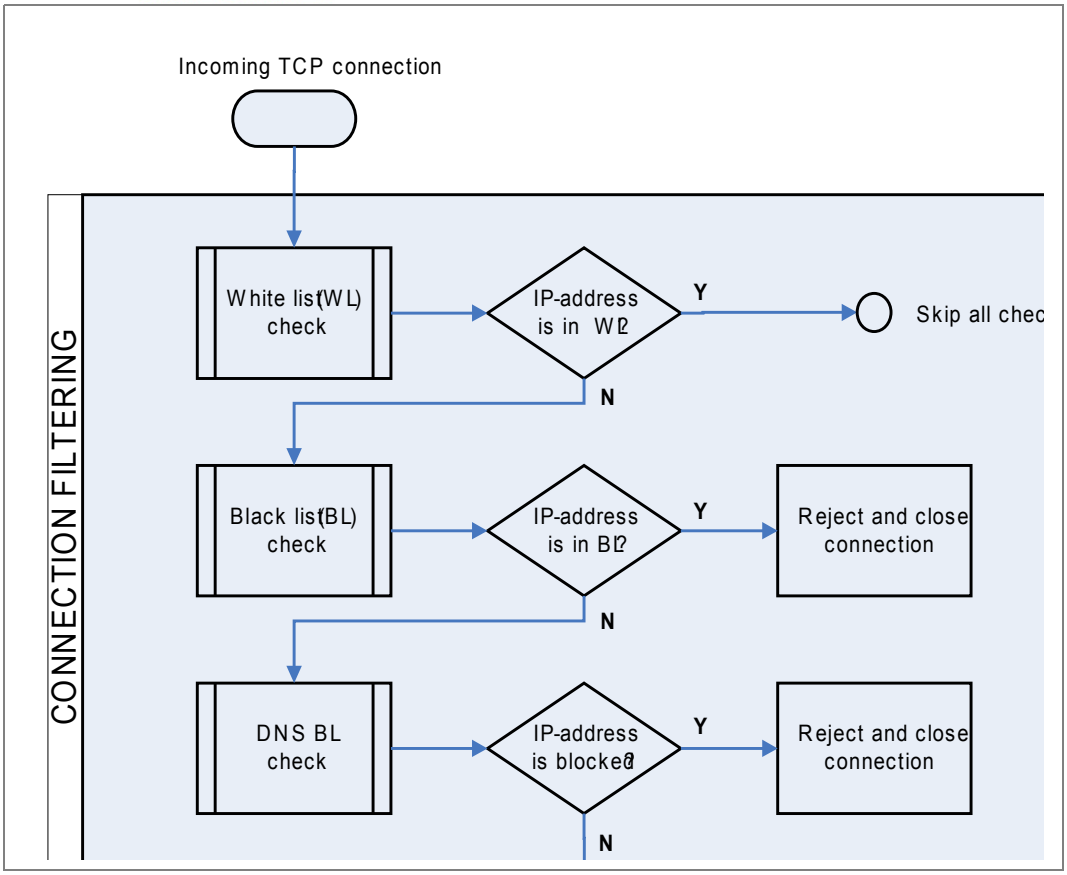
When processed by UserGate Mail Server, messages go through several filtering stages, including connection filtering, sender filtering, recipient filtering and content

filtering. At the last stage, a message is filtered in accordance with the rules created by the administrator.

Connection Filtering

Connection filtering flow chart is shown in Fig. 1. When an incoming connection is registered on TCP port 25, UserGate Mail Server scans through its global white list of IP addresses. The white list is assigned on the “Antispam – Black and White Lists” page. Each list item may be an IP address (a range of IP addresses), a domain name (A-type record) or a name of domain mail exchanger (MX-type record). UserGate Mail Server resolves the listed names into corresponding IP addresses and generates global lists of resolved and restricted IP addresses. If the incoming connection originates from a white list IP address, UserGate Mail Server will skip all subsequent checks up until the rules created by the administrator and receive the message. UserGate Mail Server will block connection for IP addresses listed on the black list.

The next step is DNSBL check. If the incoming connection originates from an IP address that is on the spam list, UserGate Mail Server will reject and close the connection and generate a corresponding error message. You can set DNSBL parameters on the corresponding page of the administrator console. DNSBL parameters include names of DNSBL servers used in the check process and the exceptions list. Each exceptions list item may be represented by an IP address, domain name or name of mail exchanger.



Sender Filtering

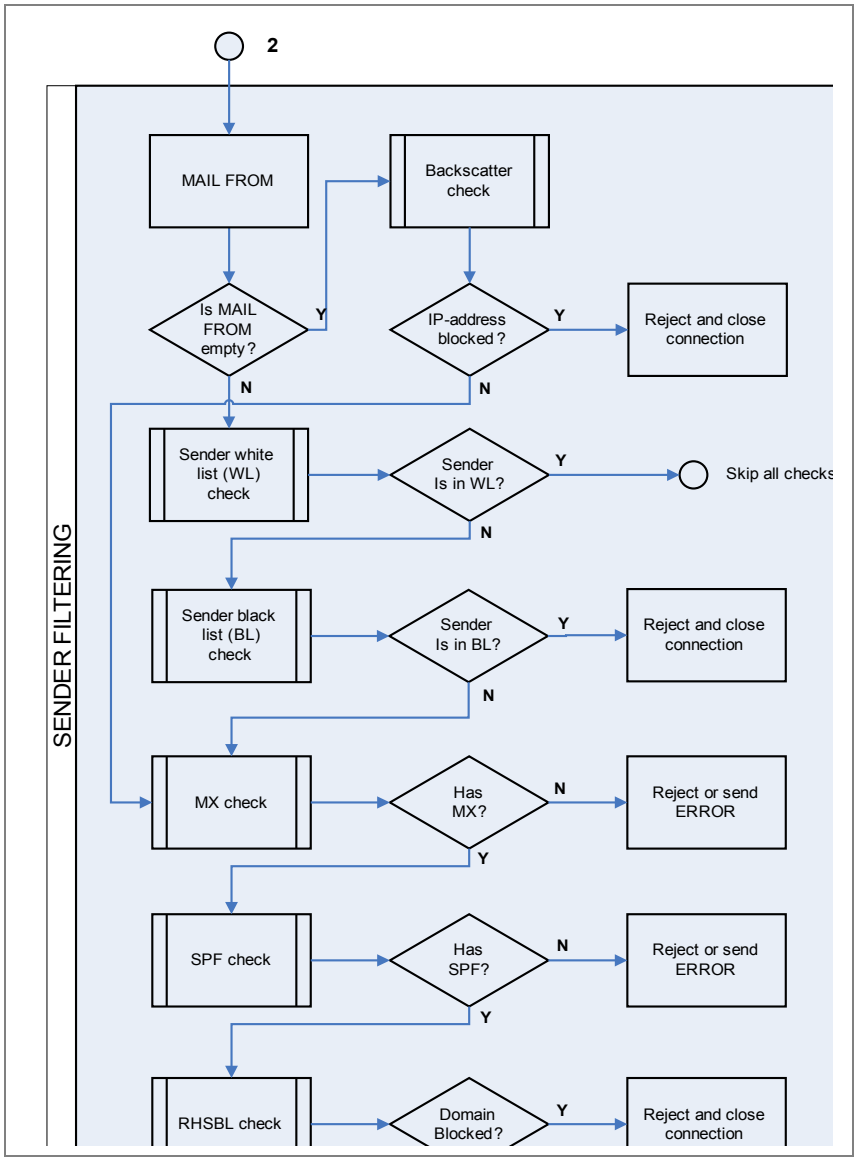
UserGate Mail Server starts sender filtering after the MAIL FROM command has been received. If the address in the MAIL FROM command is a blank address (“<>”), UserGate Mail Server will complete the Backscatter check. This check is used, for example, to block “fake” information messages, such as delivery failure messages. Backscatter settings (“Antispam – Backscatter” page) should specify the address of the server used for the check and an exceptions list.

If the MAIL FROM command does not contain a blank address, UserGate Mail Server will scan the black and white lists for this address. If the address is found on the black list, UserGate Mail Server will close the incoming connection and produce a corresponding error message. If the address is on the white list, all subsequent checks will be skipped.

The next step is to check if the domain whose address is listed in the MAIL FROM command has an MX (Mail eXchanger) record and a SPF (Sender Policy Framework) record. To enable MX record check, go to “Antispam – Settings” page of the administrator console. SPF check parameters are assigned in the Antispam

section of the corresponding SPF page. You can set UserGate Mail Server to respond to the results of MX and SPF checks in the server settings.

The last step is to complete RHSBL filtering by the domain name listed in the MAIL FROM command. If the domain name is found on the spam list, UserGate Mail Server will close the incoming connection and produce a corresponding error message.



Recipient Filtering

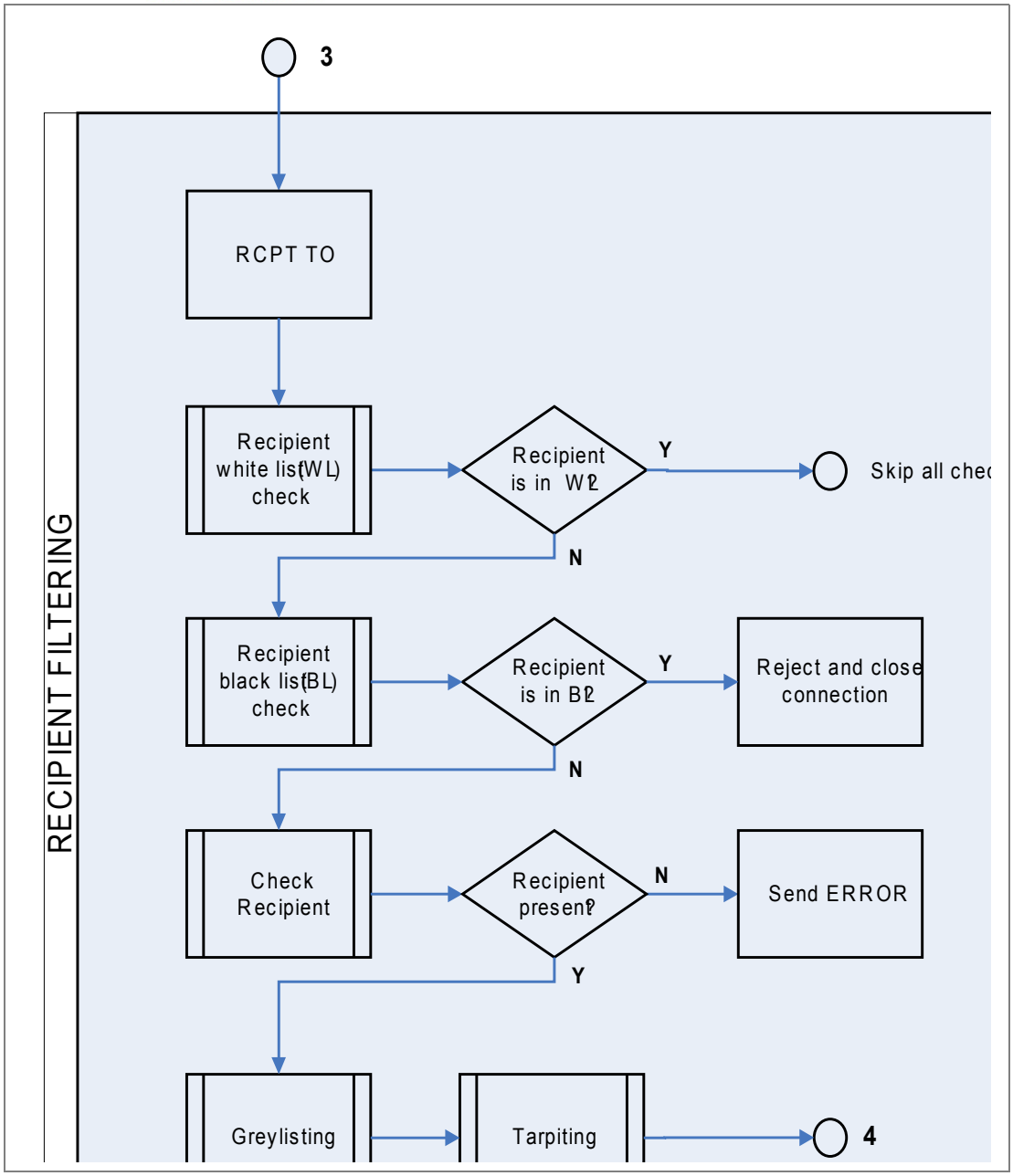
UserGate Mail Server starts recipient filtering after the RCPT TO command has been received. The received address is checked against the black and white lists. If the destination address is found in the white list, all subsequent checks will be skipped. If the address is found on the black list, UserGate Mail Server will close the incoming

connection and produce a corresponding error message.

Next, UserGate Mail Server checks the availability of the destination address in accordance with the mail domains (“Communication Server – Domains” page). If destination domain is remote domain, then UserGate Mail Server connects to the mail server specified in the route and requests the availability of the recipient by sending the RCPT TO command. If the mail server contains no such recipient address, UserGate Mail Server will produce a corresponding error message.

For each incoming connection, UserGate Mail Server creates a triplet (IP address originating the connection, MAIL FROM address and RCPT TO address) and scans the internal list of triplets for previous connections. If the received triplet is not found in the internal triplet list (i.e. the connection with the given parameters is a new connection), UserGate Mail Server will produce a temporary error message. This is a Greylisting check procedure. You can set the Greylisting parameters in the Antispam section of the corresponding Greylisting page.

UserGate Mail Server supports the Tarpiting feature to protect you from address guessing. The Tarpiting feature “delays” mail server response when a new destination address is received in the RCPT TO command. By default, response delay will be enabled if more than five destination addresses are received at once. You can set the required Tarpiting parameters on the “Antispam – Settings” page.



Content Filtering

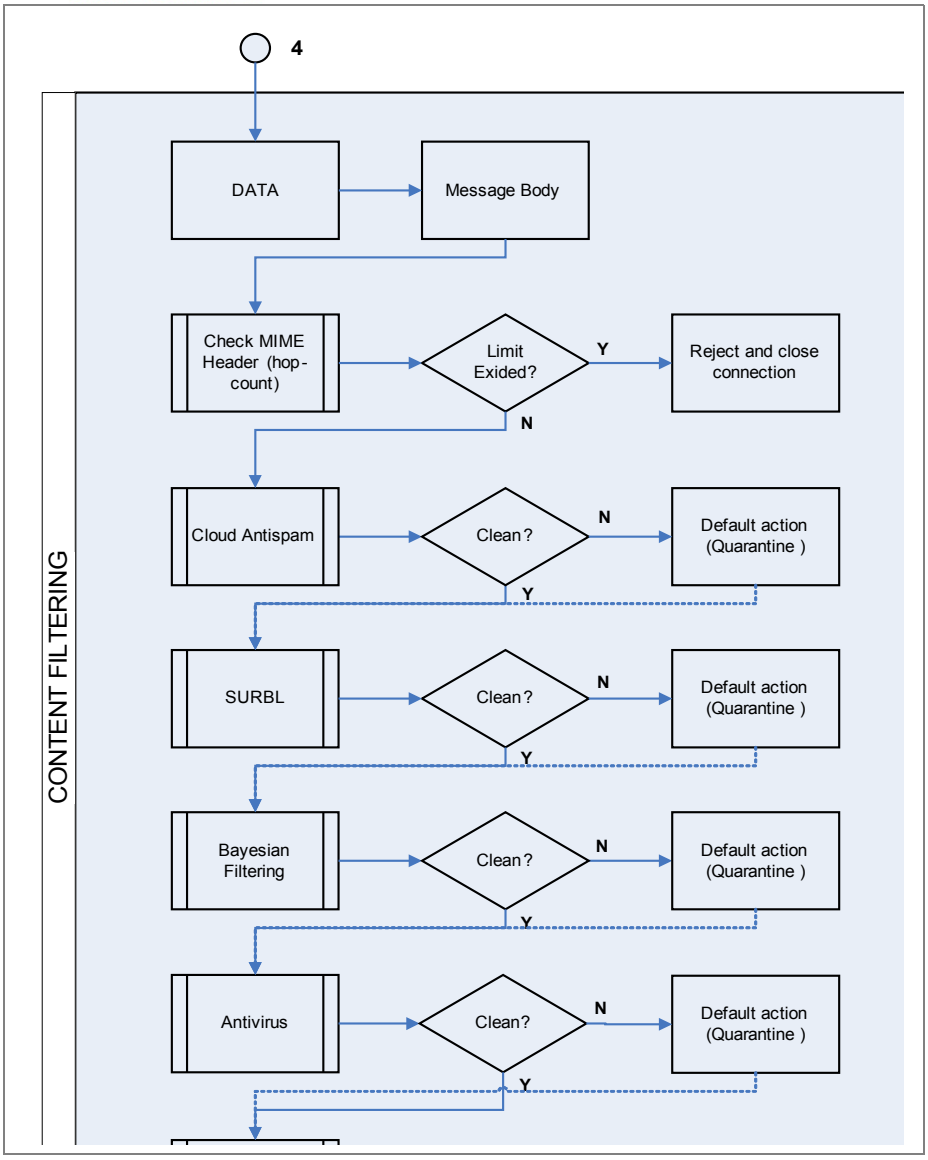
UserGate Mail Server will start content filtering after the message body has been received. The first step is to check MIME headers. If the message delivery route specified in the header is longer than the set limit ("Maximum redirect depth" parameter on "Communication Server – Settings" page), UserGate Mail Server will block the message. Besides, a reply message will be generated at the MIME check step if the Autoreply function is enabled.

The next step is to check the entire message using an online service (the so-called Cloud Antispam). The application sends a unique message hash to a remote server

using the HTTP POST method. Cloud Antispam requires HTTP to be enabled on the computer where UserGate Mail Server is installed. Messages identified as spam or infected messages (Cloud Antispam also scans messages for viruses) are placed into the quarantine folder (%CSE%\mail\quarantine). You can push messages in the quarantine folder to their destination addresses. To do so, move the corresponding *.xeml file of a message from "%CSE%\mail\quarantine" folder to "%CSE %\mail\import" folder. To push-send a message, use the shortcut menu on the "Monitoring" page.

NOTE! Quarantine folder is periodically cleaned. Cleaning settings are configured in "Antispam-Main settings" section of Administrator's console.

Next, UserGate Mail Server completes SURBL filtering and statistical check (Bayesian filtering). The Bayesian filtering algorithm designed by Entensys allows automatic learning using the messages identified by Cloud Antispam as "clean messages." The last step includes virus check and message processing using the rules.



Mail queue

You can check messages waiting for delivery in the mail queue on «Monitoring - Mail Activity» page using filter dm:pending.

Delivered messages are stored for two weeks in the folder “%CSE %\mail\sump_delivered”.

Messages which could not be delivered from a first try are placed in the folder %CSE %\mail\sump. Next delivery attempts will be happening according to the following schedule:

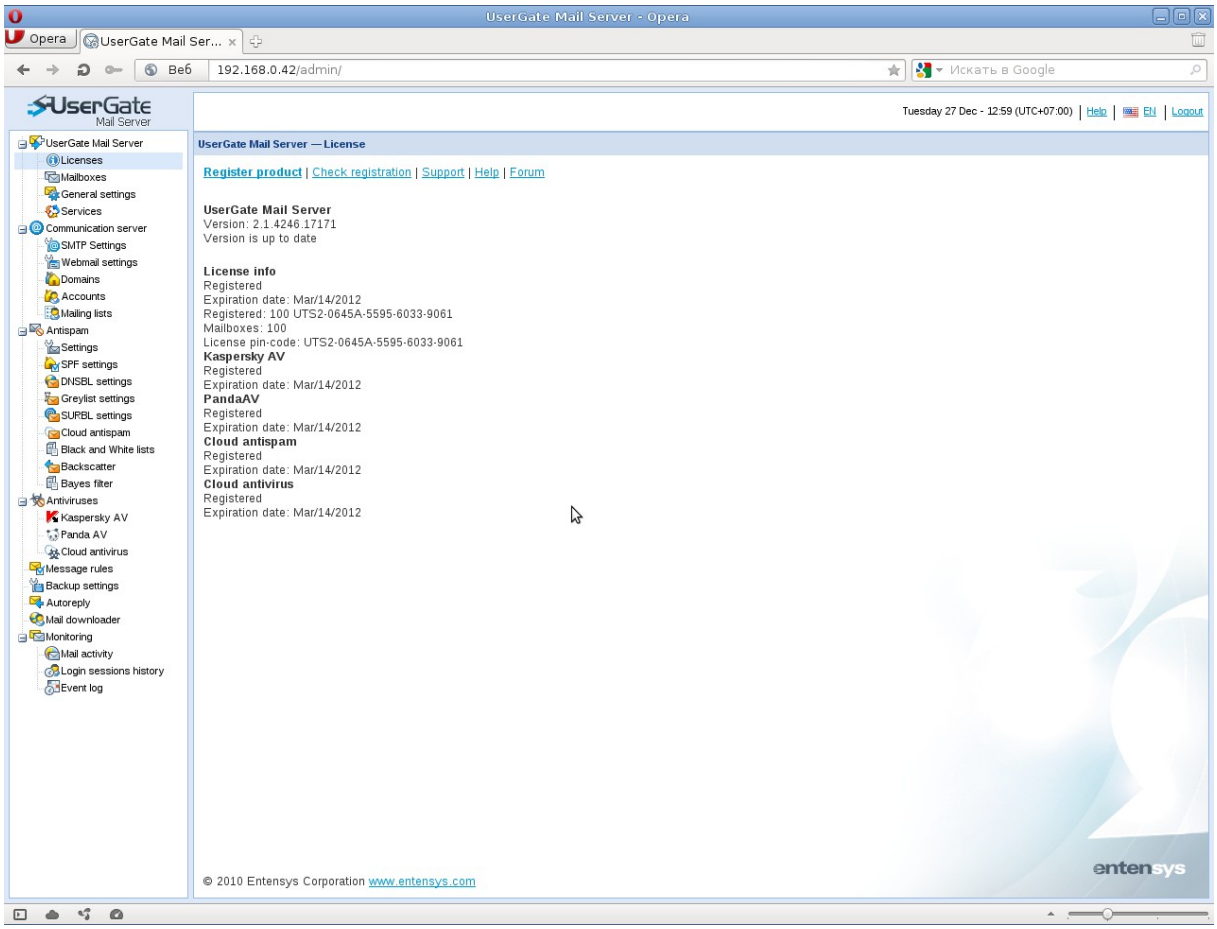
- after 30 minutes after previous attempt;
- after 1 hour after previous attempt;
- after 2 hour after previous attempt;
- after 3 hour after previous attempt;
- every 4 hours after previous attempt.

UserGate Mail Server Administrator Console

UserGate Mail Server

Licenses

The Licenses page features all information on the UserGate Mail Server and additional modules licenses. The page also contains “Register product” and “Check registration” buttons. All other links will take you to the technical support section at the Entensys web-site. This page can also check if new version is available at the vendor’s site.

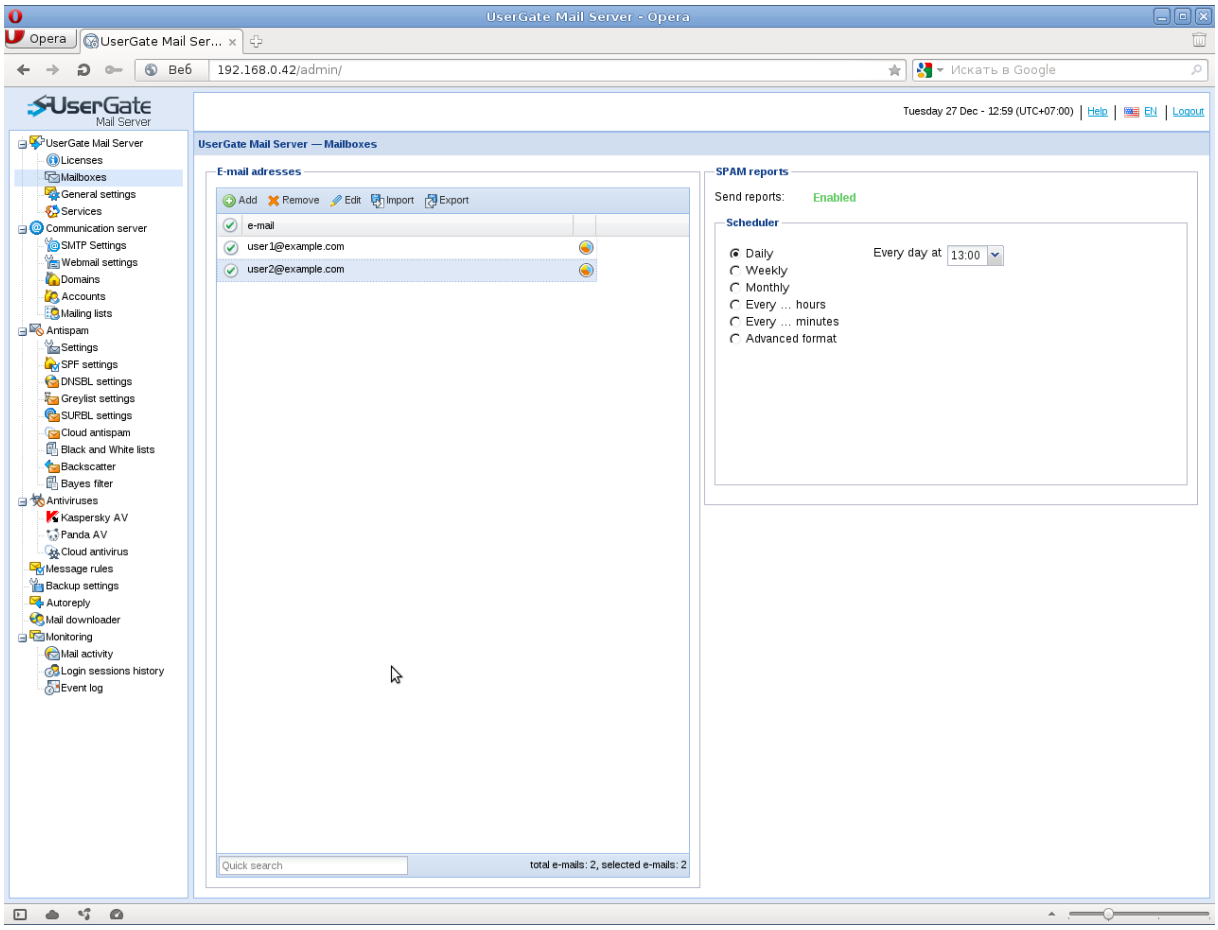


Mailboxes

Mailboxes page lists all Email addresses servicing by the UserGate Mail Server. This list contains e-mail addresses and their aliases. Email accounts which are not covered with the license are marked by a red “x”. You cannot set more processed accounts that the license allows.

Contact list can be uploaded into the application or dumped from it when necessary. When the contact list is exported, each contact must be listed on a separate line. For more convenience, the page now allows searching and highlighting the desired accounts and displaying general status of all processes accounts

The addresses page contains a spam statistics distribution scheduler. You may use it to list accounts to which statistics will be distributed or deny such distribution for specific accounts (see column opposite the email accounts). Grey icon color means that spam statistics will not be sent to the user, colored icon means that statistics will be sent according with the schedule.



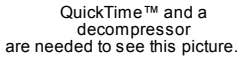
Spam statistic report is sent as an email with the list of all messages blocked as spam. It contains time, sender's email address and link to release spam messages from quarantine and deliver them to recipient.

Genaral Settings

The page contains the following parameters:

- DNS configuration (if DNS addresses from the system are used, they are specified in brackets).
- Web interface configuration (administrator log-in and password).
- Information about free space on the server's disk.
- Web interface language set the default language for Administrator's console and web mail client. You need to reload web console to apply new settings.
- Time zone setting.

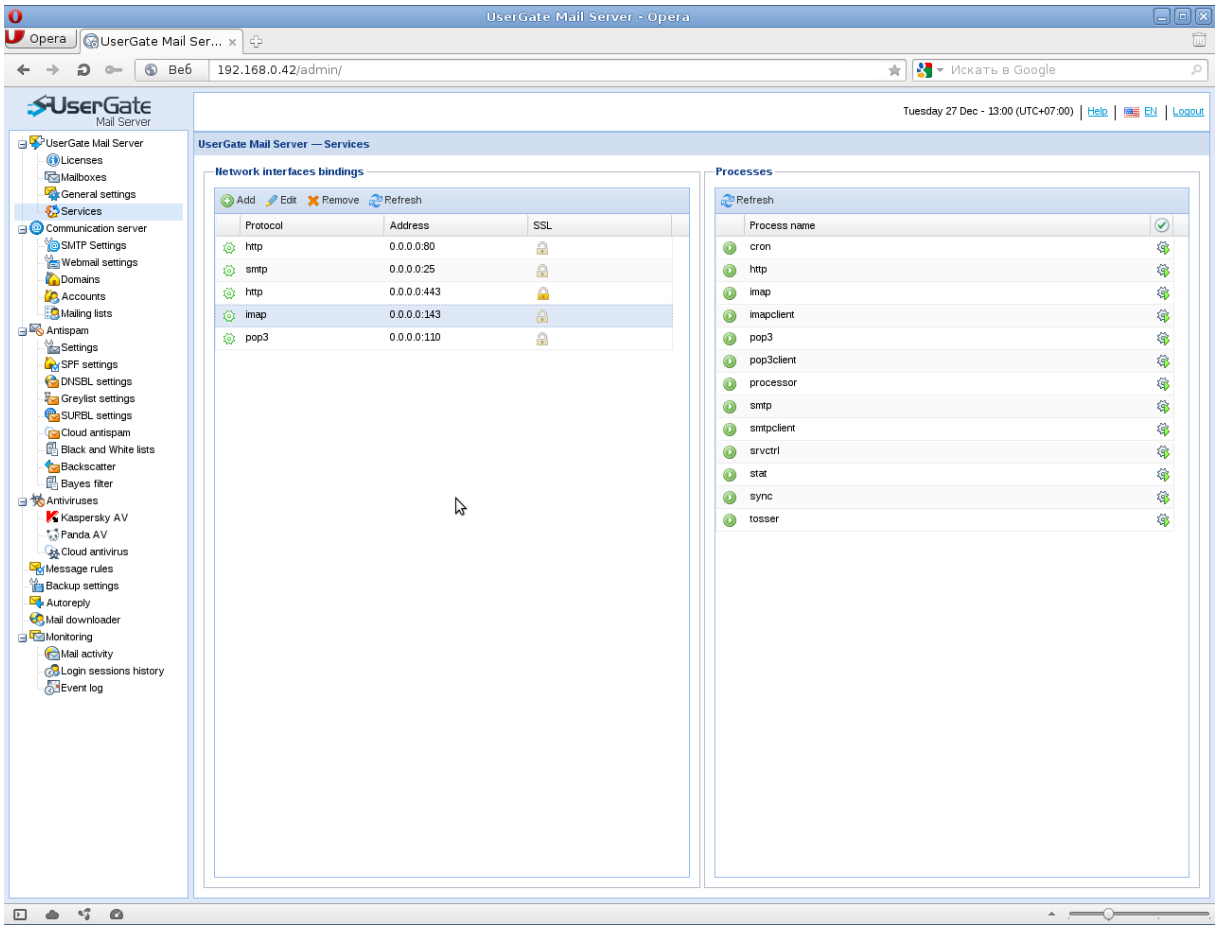
  Attention! You should set correct time zone to show correct time in the "Message log". Make sure that computer system time and time zone in operating system have valid values as well.
- Send bug-report for vendor for analysis. New feature which allows automatically sending crash-reports to vendor. If enabled, crash report will be sent to "dump@entensys.com" every time any UserGate module will be crashed. Usually, mail is about 100-200 Kb.
- Mailing address for important notifications. This address will be used about important mail server events, such as low disk space.



Services

This page is designed for determining listening ports, starting/stopping UserGate Mail Server services and establishing how they are launched.

All the UserGate Mail Server's services are shown in the right pane. They can be stopped, and the start up mode can be changed from automatic to manual.



Communication Server

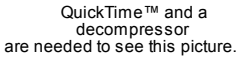
SMTP server settings

SMTP server processes inbound and outbound mail. The following parameters are specified in the settings:

- Server domain name (Server address). Usually it should be the MX-record for your domain.
- Outbound relay settings. If it must be used, specify server address, port and login and password for relay server authorization. The check connection button is provided to verify that all parameters are correct. When you press the button, the server tries to connect to the specified server and send a message. In any event, you will see the connection check result in a corresponding notification.
- Incoming relay settings. Mail server may be used as a server forwarding mail from third party domains. To make it run as a relay server without authorization (open-relay), we recommend restricting the number of IP addresses to which

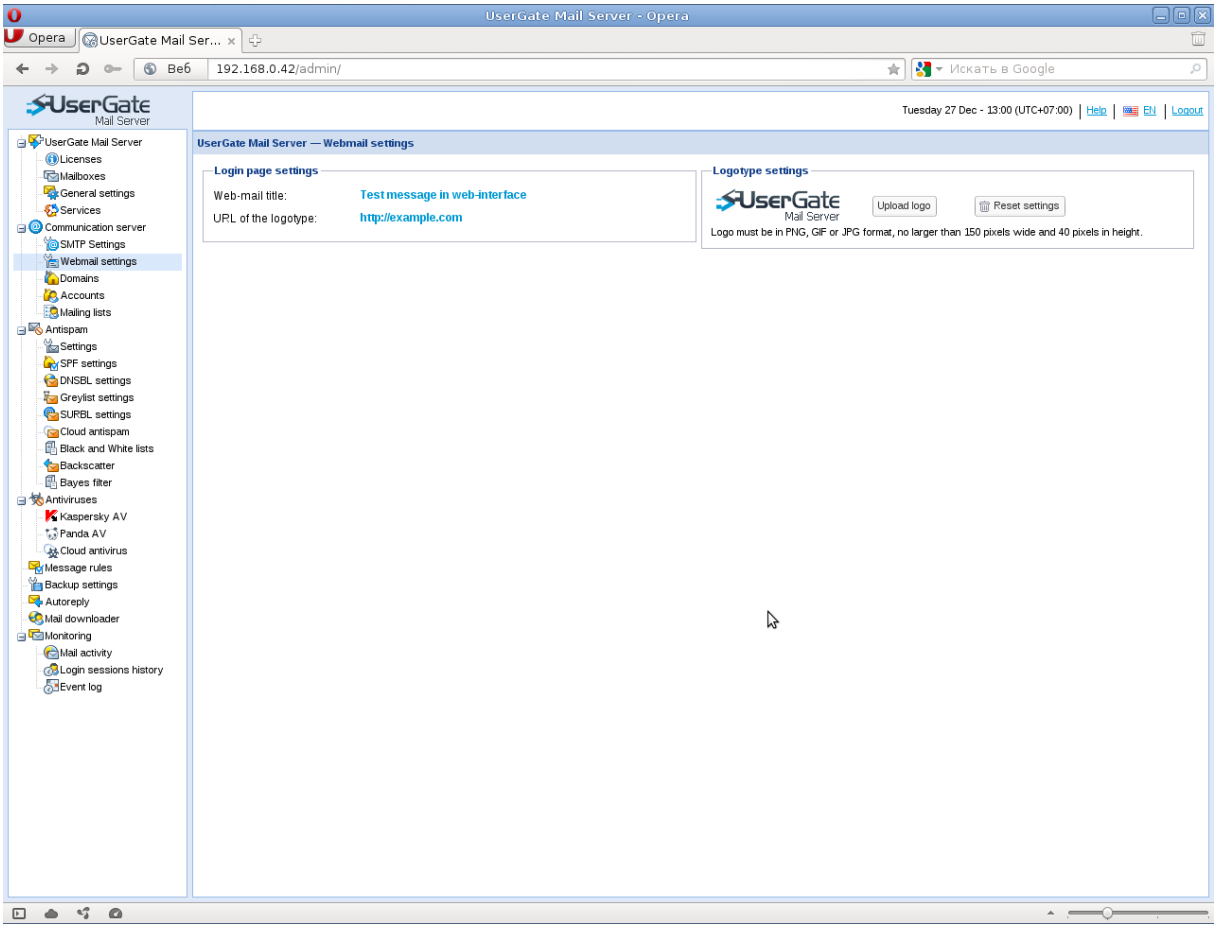
connection is permitted. Specify the applicable IP addresses in the “SMTP – No authorization servers” section.

- TTL for delivered messages. Set time which all delivered messages stored in the specific folder.
- Maximum recipients in batch – maximum number of recipients which can be set in “To” field in e-mail.
- Maximum redirect depth parameter sets the number of intermediate servers delivering a message.
- Maximum message size. Maximum message size which can be sent over mail server.
- Delivery expiration time. Maximum time in minutes server trys to deliver message. Default is 7 days.
- Send DSN (delivery status notification). Enables or disables sending DSN.
- “Server address and port for SPAM messages” is the address specified in the spam distribution emails to remove messages from quarantine. Usually, this parameter is equivalent to the local IP address or (domain name) of the machine on which the mail server is installed. You can also set a port by specifying it using colon, for example «IP-address:8080».



Web interface settings

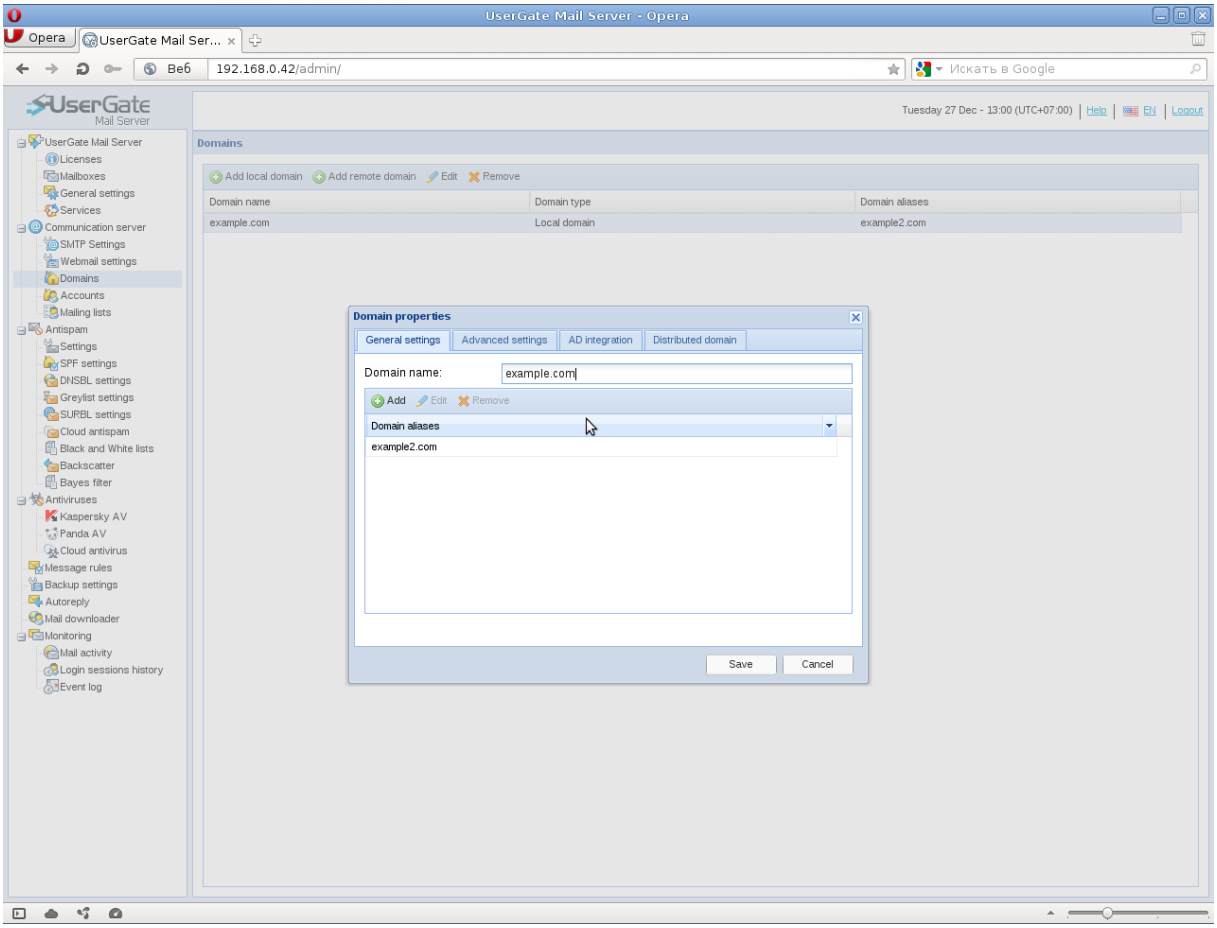
On this page, you can assign and manage the company logo that users will see when entering the web interface of their mailbox. The logo image must be in the png, jpg or gif format and have the maximum size of 140x40 pixels. You can always reset the logo to its original view by pressing the “reset” button.



Domains

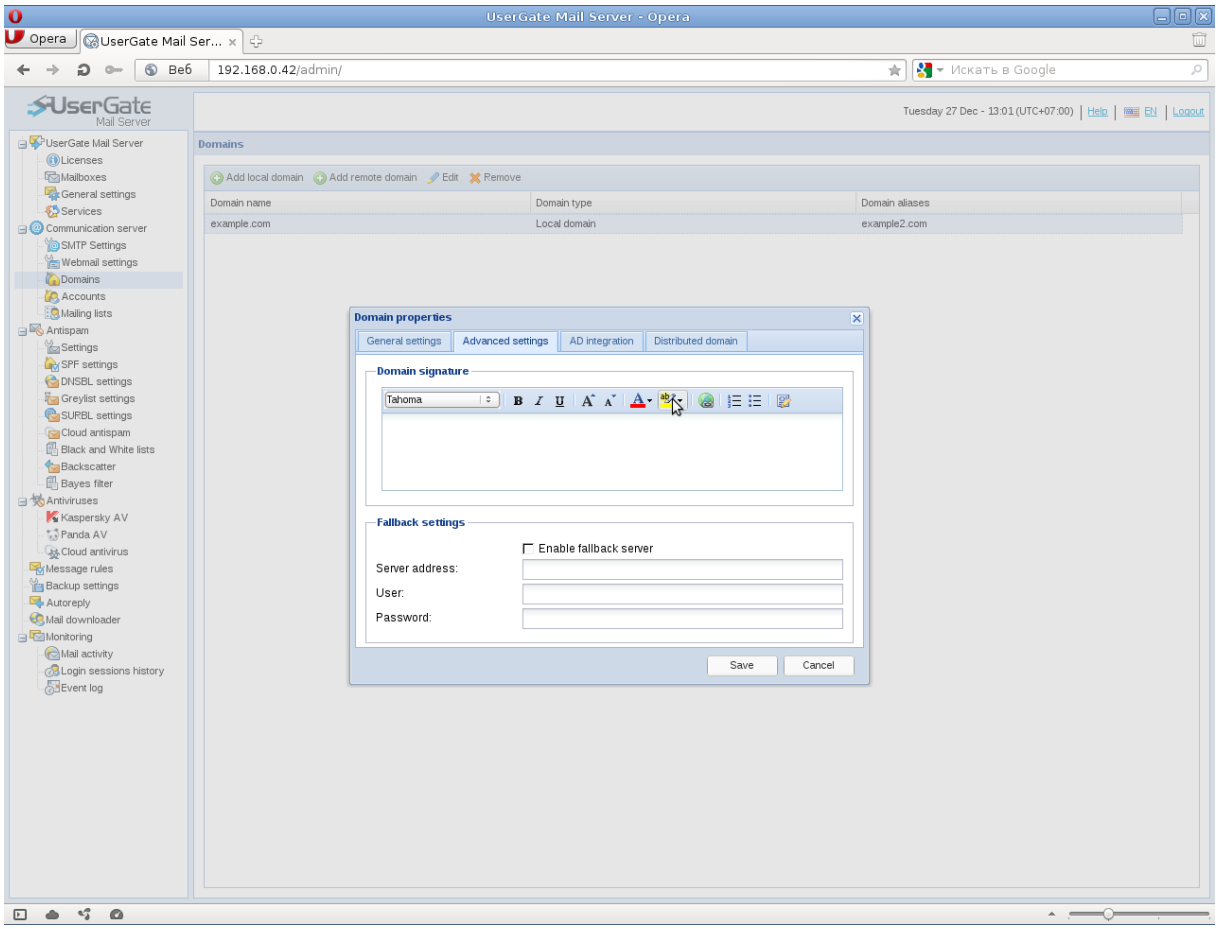
UserGate Mail Server supports two types of mail domains, – local domains and remote domains. A domain is called local if accounts on this domain are serviced by Mail Server itself. For a remote domain, Mail Server acts as a mail gateway that receives incoming mail and forwards it to a remote mail server.

A local mail domain can be a simple domain, or it can be integrated with Active Directory. In the case of simple domain, all account data is stored on the mail server. In cases of integrated domains, accounts are stored in Active Directory service.



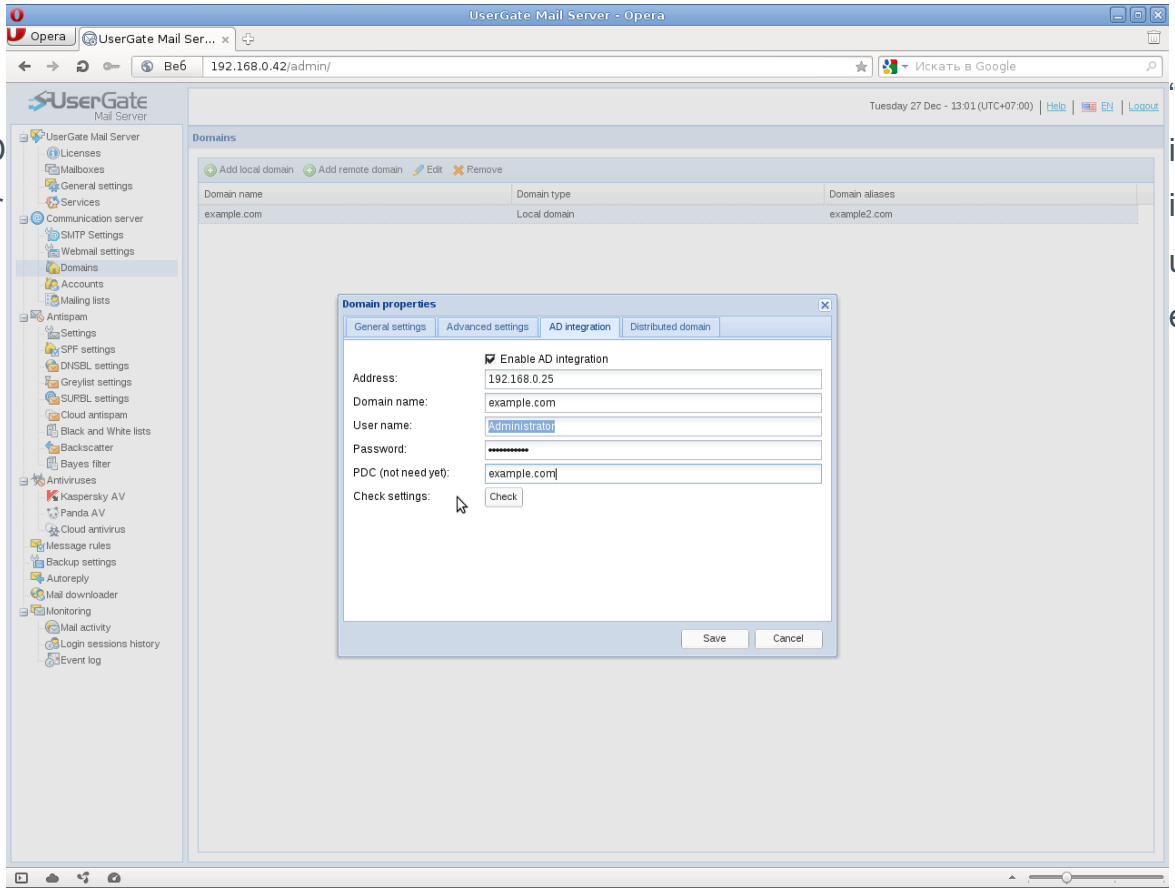
Domain settings

- “Domain name” is the name that will be placed in all messages after @. “Alias” is a full equivalent of the domain, but when messages to the recipient are processed, the alias will be placed to check validity of the recipient. A message will be accepted for delivery if the alias matches the recipient (domain name).
- “Additional settings” include the “Domain signature” that will be added to each message sent by the mail server.
- “Enable fallback server” is a special option that can be used to send messages to a different server containing a full copy of the local domain or its missing portion. For example, a number of mail accounts may be stored on a local domain and another part – on a remote server. In order for the mail server to send mail to this remote domain, enable the “fallback server” option and set the authorization parameters. If, during further verification, a specified recipient is not found on the local domain, the mail server will try searching the recipient on the fallback server. If the search is successful, the mail will be delivered to the recipient.



■ “AD integration”. To enable Active Directory integration, specify the following parameters in the Active Directory tab of the mail domain properties page: domain controller IP address, Active Directory domain name, domain controller name, as well as login and password of user authorized to access the LDAP directory. When you press “Check” button, UserGate Mail Server will modify the AD schema by adding the required user classes and attributes. Mail domain name in UserGate Mail Server should not necessarily match the Active Directory domain name.

NOTE! If you cannot modify AD schema, please check if you can access domain controller over LDAP protocol (TCP 389), and you have required privileges. Changes made to AD schema cannot be reverted back.

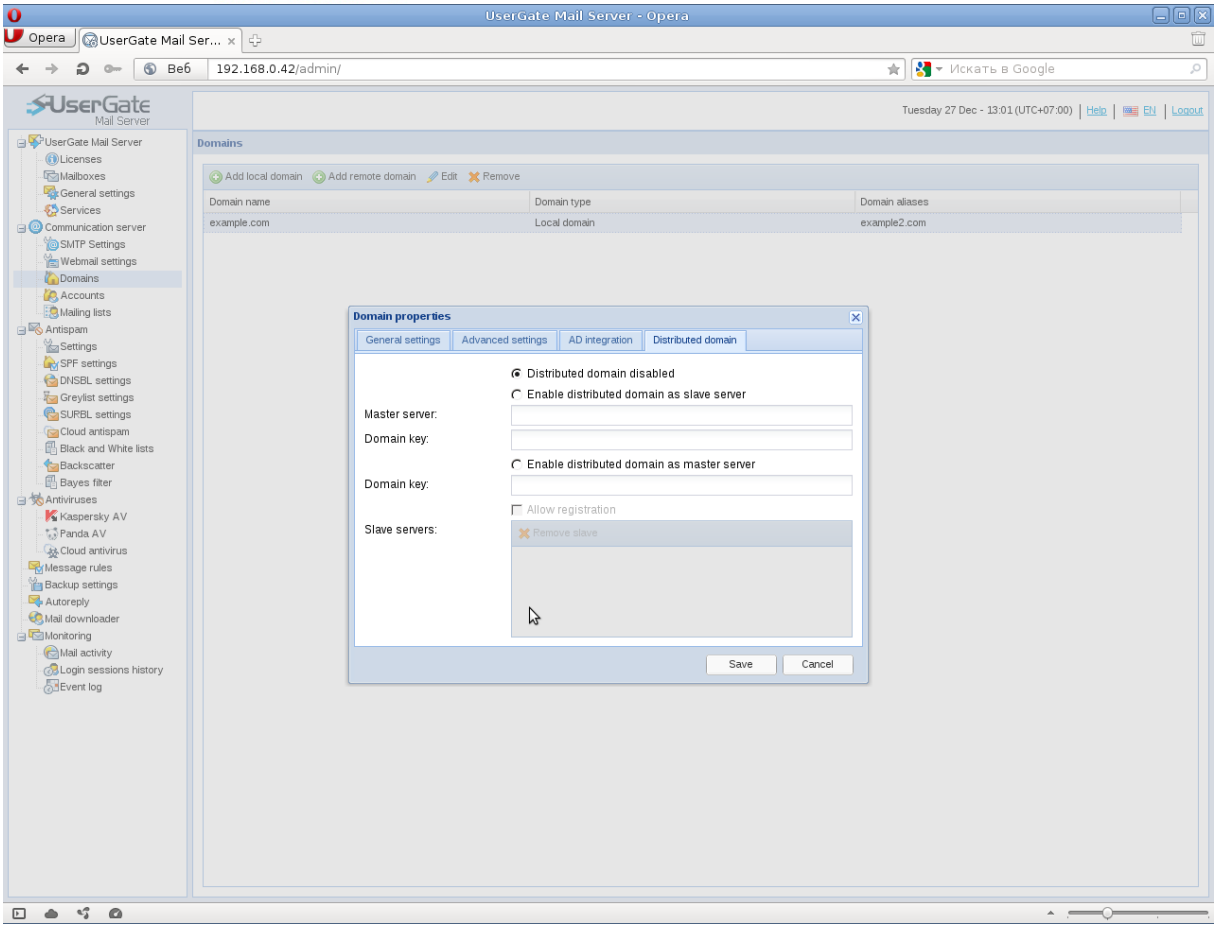


■ “Distributed domain” is a mail server mode that allows distribution across several servers. This mode helps distribute the load among several servers or separate the mail domain by company branches. If you use the distributed domain mode, one of the servers will be the master server, and others – slave servers. Connection to the master server will only be allowed if a secret authorization word is specified (Domain key).

“Master server” – IP address of the master server in the distributed domain;
“Domain key” – password of the master server domain;

“Enable as master server” – allows making a current server the master server of the distributed domain. In this case, you must enter the password.

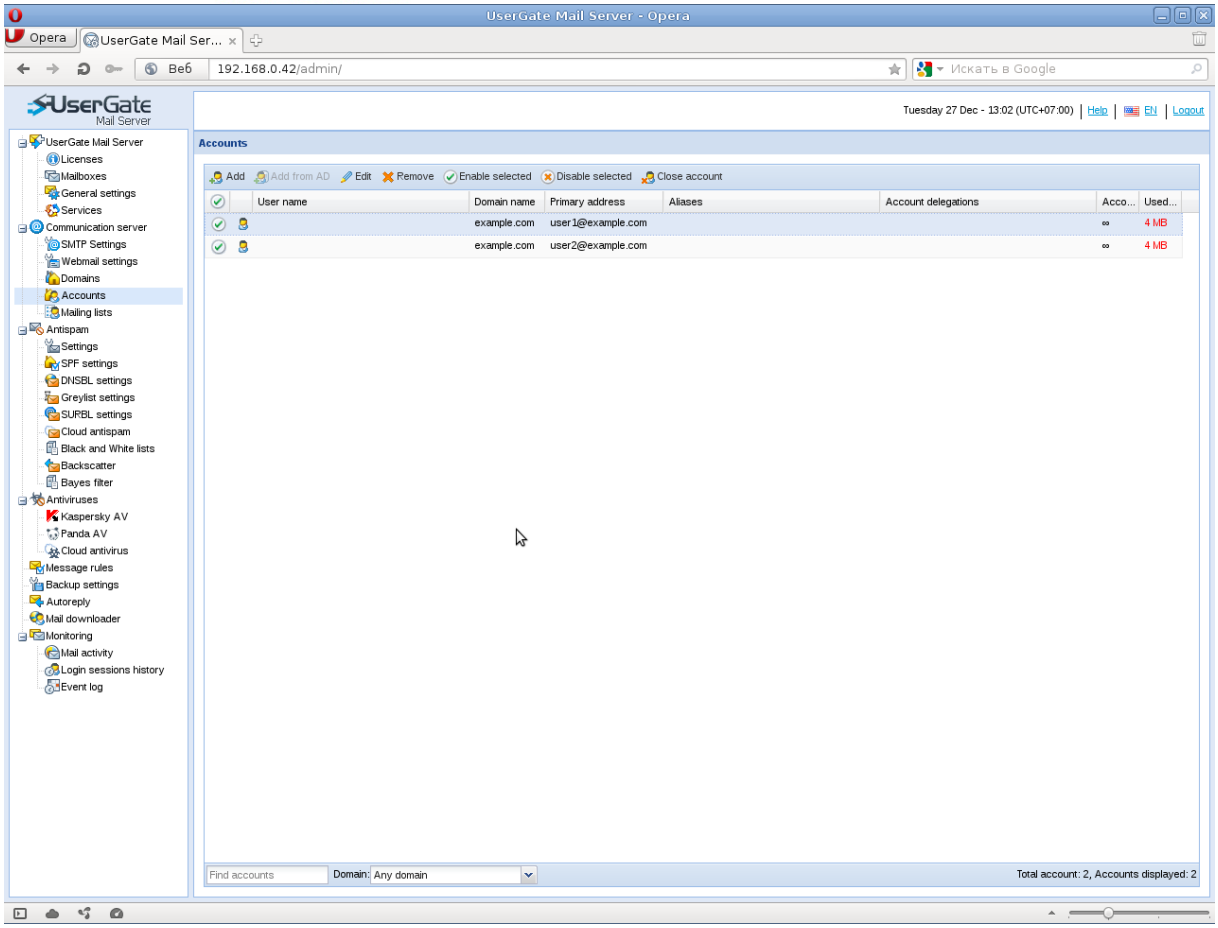
“Allow registration” – allows you to enable or disable authorization of slave servers in the distributed domain.



Accounts

The Accounts page is used to create new user accounts for UserGate Mail Server. When you create a new account, please specify the following parameters:

- Primary address;
- Domain name;
- Password.


UserGate Mail Server - Opera
Opera
UserGate Mail Ser...
Веб
192.168.0.42/admin/
Искать в Google
UserGate Mail Server
Tuesday 27 Dec - 13:02 (UTC+07:00) | Help | EN | Logout
UserGate Mail Server
Licenses
Mailboxes
General settings
Services
Communication server
SMTP Settings
Webmail settings
Domains
Accounts
Mailing lists
Antispam
Settings
SPF settings
DNSBL settings
Greylist settings
SURBL settings
Cloud antispam
Black and White lists
Backscatter
Bayes filter
Antiviruses
Kaspersky AV
Panda AV
Cloud antivirus
Message rules
Backup settings
Autoreply
Mail downloader
Monitoring
Mail activity
Login sessions history
Event log
Accounts
Add
Add from AD
Edit
Remove
Enable selected
Disable selected
Close account
User name
Domain name
Primary address
Aliases
Account delegations
Acco...
Used...
example.com
user1@example.com
∞
4 MB
example.com
user2@example.com
∞
4 MB
Find accounts
Domain: Any domain
Total account: 2, Accounts displayed: 2

The following parameters are optional:

- Quota;
- Delegation;
- Personal information;
- Mailing list;

«Quarantine enabled» moves all marked as SPAM messages into IMAP-folder «Quarantine» in the user's mailbox. This folder is accessible via IMAP enabled mail client or via web-interface.

«Mailing lists» allows to include user to required distribution lists.

"Account Quota" parameter is used to limit the size of a user's mailbox. Mailbox size is unlimited by default. The size of the user's mailbox and the applied quota is displayed on the Accounts page.

To create new mail accounts on a domain integrated with Active Directory, choose "Import from Active Directory." The import dialog window will display all users of the Active Directory domain. To create a mail account, select the appropriate users and press "Import." The default user address format is *username@mail_domain_name*, where *username* is the user's Active Directory login. You may change the address prefix (the part before @) in the import dialog window and in the mail account properties.

NOTE! User's Active Directory password will be used for their authorization in UserGate Mail Server. The username can be represented by either the domain login, or the mail prefix, to include any of the aliases, if listed in the account properties.

"Delegation tab" in the account properties can be used to grant other users access to the account. UserGate Mail Server supports two types of delegations:

- Administrator delegation
- User delegation.

The first type of delegation is created by UserGate Mail Server administrator. The second type is created by the user through the web client. User delegations will not be displayed in UserGate Mail Server Administrator Console.

To work with delegated accounts, user should include delegated account in the general settings of UserGate Mail Server web client. UserGate Mail Server web client allows working with a delegated account on behalf of such a delegated account.

"Distribution list" is an e-mail address for a certain mail server user group. Any distribution list can be one of the following:

- Public distribution list
- Subscription

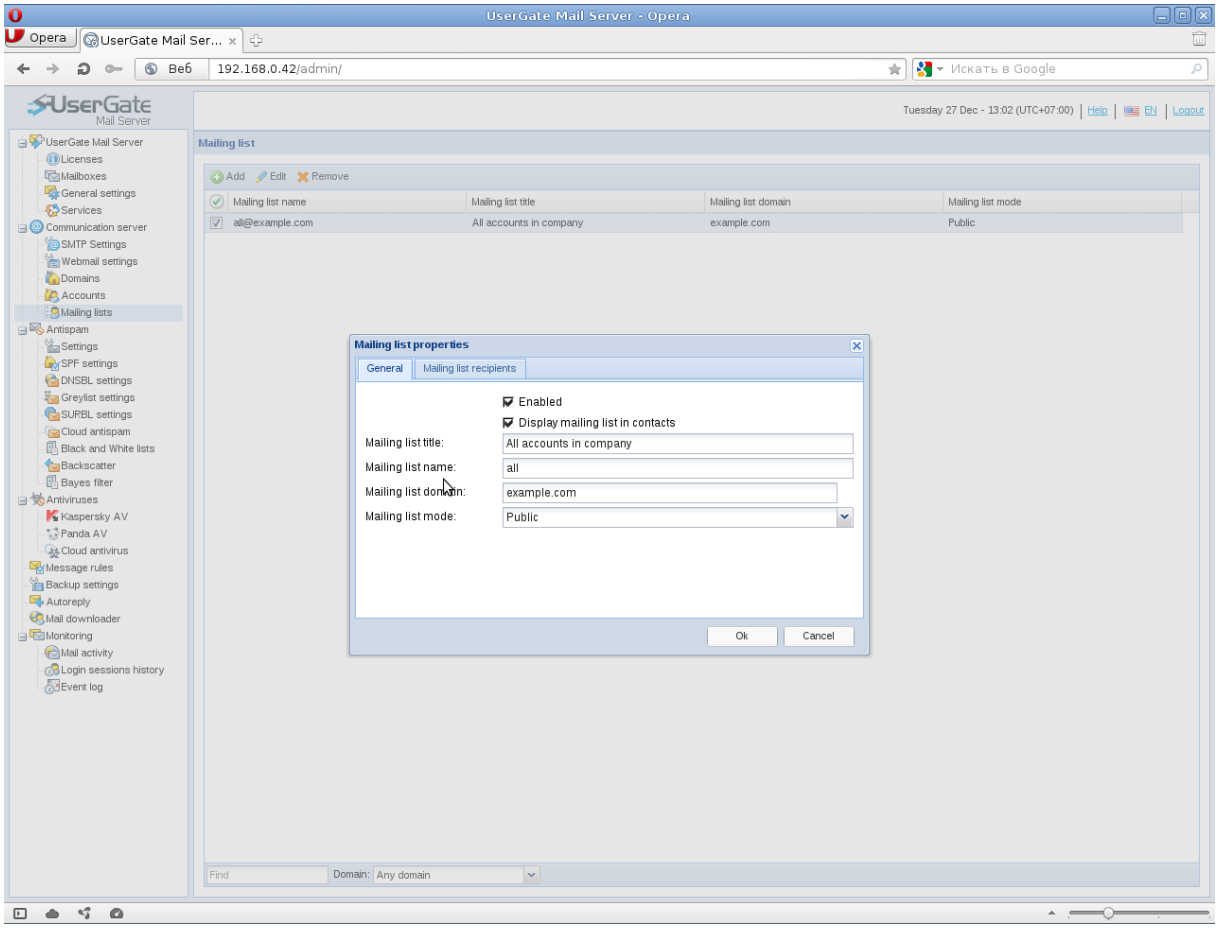
A public distribution list is an e-mail address of a user group within UserGate Mail Server that is accessible for all users, i.e. messages from all senders will be delivered to the public distribution list address.

A subscription is a group address accessible only for the group users (those on the distribution list). Messages from other users will not be delivered.

When creating a distribution list, specify the following parameters:

- Distribution name;
- Mail domain;
- Header (comment);
- Distribution list type (public/subscription);
- Recipients list.

The resulting distribution list address will look as follows: *distribution_name@domain_name*. You may include non-local accounts on the mailing list.



Antispam

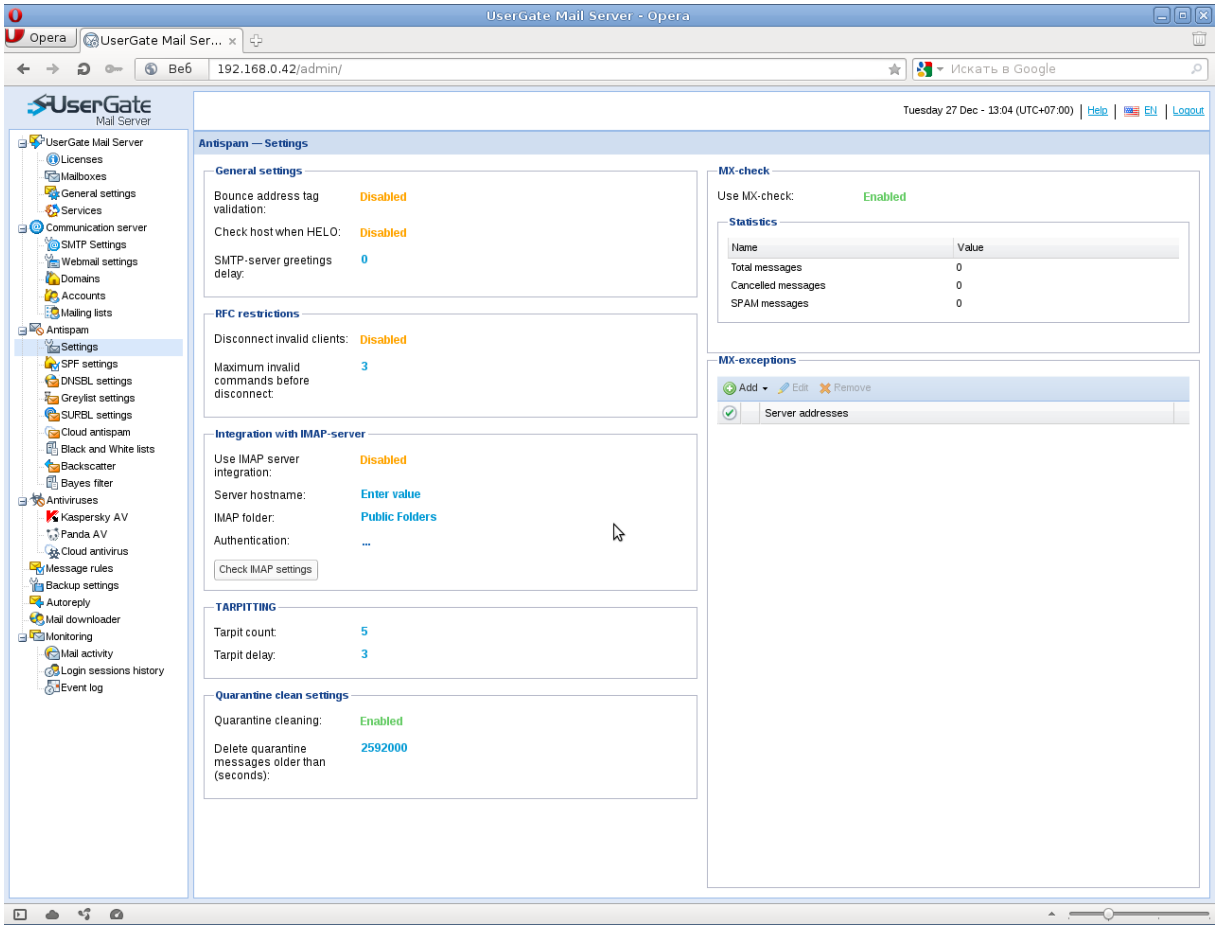
Settings

Key settings include the following general check parameters:

- Use MX check. If enabled, UserGate Mail Server will check for MX record availability on the domain specified in the MAIL FROM command, while receiving e-mails.
- Disconnect invalid clients. Connection with the client sending incorrect SMTP commands will be closed when the number of bad commands exceeds the limit.
- SMTP-server greetings delay.
- Check host when HELO. Verification of host name received in HELO command. Host name should be represented by a domain name.

- Tarpiting. Delay in server response when receiving a new address in RCPT TO command. Tarpiting makes destination address scanning a more time-consuming process.

- "Quarantine Clean settings" allows setting the frequency of erasing mail from the quarantine folder. The default frequency is two weeks.



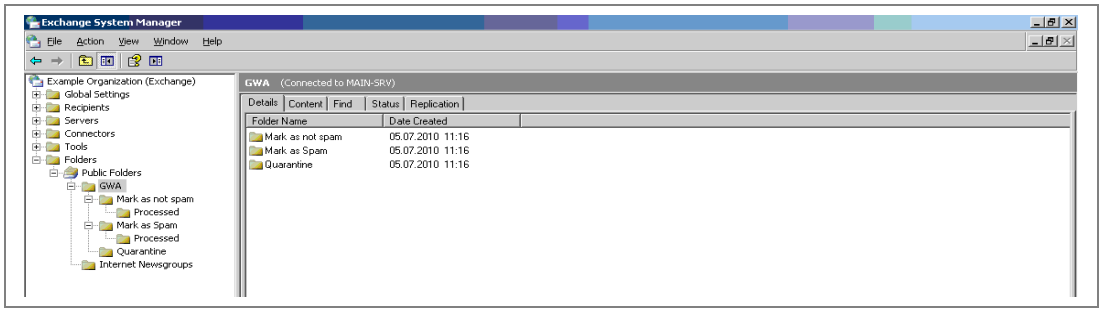
- Integration with IMAP server. Support IMAP integration with MS Exchange 2003 and Lotus Domino R7 servers. IMAP integration is used to receive feedback from the mail server users by way of processing messages in special IMAP folders.

IMAP Synchronization in MS Exchange

Complete the following actions to configure IMAP integration for MS Exchange 2003:

1. Go to "UserGate Mail Server – Settings – Integration with IMAP server". Specify MS Exchange server's IP address, Public Folders prefix and the log-in and password of the user authorized to create and delete folders in Exchange Public Folders. The user must be authorized to work over IMAP protocol.

Click the “Check settings” button. UserGate Mail Server will authorize with MS Exchange server using the specified user account information and create subfolders as shown in the picture below.



When the option is enabled, UserGate Mail Server will connect to the MS Exchange server every 2 seconds and scan folders "GWA/Mark as Spam" and "GWA/Mark as not Spam" for messages. Messages identified as spam will be automatically moved to "GWA/Quarantine" folder.

A mail client synchronized with an IMAP server may subscribe to UserGate Mail Server folders. Users may move messages to “Public Folders\GWA\Mark as Spam”, which will facilitate automatic learning of Cloud Antispam. There is a slight lag in the learning process because Cloud Antispam is an online service. UserGate Mail Server IMAP client places all the processed messages into the “Public Folders\GWA\Mark as Spam\Processed” folder.

Configuring IMAP folder access permissions

By default, all MS Exchange users authorized to work over IMAP can view messages from other users in “Public Folders\GWA” folders. However, you can configure folder access permissions to hide messages posted by other users. Complete the following steps:

1. Open Exchange System Manager console.
2. Select "Properties" in "Public Folders\GWA" shortcut menu.
3. Open “Permissions” tab and press "Client permissions."
4. Press “Add” and add one or more users who will not be authorized to view messages from other users. Select “Contributor” as user role.

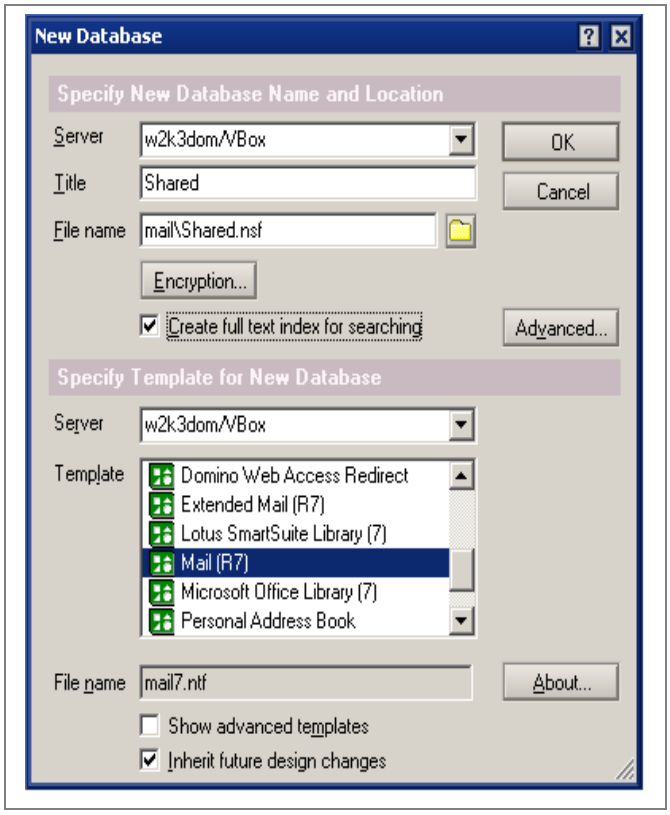
5. Close the properties window, select "Public Folders\GWA" and click on "All tasks - Propagate settings" in the shortcut menu.

NOTE! Users marked as Contributor will only be allowed to view their own messages in “Public Folders\GWA” folders.

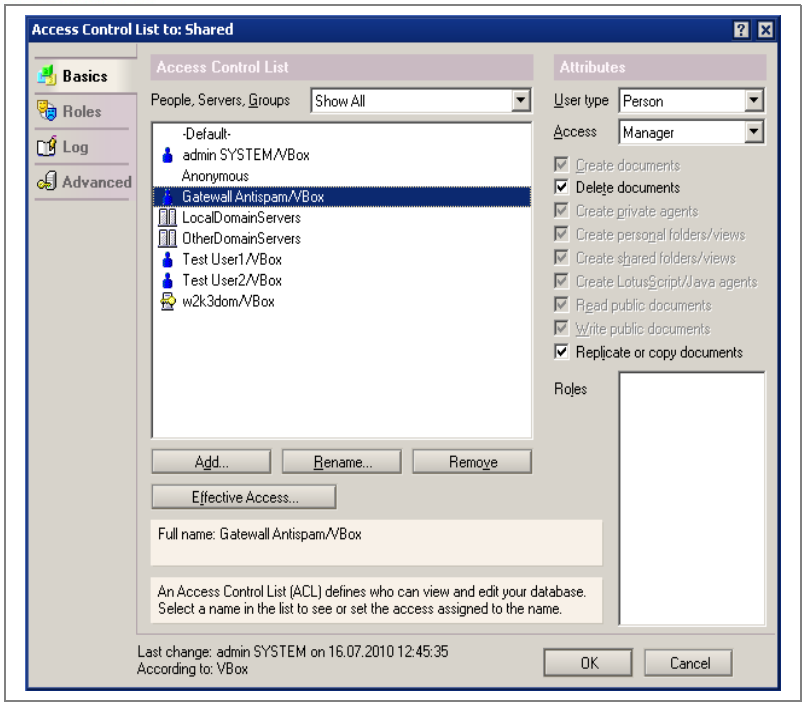
IMAP Synchronization in IBM Lotus Notes

Complete the following actions to configure IMAP synchronization for IBM Lotus Domino:

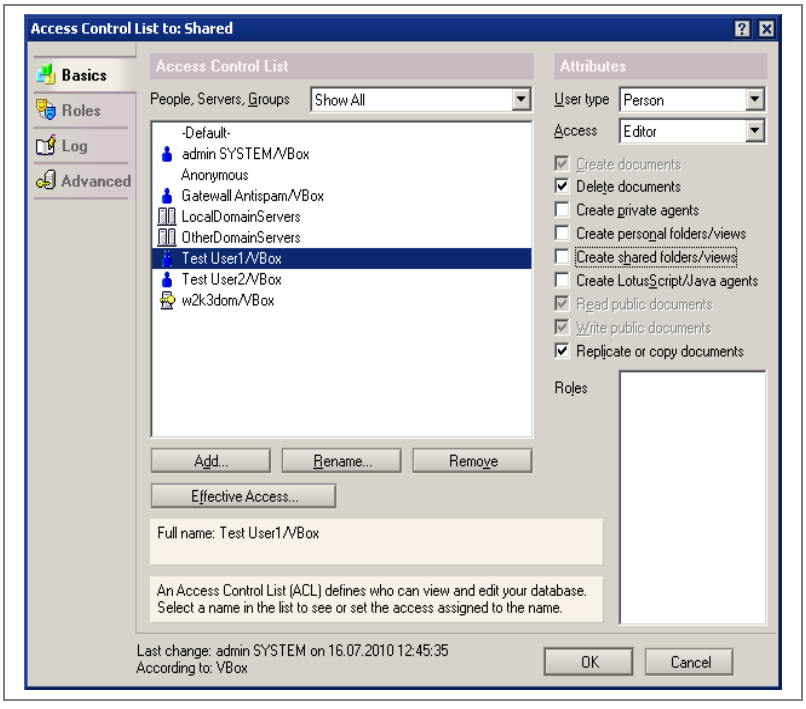
1. Use mail template to create a new Lotus Domino database. The new database will be used as a public IMAP folder. Go to File – Database – New in Lotus Administrator menu and specify parameters as shown in the picture below.



2. Link the new database with a user and assign user rights as shown in the picture below.



3. Assign corresponding rights to users authorized to work with the public IMAP folder.



4. Prepare mail databases for IMAP integration. Open the “Server – Status” tab in Lotus Administrator, select “Server Console” and execute the following commands in the Live mode:

   tell router quit

load convert -e mail.nsf*

load router

5. Enable IMAP Public Folders. Open “Configuration - Messaging – Configurations” in Lotus Administrator. Go to “IMAP - Public and Other Users' Folders” tab, check “Public Folders Prefix” parameter and insert link to the new database from item (1) above to “Public folder database link.”

6. Restart the IMAP service. Execute the following commands in “Server Console;”

   tell imap quit

   load imap

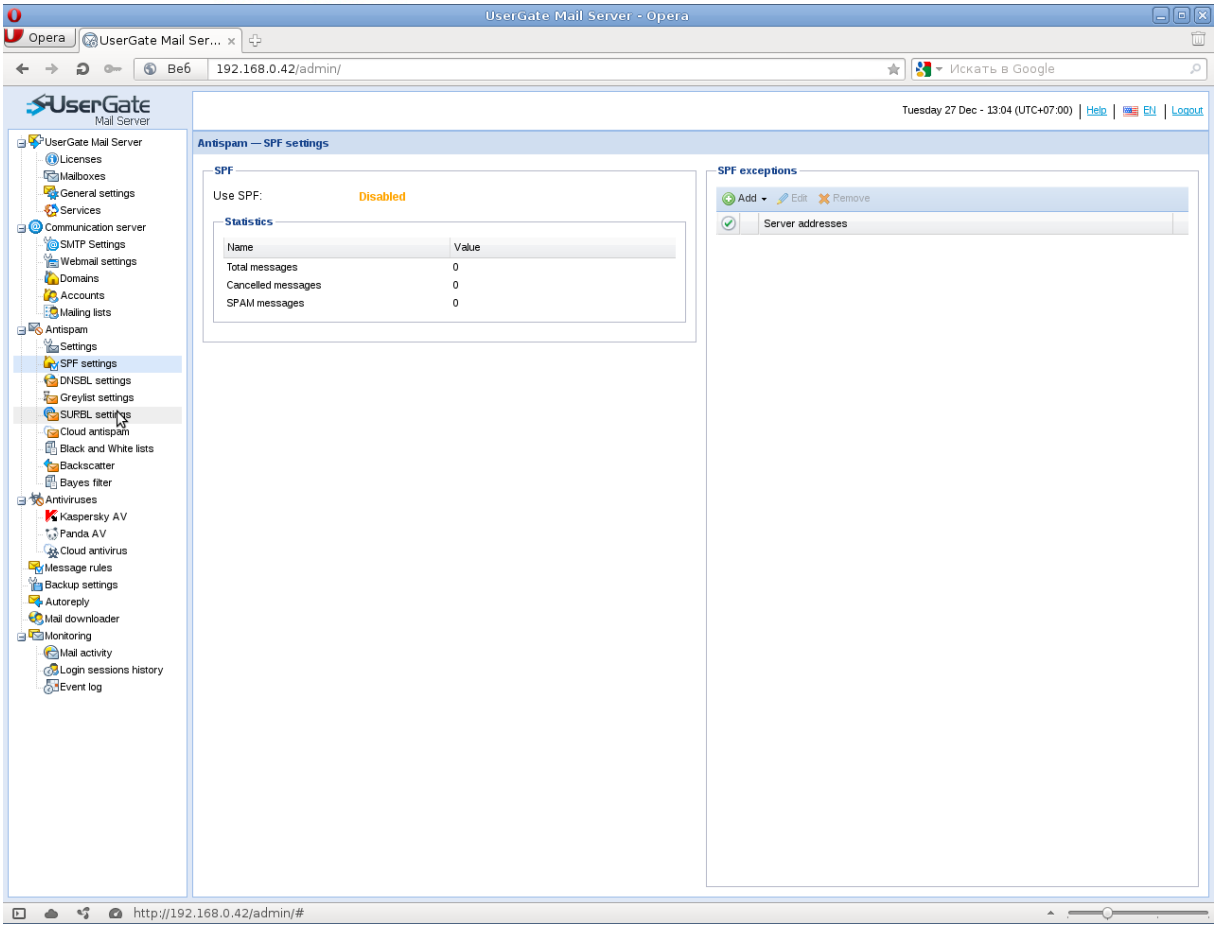
7. IMAP folder has the following full path in Lotus Domino: Public_Folder_Prefix\Public_Folder_Database_name. Specify this path as the “IMAP folder” parameter in UserGate Mail Server settings.

NOTE! Due to certain operating parameters, IMAP integration is not supported by later MS Exchange and Lotus Domino versions.

SPF Settings

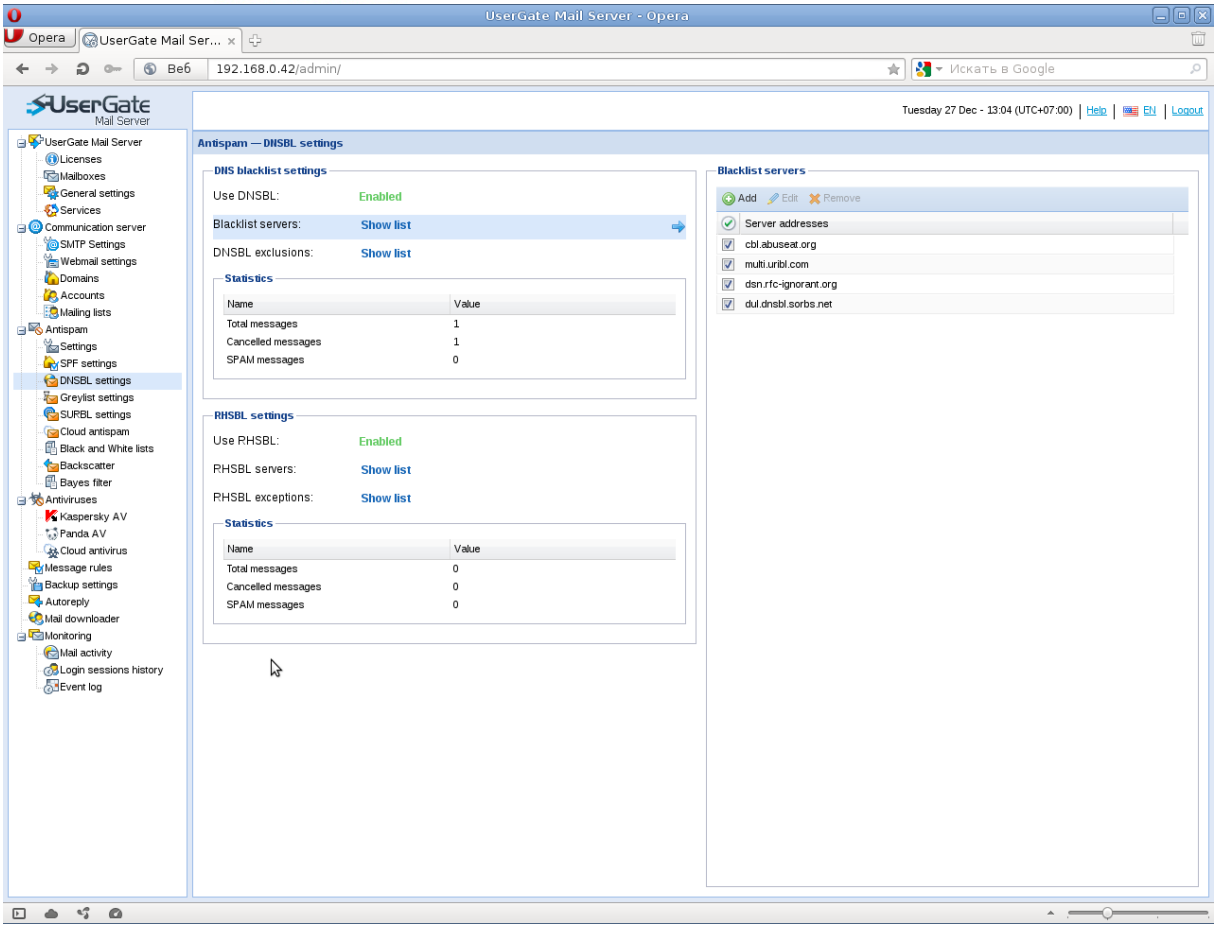
SPF (Sender Policy Framework) is a method used to verify sender’s domain name that is based on special DNS records (TXT type). These records indicate which hosts on the Internet can send messages on behalf of the domain. To set UserGate Mail Server to respond to SPF check results, use the *reject* parameter in the server settings file (%CSE%\settings.xml):

<spfcheck enabled="false" reject="Soft Fail;Hard Fail;Error"/>



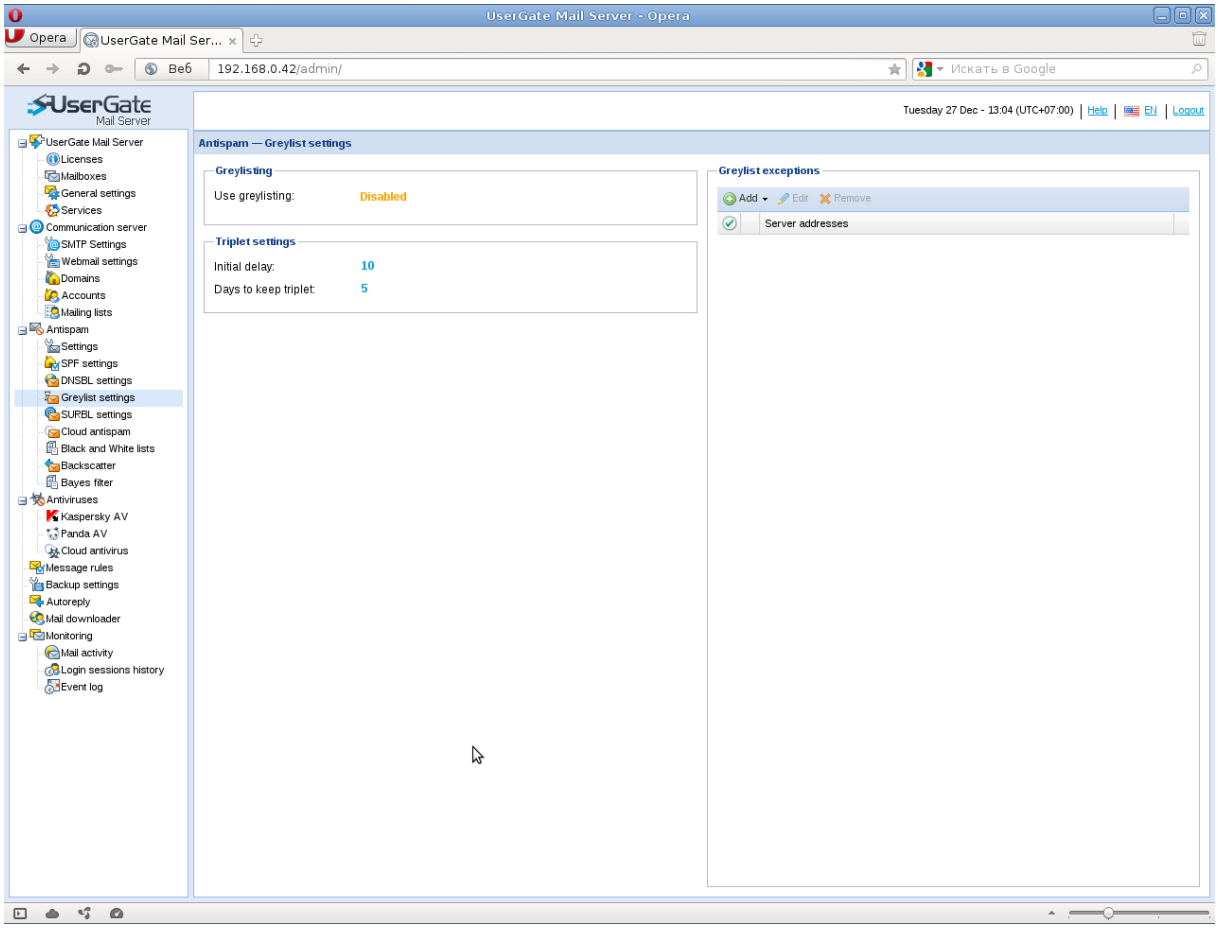
DNSBL Settings

Use DSNBL Settings page to create a list of servers to be used for DNSBL (DNS Black Lists) and RHSBL (Right Hand Side Block Lists) checks. DNSBL check verifies the IP address originating a connection, while RHSBL check verifies the domain name specified in MAIL FROM command.



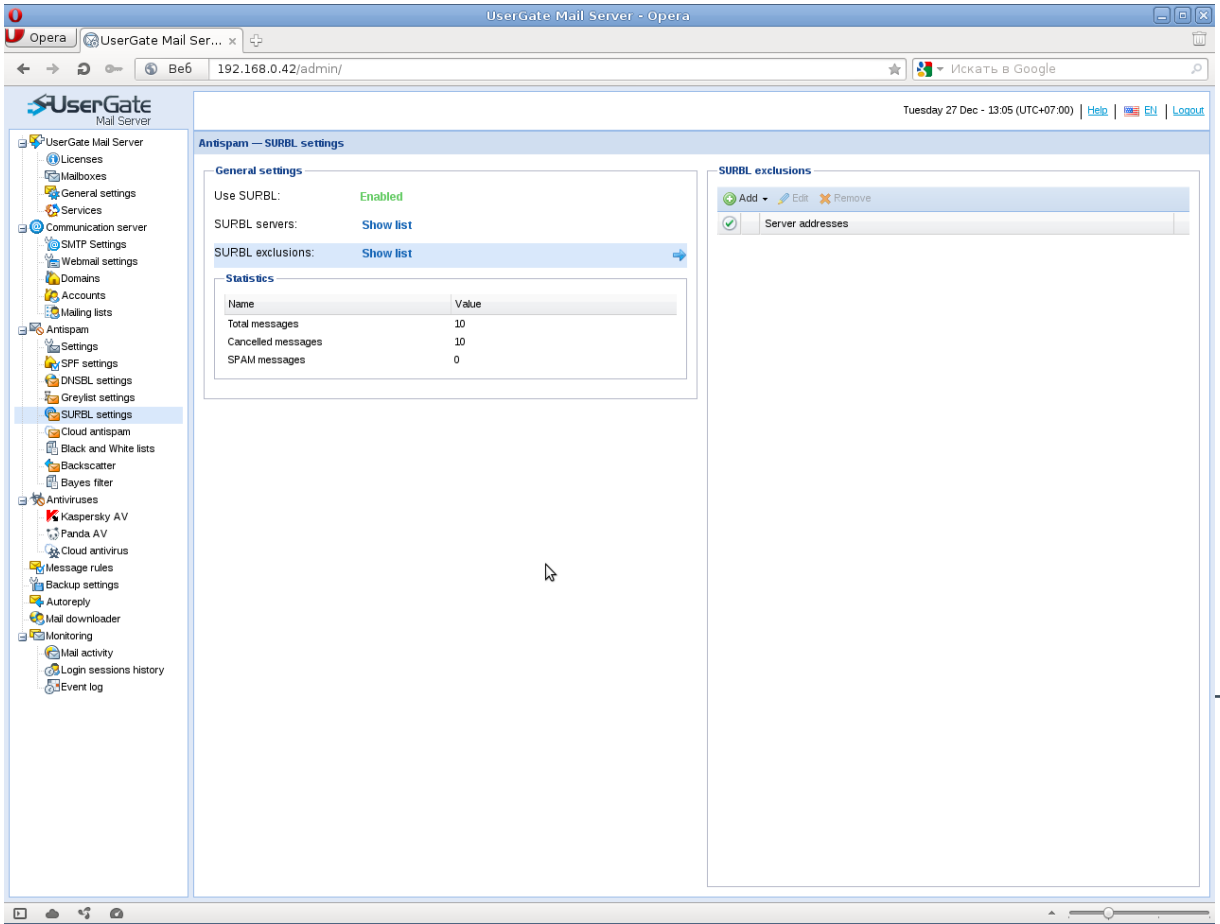
Greylisting

Greylisting is a spam filtering method that consists in blocking the initial attempt to receive a new message. UserGate Mail Server generates a list of triplets including the IP address originating a connection, the address received in MAIL FROM command and the address specified in RCPT TO command. A message is qualified as new mail if its triplet has never been received before. The message is blocked, and a “temporary error” notice is sent. When a sender’s server receives a “temporary error” notice, it is supposed to retry sending the message later. Greylisting settings specify triplet storage time and exceptions lists.



SURBL Settings

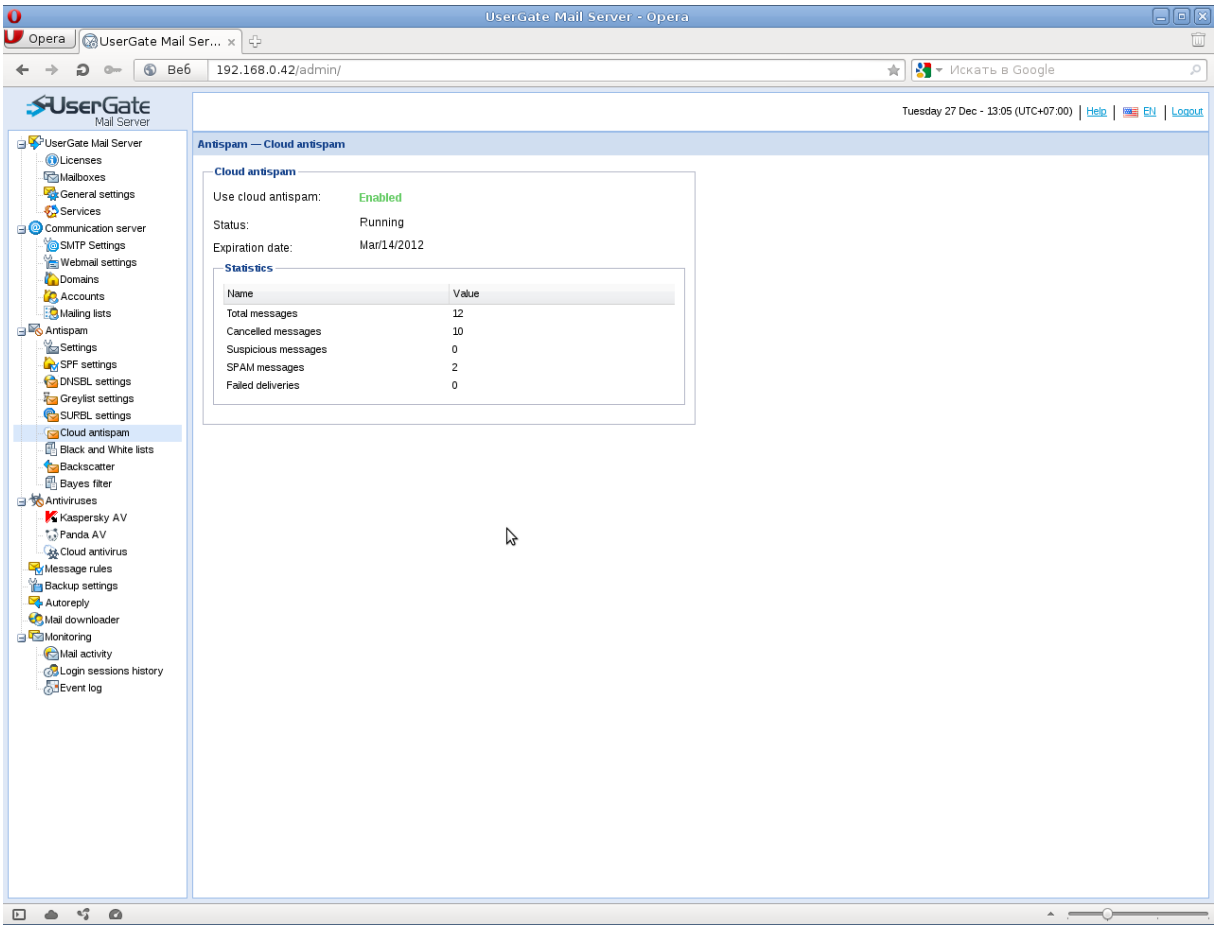
SURBL (Spam URI Block Lists) is a method of filtering spam by checking the message body for spam links. SURBL settings include the list of servers of exceptions lists. Messages that contain spam links will be blocked.



Cloud Antispam

UserGate Mail Server interfaces with the Cloud Antispam online service via HTTP POST requests. Each request to the online server contains a unique message hash computed based on the full message body (including headers). Hash does not contain any information about email content and cannot be used in any way to disclosure any confidential information. A reply from service containing a notification with options as follows: Spam / Not spam / Suspicious / Error, and a decision to block the message is made on the applicable option.

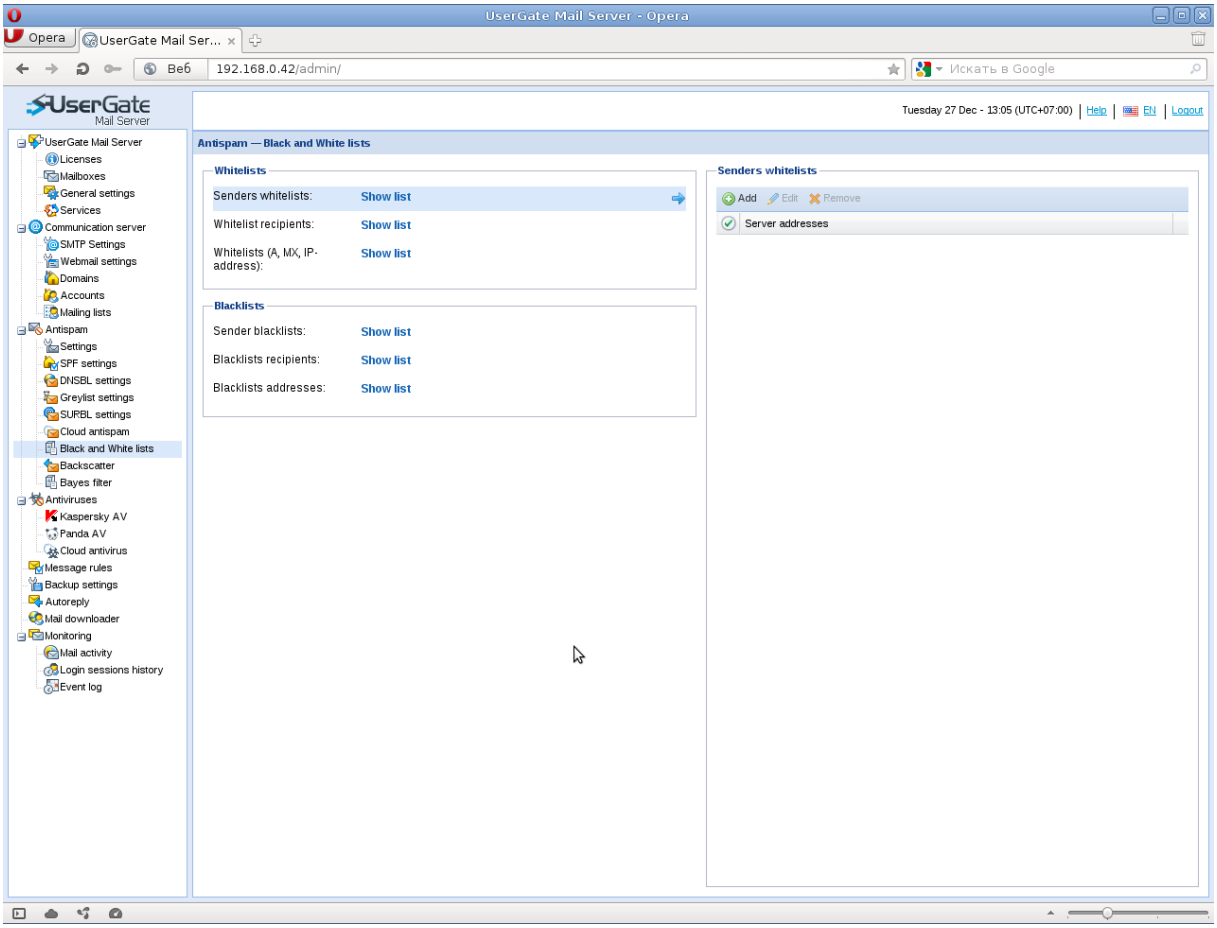
Note that Cloud Antispam offers the best filtering of unwanted mail (minimum 97% efficient), at the same time keeping a low threshold of false spam detection (maximum 1 out of 1,500,000 messages).



Black and White Lists

The page is used to create global lists of allowed and blocked addresses. These lists allow blocking messages at the initial processing stage (black lists) or skip all further checks (white lists). Settings include the following parameters:

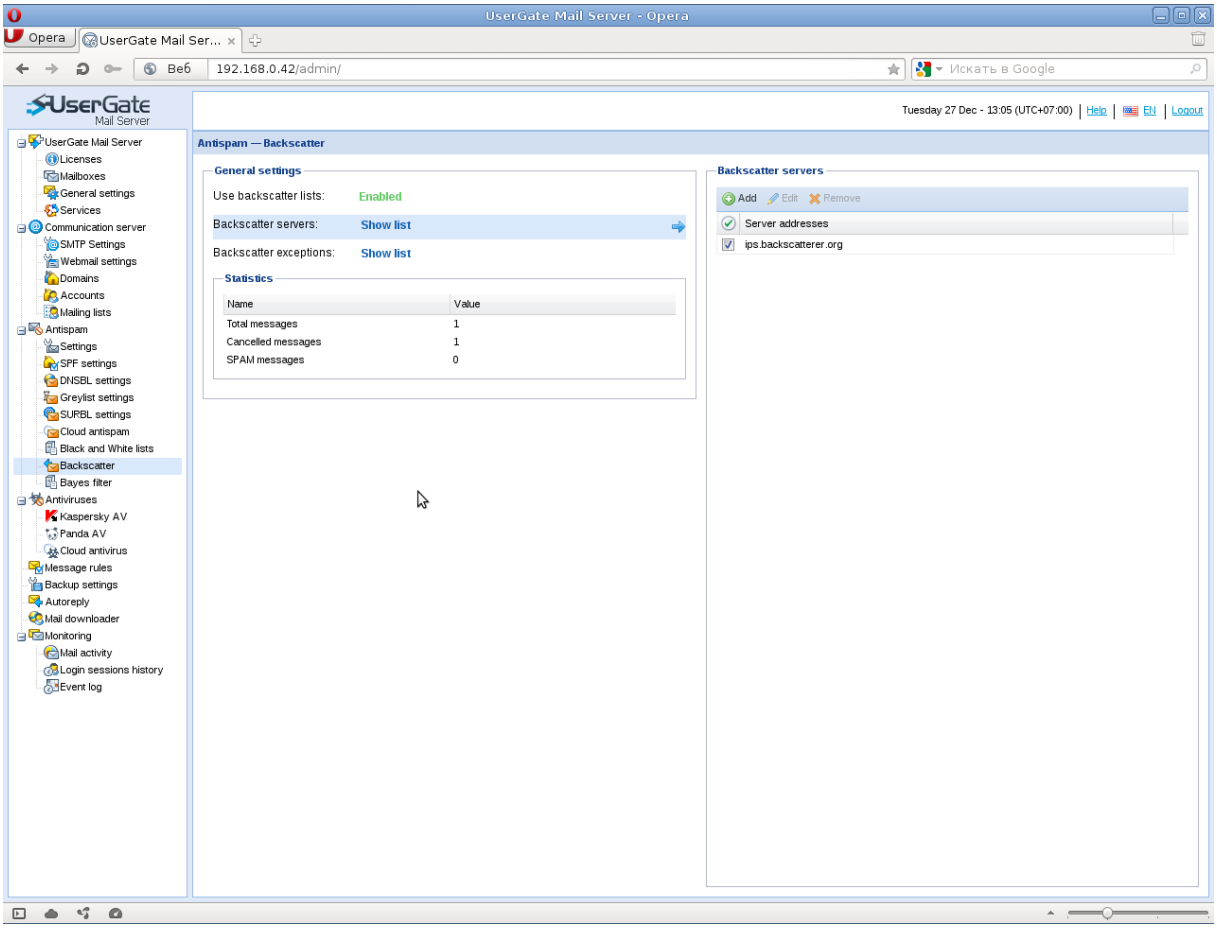
- IP address
- Domain name
- Domain MX record



UserGate Mail Server will resolve any specified parameter to the given IP address.

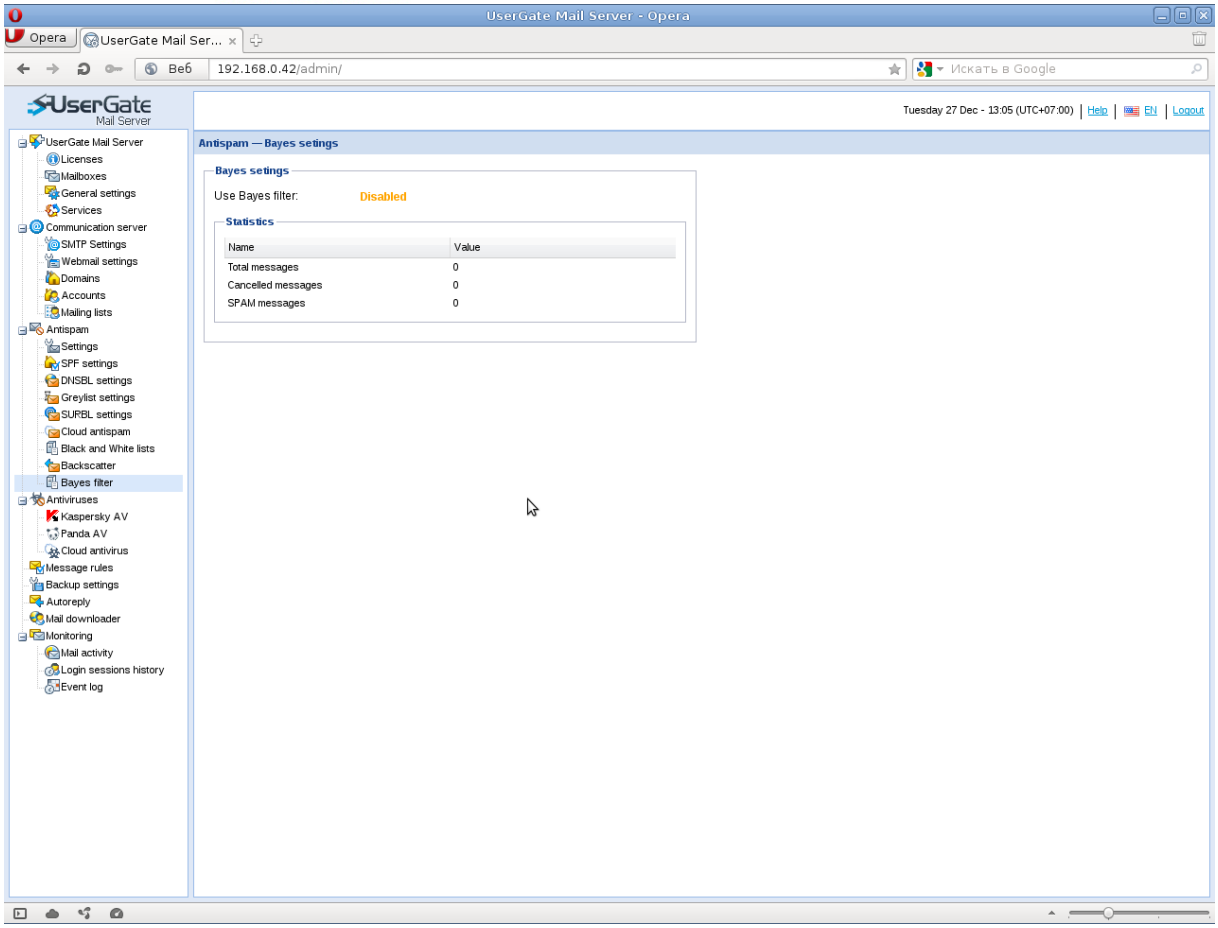
Backscatter

Backscatter filtering method is used to block service messages, e.g. delivery failure messages. For instance, if a spamming system uses your mail domain name to distribute spam messages, remote mail servers may generate a large number of delivery failure messages.



Bayesian Filter

This module filters spam using the statistical message processing algorithm. The filter determines the probability of each message containing spam. If the estimated probability exceeds the set limit, the filter blocks the message. The probability is estimated based on the recorded statistics of clean and spam messages. Entensys' own design of the Bayesian algorithm allows the filtering module to learn from the Cloud Antispam results, the administrator's actions (marking a message as "not spam" on the Monitoring page) or users' actions provided IMAP integration is enabled.

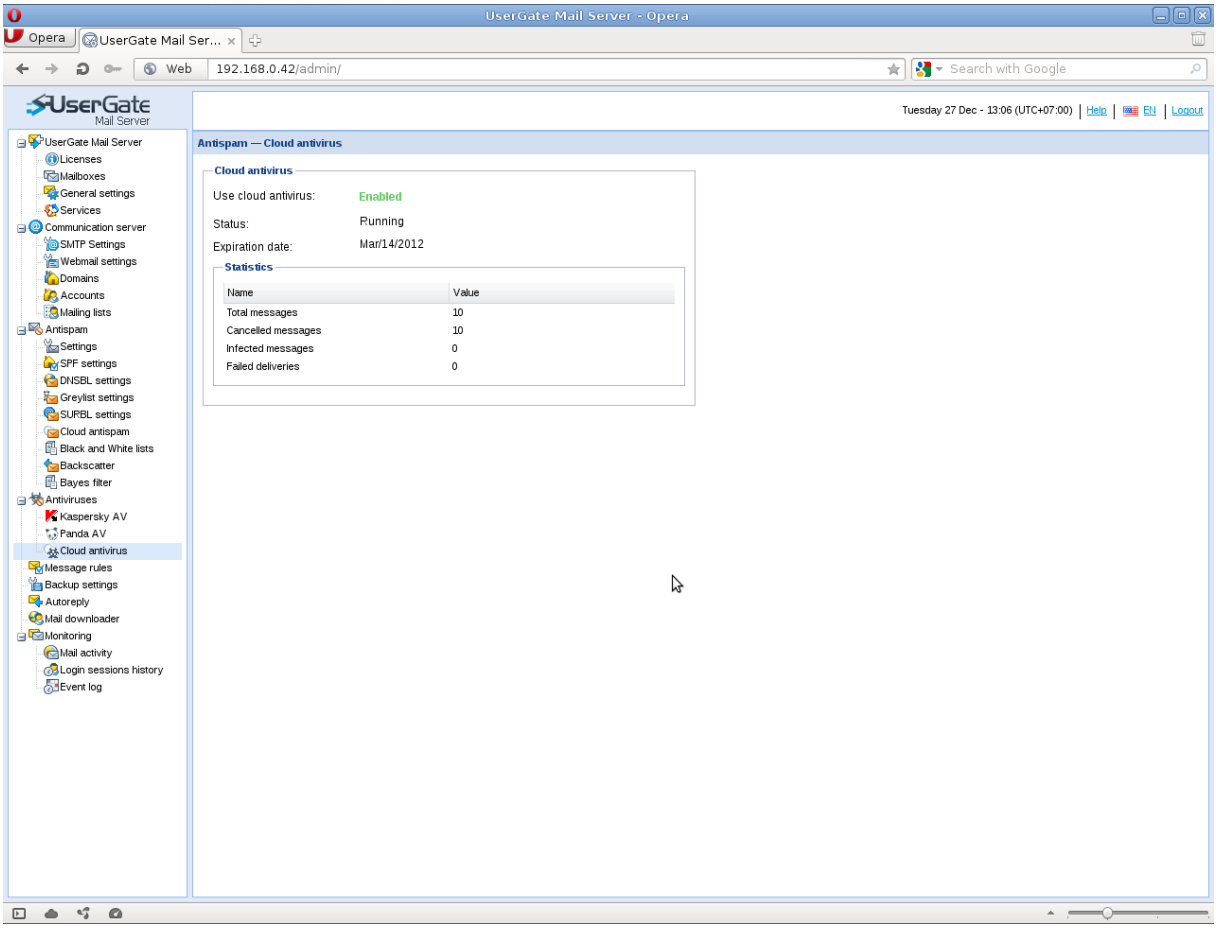


Antiviruses

UserGate Mail Server features three integrated antivirus modules from Kaspersky Lab, Panda Security and Cloud Antivirus. All of these modules are used to scan mail traffic for viruses. You can configure the modules on the corresponding page of the administrator console.

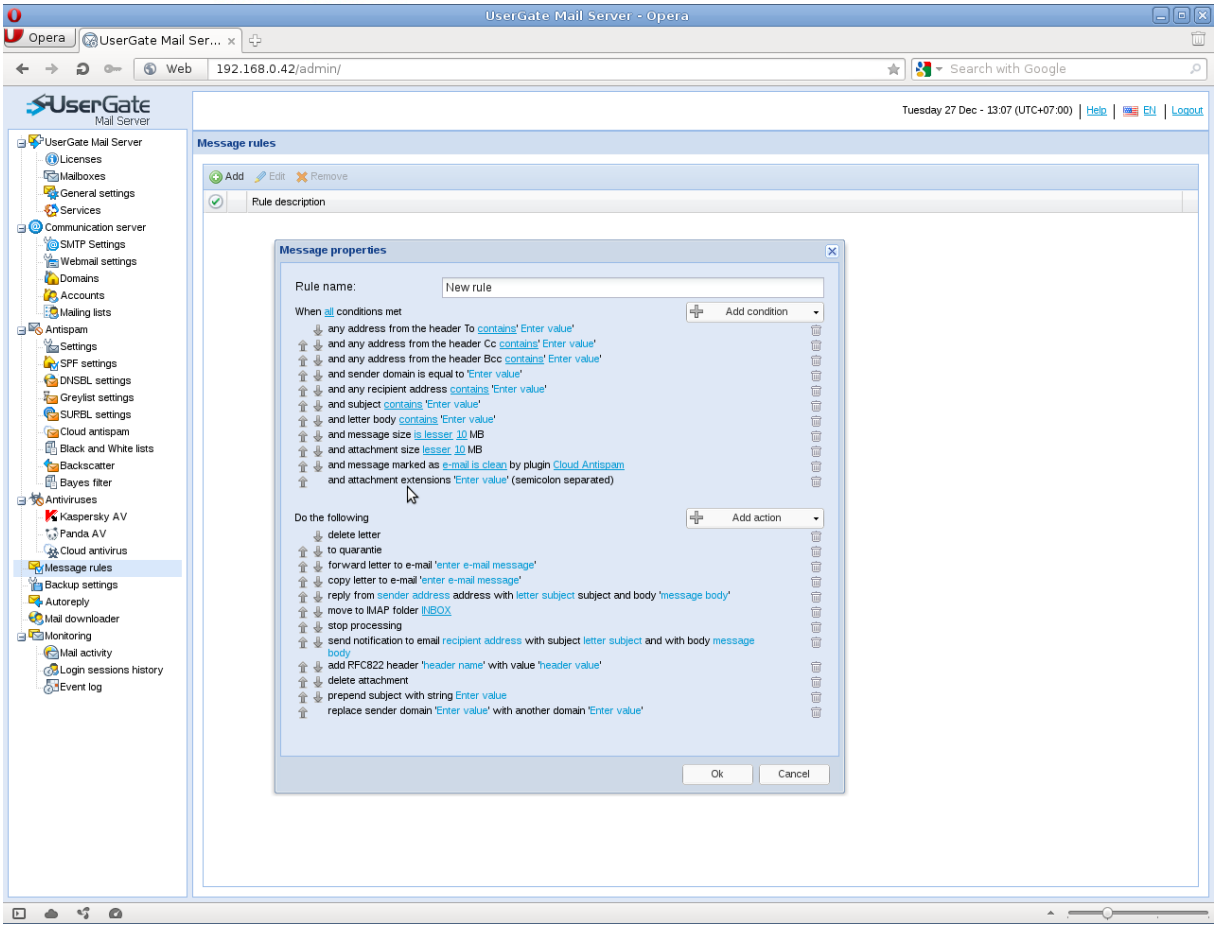
Prior to enabling an antivirus module, launch virus definition update and wait for the update process to complete. The antivirus page indicates if your virus definitions are up to date. You can also use this page to schedule virus definition updates.

Cloud-based antivirus checks messages and attachments for viruses similar to the cloud-based antispam – it sends to the server a unique message hash and matches it against the known virus signatures. For this reason, the antivirus requires no updates and starts running immediately when launched. Besides, such virus check minimizes mail server's processing capabilities.



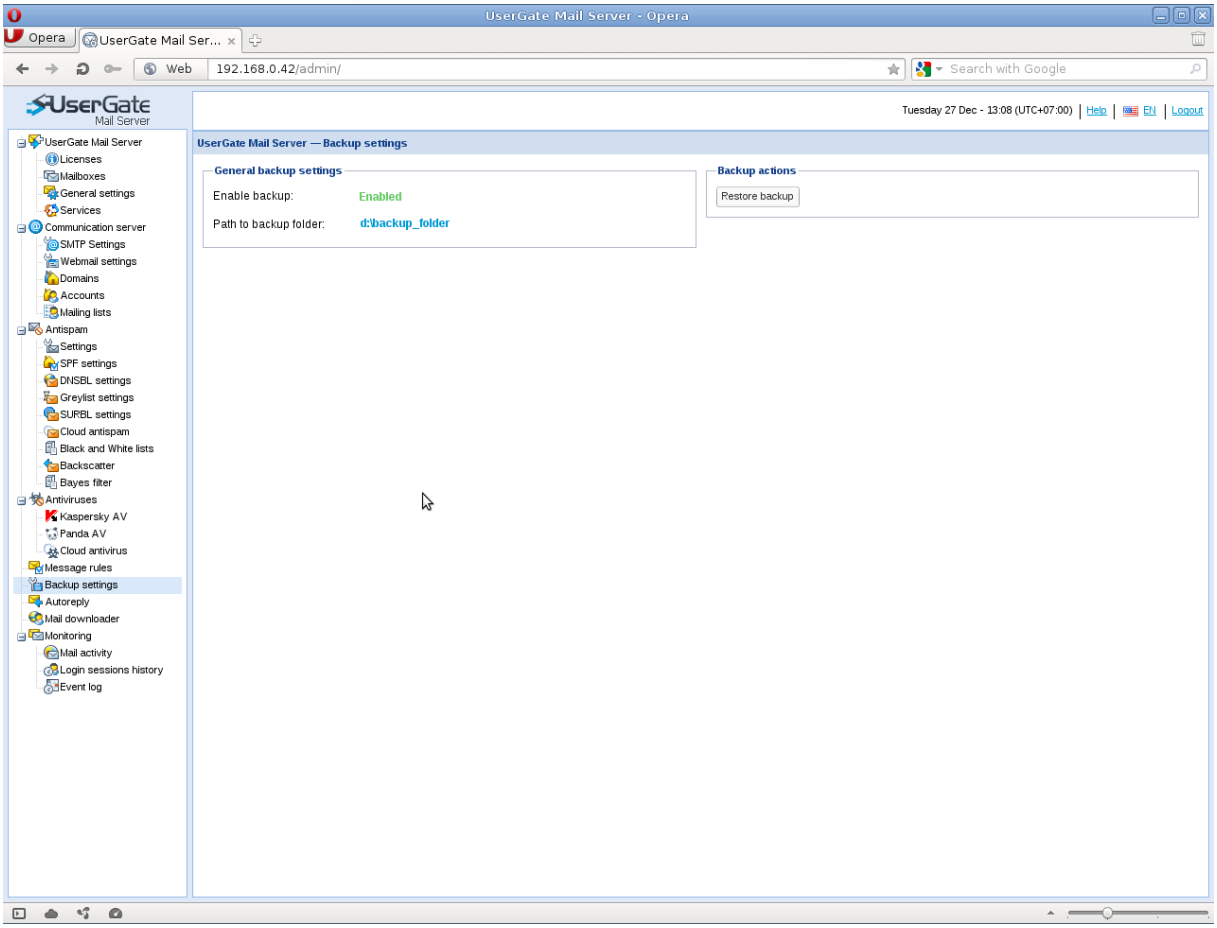
Message Processing Rules

UserGate Mail Server features message processing rules. A rule generally contains one or more conditions with the AND/OR logic and actions that will be applied to a message if the conditions are met. Rules are processed top-down in the list. UserGate Mail Server scans the entire list of rules for each message. It also supports non-sequential processing through applying two actions: “Cancel processing” and “Redirect action to rule.” The first action ignores all subsequent rules and the second allows switching directly to a specified rule. Redirection is only allowed to rules located below in the list.



Backup settings

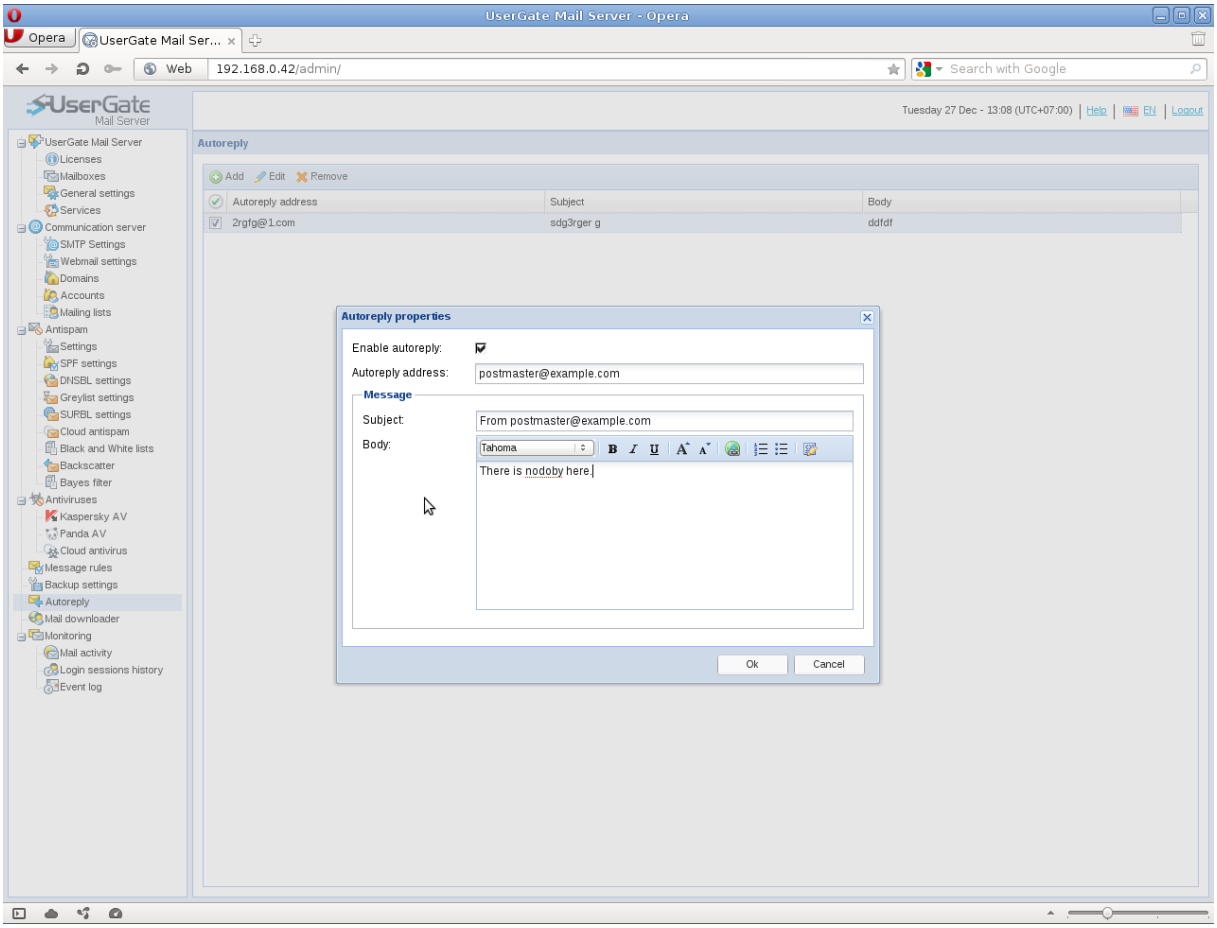
With UserGate Mail Server, you may back up all messages stored in the “%CSE %\mail” folder. Message copies are backed up in a folder specified on the mail backup page. This folder is not set by default, so you will need to specify the folder (e.g. “d:\mail_backup”) and enable mail backup feature. In the backup settings, you can specify the backup address and restore a backup copy of a message. By default, all messages are backed up into the specified backup folder every 15 minutes. The backup process is run by a special utility (CSESync). Only new messages are added to the backup copy.



NOTE! Current UserGate Mail Server version features no components to view the mail backup file. Messages are copied into files in the specified backup folder having the structure equivalent to the initial folder “%CSE%\mail”.

Autoreply

When the Autoreply function is enabled, UserGate Mail Server will automatically generate a reply to messages sent to the specified address. Specify the destination address, subject and the message in the Autoreply settings (“Autoreply” page). Autoreplies will be generated at the Content Filtering stage.



Mail downloaders

UserGate Mail Server can download e-mail from any external POP3 or IMAP accounts and distributd to users' mailboxes. Two methods of collecting mail are supported:

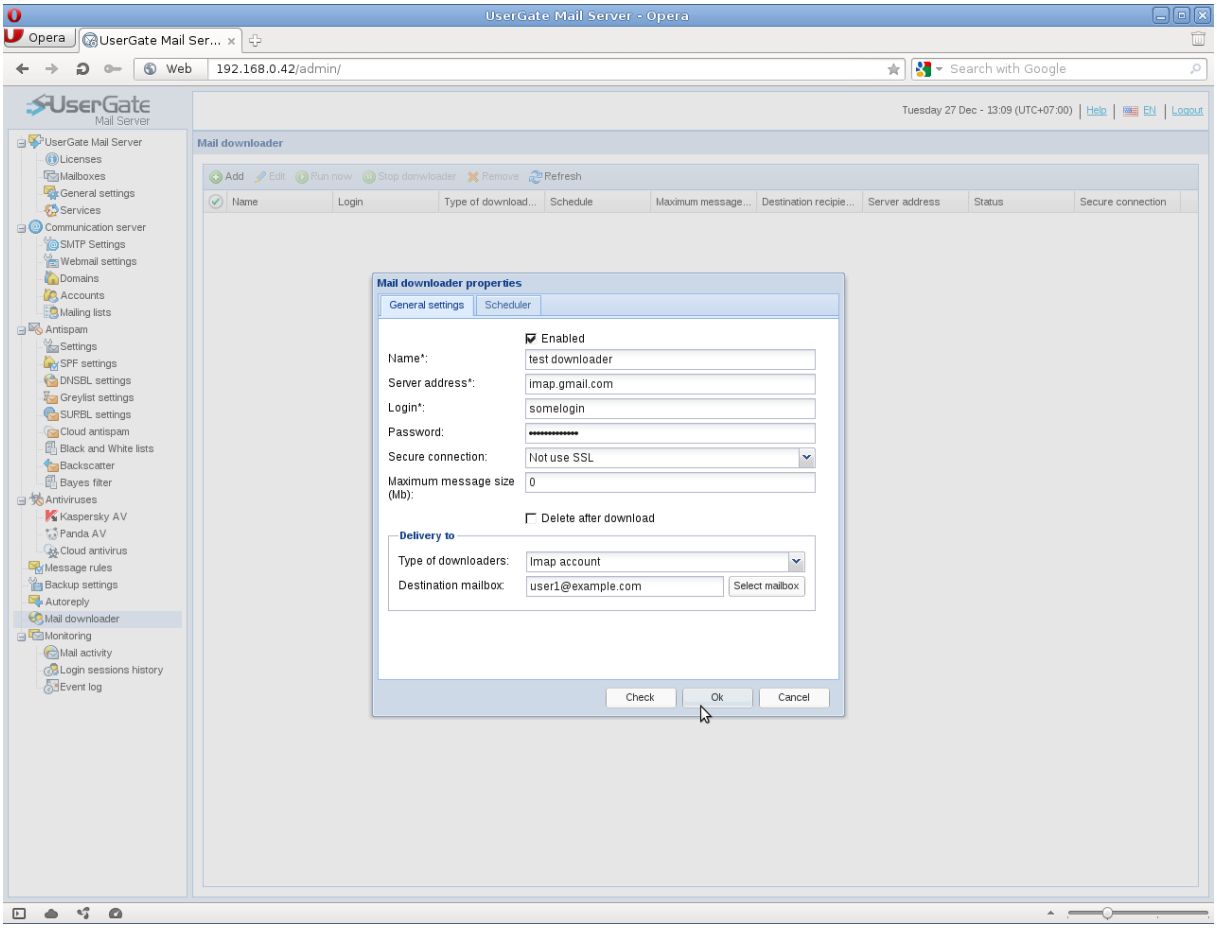
- Collecting from mailbox utilized for one user.
- Collecting mail from one mailbox to many users, the "multiboxes."

In the first case, one POP3 account corresponds to one user located in the list of addresses serviced by Mail Server. In the second case, correspondence is set based headers «X-Delivered-To», «to» or other field, between the mailbox and the users in addresses that are serviced by UserGate Mail Server.

Secure connections (POP3S, IMAPS) are also supported.

It is possible to verify downloading by clicking on the “Check button”. In the event of successful / unsuccessful connection on the server, you will receive an appropriate message. You can set up a schedule for the mail downloader using the extra tab, or

force mail downloader to execute mail check immediately.



Monitoring

Mail activity

Mail activity page shows status details for all messages that have been processed by the server and that are still on the server.

The page features an easy search filter:

- by any portion of message;
- by sender address;
- by recipient address;
- by message subject;
- by message status.

The above listing of search filter parameters needs no explanation, with the exception of the last item – “by message status.” Mail server supports search by internal status of messages that can be easily filtered, for instance, to show only

messages qualified as spam or display a sequence of messages. To apply such filter, you will need to enter a special variable parameter in the search box. For example, to search for all quarantined messages, enter the following parameter in the filter box:

status:quarantine

To find all messages in the outgoing queue, enter:

dm:pending

Below is a full list of variable parameters:

all:clean — search messages for which all plugin statuses are clean

each:clean — = all:clean all plugins report that the message is clean

any:clean — search messages for which at least one plugin status is clean

plugin:clean — = all:clean

plugin:infected — = any:infected

plugin:suspicious — = any:suspicious

plugin:spam — = any:spam

cloudantispam:suspicious — search messages that CloudAntispam regards as suspicious

cloudantispam:clean — search messages that passed through CloudAntispam

cloudantispam:infected — search messages marked by CloudAntispam as infected

cloudantispam:spam — search messages marked by CloudAntispam as spam

surbl:clean — search messages that passed SURBL check

surbl:spam — search messages blocked by SURBL

antivirus:infected — search messages in which at least one antivirus plugin found viruses

antivirus:suspicious — search messages which at least one antivirus plugin found suspicious

antivirus:clean — search messages in which neither antivirus plugin found viruses

kav:infected — search messages in which KAV found viruses

kav:suspicious — search messages which KAV found suspicious

kav:clean — search messages in which KAV found no viruses

panda:infected — search messages in which Panda found viruses

panda:clean — search messages in which Panda found no viruses

dm:pending — search messages that are pending delivery

dm:success — search successfully delivered messages

dm:expanded — search messages that were partially delivered (delivered to only some of the listed recipients)

dm:failed — search messages whose delivery failed (not completed, completed with 5XX errors)

status:quarantine — search only quarantined messages

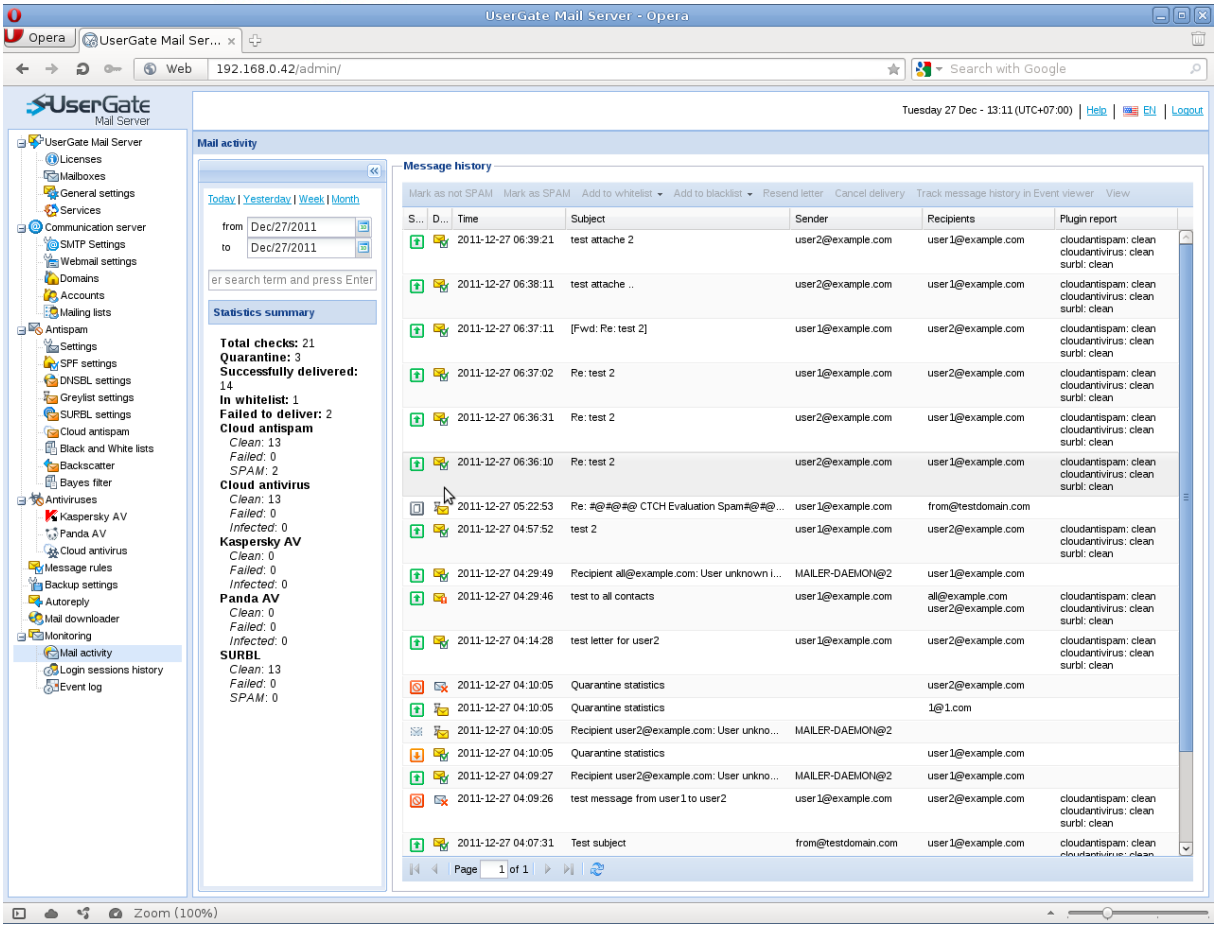
status:whitelisted — search whitelisted messages

status:failed — search messages blocked by filters

status:success — search messages that successfully passed all filters

status:received — search messages that were received via SMTP but have not been processed yet

You may also apply filter by message status by double-clicking on the applicable icon in the “message status” column.



Graphic representation of message status

For easy use of the status page, the application features graphic message status indications. There are also pop-up prompts containing more details on message status.

Description of icons:

- message successfully delivered to recipient.
- message successfully delivered and time of last delivery attempt.
- message delivered because whitelisted.
- message delivery failed.
- message pending delivery, in the delivery queue.
- message blocked by message rules.
- message delivered by server but not processed yet, pending processing.
- message not delivered; the reason of delivery failure will pop up if you point with the cursor on the icon.

Control buttons

Message control buttons are located at the top of the page. You may use these buttons to:

- Mark a message as “Not spam” (if it was marked as spam by mistake);
- Mark a message as “Spam”;
- Place a recipient or domain to the Whitelist;
- Place a recipient or domain to the Blacklist;
- Resend message to the recipient;
- Cancel message delivery;
- Find message route details by tracking the delivery process in the “Event Log”;
- View a message.

You may also right-click on a message to do the above actions.

When viewing a message, you can also apply a number of other actions that may be useful for message delivery processing:

- Remove from quarantine and close;
- Mark as spam and close;
- Resend and close.

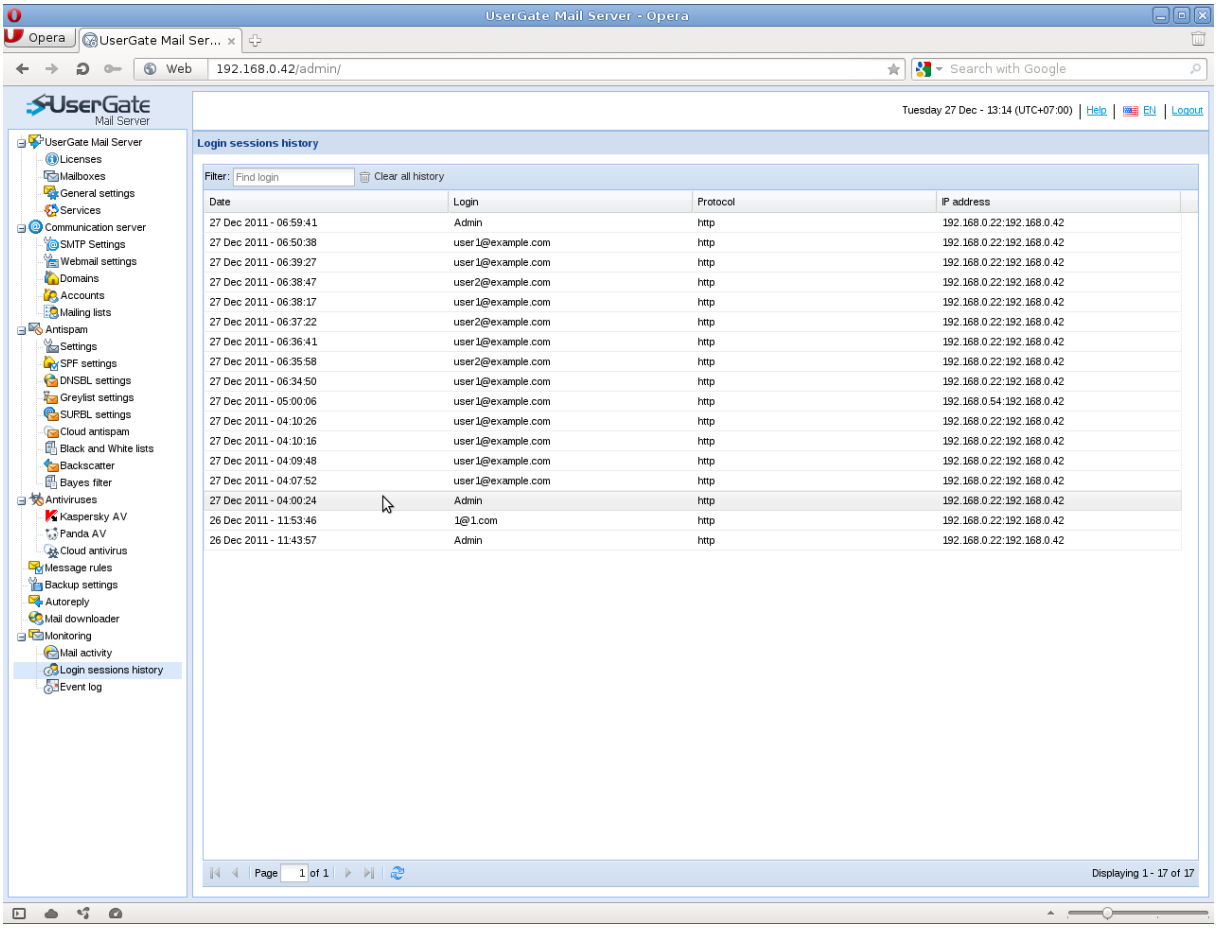
The first action will mark the message as “not spam”, if it was previously marked as spam, send the message to the recipient and close the message window.

The second action will mark the message as spam and close the message window.

The third action will resend the delivered message and close the message window.

Login session history

Login sessions history page can be used to browse the history of log-ins to UserGate Mail Server Administrator Console and web mail. The page logs the login, authorization date, and IP address



Event Log

On the Event Log page, you can track the life cycle (receipt – processing – delivery) of messages received by the mail server, as well as monitor performance of server modules. You can filter messages by one or more of the following criteria:

- Time;
- Field: From, To, Subject, Status;
- Service;
- Type;
- Random field;
- By message ID.

NOTE! You can enable logging for some or all server modules as may be necessary. To enable logging for a certain module, complete the steps below:

- Create an empty log named "log.module_name.enable" in %CSE% folder.

For example, if you want to create a log for SMTP client, create file

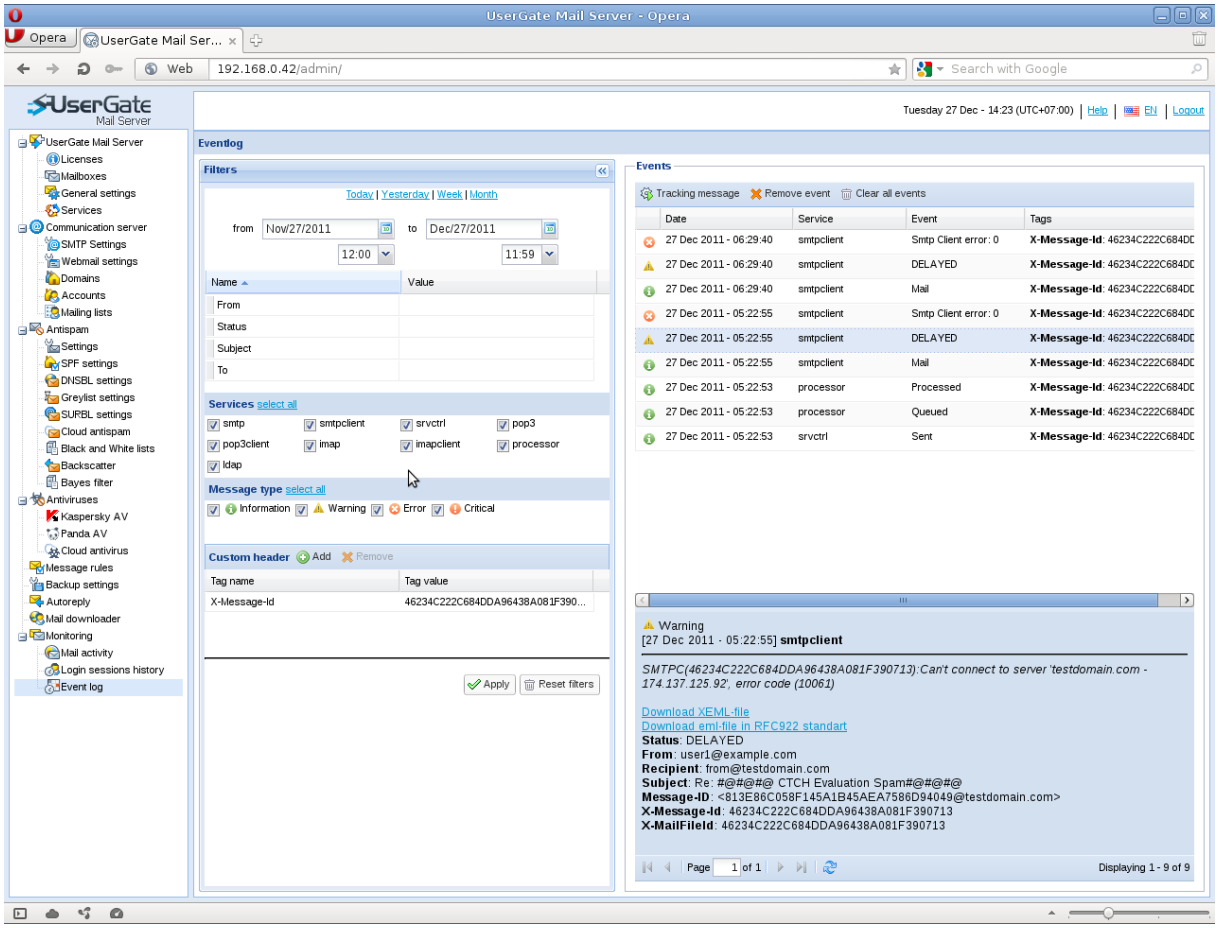
"log.csesmtpc.enable" in %CSE% folder. To enable logging for all server modules, create file "log.all.enable".

- Restart server by selecting "Restart all" in the agent`s system tray menu.

To track route of a certain message:

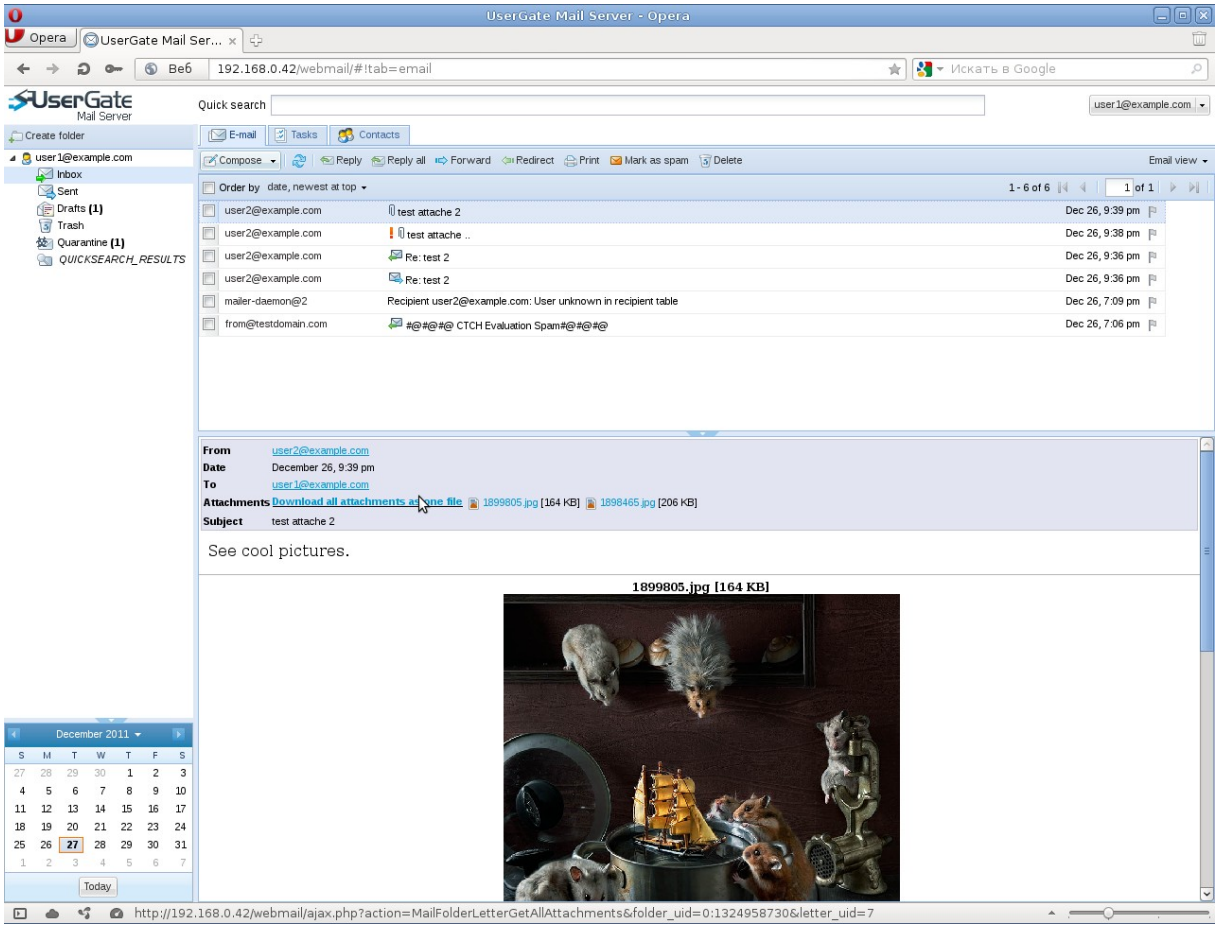
- Select corresponding time period.
- Create filter by completing at least one of the fields: "From", "To", "Subject".
- Apply filter by pressing "Apply" button in the bottom of the page.
- Select one of the messages in the right window and press "Track message" in the pop-up menu.

Message events are tracked by a unique MIME header (X-Message-Id) tagged to each message received by mail server. You can also filter messages by random message fields.



UserGate Mail Server Web Client

Users may access UserGate Mail Server through the web interface (web client). To access the web client, go to http://IP_server/webmail, where **IP_server** is the IP address of the computer with installed UserGate Mail Server.



NOTE! UserGate Mail Server web client works in the following web browsers: Internet Explorer 7/8, Mozilla Firefox, Opera and Chrome.

Web client users have access to the following settings:

- Interface language;
- Delegation;
- Personal information;
- Message display parameters;
- Aliases;
- Message rules.

Through the Delegation settings, a user can grant other users access to their own mailbox through UserGate Mail Server web client.

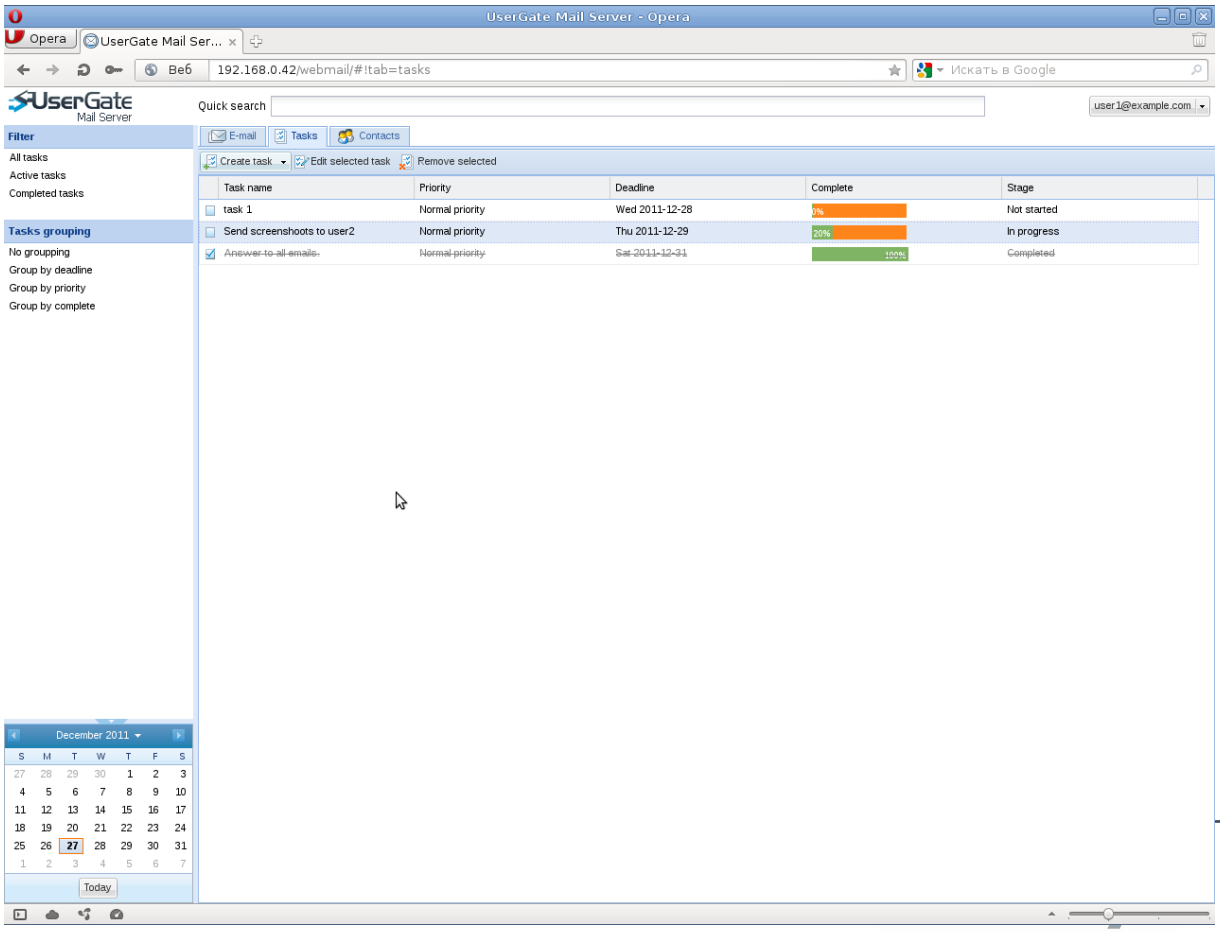
NOTE! Editing of personal information for accounts imported from Active Directory is not supported. Such personal information is stored in Active Directory.

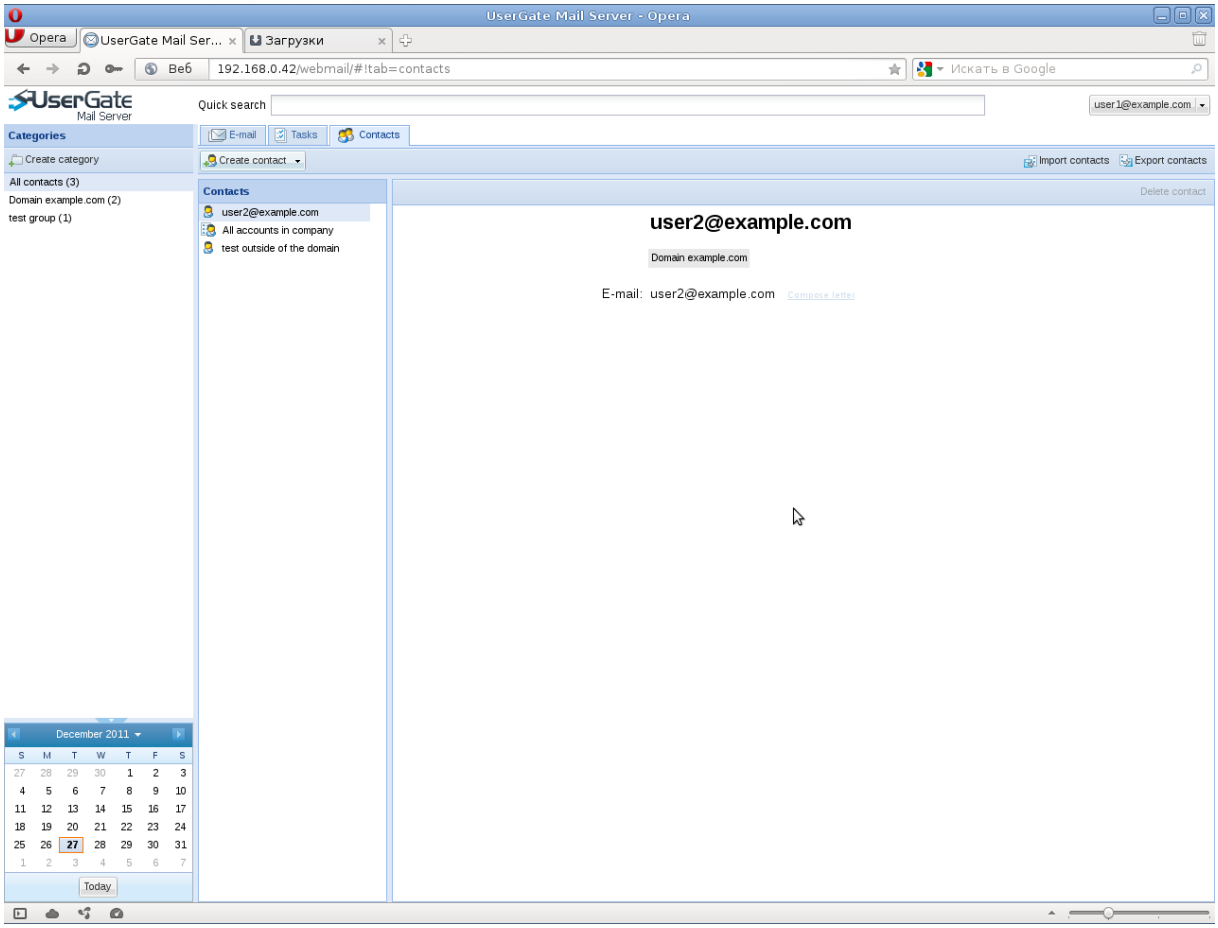
Users can create mail folders and message processing rules for a more convenient mail processing. You may create, delete or rename a folder from a pop-up menu of a folder tree displayed on the right side of the window.

Custom message processing rules can be created in the corresponding section of the Settings menu.

In addition to mail processing capabilities (create/edit/delete), the web client features an integrated task scheduler and contacts browsing and editing tool. Contacts can also be grouped into categories.

UserGate Mail Server web client features a full-text search of messages in all folders. Search results are placed in the “SEARCH RESULTS” folder, where results of the latest search requests can be easily stored and viewed.





Getting support

Additional information and support for Entensys software products are available at http://www.usergate.ru/support.