

UserGate Mail Server 1.x

Руководство администратора

Содержание

Введение	3
Системные требования.....	3
Установка	3
Обновление и удаление	4
Быстрая настройка	4
Настройка соединений.....	4
Установка пароля на подключение.....	5
Установка пароля на доступ к базе статистики UserGate.....	6
Настройки сервера	6
Сервисы.....	8
Домены	9
Маршруты.....	12
Свойства Web-почты.....	13
Настройка доступа к серверу.....	14
Настройка резервного копирования в UserGate Mail Server.....	15
Время старта системы резервного копирования.....	15
Восстановление состояния UserGate Mail Server из резервной копии	16
Сервер SMTP.....	17
Домены	19
Настройки домена.....	22
Удаленные аккаунты	24
Списки рассылки.....	25
Правила для сообщений.....	26
Антивирусы	28
Антиспам	29
Очередь сообщений.....	31
История сообщений.....	31
Журнал сервера.....	32

Введение

UserGate Mail Server – это полнофункциональный почтовый сервер с поддержкой протоколов: POP3, IMAP4, SMTP, HTTP, HTTPS, SSL. В числе основных функций UserGate Mail Server – поддержка локальных и удаленных аккаунтов, работа со списками рассылок, возможность синхронизации со службой каталогов LDAP, Webmail, встроенные антивирусные и антиспам модули, а также мощная и гибкая система правил. Для обеспечения безопасности почтовых сообщений в UserGate Mail Server интегрированы два антивирусных модуля от Kaspersky Lab и Panda Security. Оба антивируса предназначены для проверки почтового трафика и могут быть использованы как отдельно, так и совместно, проверяя сообщения последовательно.

Антиспам защита в UserGate Mail Server, помимо стандартных методов фильтрации (черные/белые списки) обеспечивается двумя полнофункциональными модулями от Commtouch и SpamAssassin. Пакет компании Commtouch использует уникальный фильтр, основанный на фирменном алгоритме RPD (Recurrent-Pattern Detection), идентифицирующем спам по его основному признаку — по распространенности. В отличие от других производителей антиспам - фильтров компания Commtouch не обновляет базу данных (БД) типовых определений фильтров контента, ее продукт отыскивает паттерны в почтовом трафике.

Антиспам модуль SpamAssassin - это расширяемый почтовый фильтр, используемый для идентификации спама. Модуль обеспечивает выполнение фильтрации почтовых сообщений путем последовательного просмотра набора тестов. Каждый тест имеет некоторую «стоимость». Если почтовое сообщение успешно проходит тест, эта «стоимость» добавляется к общему балу. Стоимость может быть положительной или отрицательной, положительные значения называются «spam». Сообщение проходит через все тесты, подсчитывается общий бал. Чем выше бал, тем больше вероятность, что сообщение является спамом.

Системные требования

UserGate Mail Server рекомендуется устанавливать на компьютер с операционной системой Windows XP/2003/Vista. Если почтовый сервер планируется использовать для работы с внешней сетью, компьютер, на который устанавливается UserGate Mail Server, должен быть подключен к сети Интернет.

Установка

Процедура установки UserGate Mail Server сводится к запуску установочного файла и выбору опций мастера установки. При запуске инсталлятор выполнит установку всех выбранных компонент, а также установит дополнительный пакет MS Visual C++ Redistributable. Все системные службы будут установлены автоматически, а почтовый сервер будет запущен сразу после завершения процесса установки. По умолчанию, почтовый сервер устанавливается в директорию “%Program files%\Entensys\UserGate Mail Server” (в дальнейшем %UserGate Mail%).

Если почтовый сервер не отвечает на запросы подключения к основным сервисам (SMTP, POP3, IMAP) следует проверить порт, используемый для подключения

консоли администрирования. По умолчанию, для подключения консоли администратора почтовый сервер прослушивает порт 2222 TCP.

Обновление и удаление

Перед установкой новой версии рекомендуется удалить предыдущую версию UserGate Mail Server, сохранив при необходимости файл настроек сервера «%UserGate Mail%\settings.xml» и резервную копию базы статистики. Резервные копии базы статистики складываются в директорию “%UserGate Mail%\Backup”

Удаление сервера UserGate выполняется через пункт меню «Пуск – Программы» или через консоль «Установка и удаление программ» в панели управления Windows. После удаления UserGate Mail Server в директории программы останется файл настроек сервера (settings.xml), копии базы статистики (папка Backup) и некоторые другие.

Быстрая настройка

1. Открыть консоль администрирования и подключиться к серверу
2. Перейти на вкладку Server Settings - Domains, нажать правой кнопкой на пустом месте и выбрать пункт добавить домен.
3. Указать параметры домена, его полное имя, например esafeline.net, и если нужно его Псевдоним (Alias), подпись домена (например подпись вашей организации) и сохранить изменения.
4. Добавить некоторое количество пользователей, на странице "Domain Settings - Local accounts", указывая при этом имена которые будут использованы в названии почтового адреса до собачки и их пароли.
5. По большому счету, настройки можно считать завершенными, для защиты от спама по умолчанию применяется техника проверки по известным спам-листам, (DNSBL), например (sorbs.net, spamhause.org). Так же включены антивирусные модули и Модули анализа писем на наличие спама от компании Commtouch и бесплатного SpamAssasin. Так что большинство спаммеров будет остановлено ещё до получения писем пользователями.
6. Доступ к своим почтовым ящикам через Веб-интерфейс можно организовать набрав в браузере IP-адрес машины с Почтовым сервером и порт 5555, например: <http://192.168.0.1:5555>
7. Настройка почтового клиента будет выглядеть очень просто, в качестве сервера для POP3 и SMTP протоколов указывается IP-адрес машины с UserGate Mail Server, например 192.168.0.1, как из примера выше, и имя пользователя и пароль.

Если мы завели пользователя с именем **testuser** в домене **esafeline.net**, то в параметрах авторизации имя пользователя можно указать с указанием собачки и имени домена (**testuser@esafeline.net**) или без ее (**testuser**).

Настройка соединений

При первом запуске консоль администрирования открывается на странице “Connections”, на которой присутствует единственное соединение с сервером UserGate Mail Server, работающем на интерфейсе 127.0.0.1 для пользователя

Administrator. Подключить консоль администрирования к серверу можно, щелкнув дважды на строке подключения или нажав на кнопку “Connect” в панели управления. Если консоль администрирования используется для работы с несколькими почтовыми серверами, на странице “Connections” можно создать несколько подключений. В свойствах подключений указываются следующие параметры:

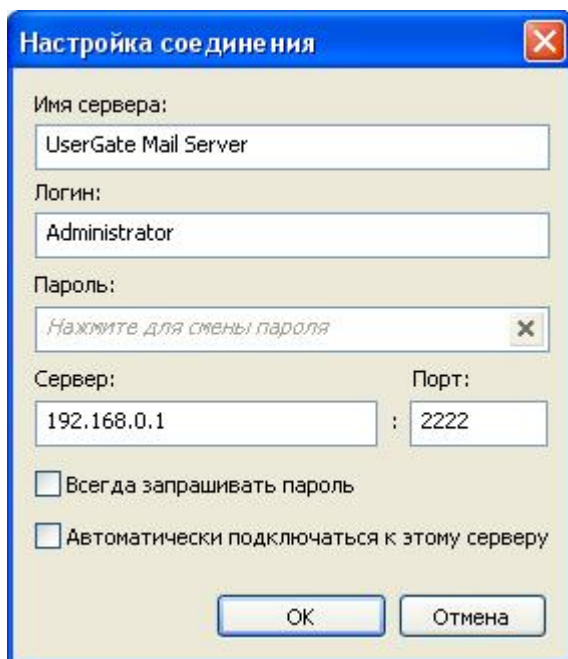
Название сервера — это название подключения

Имя пользователя — логин для подключения к серверу

Адрес сервера — доменное имя или IP-адрес сервера UserGate

Порт — TCP порт, используемый для подключения к серверу (по умолчанию используется порт 2222)

Пароль — пароль для подключения



Изображение 1, Настройка соединения

Дополнительно можно включить опции «Запрашивать пароль при подключении», а также «Подключаться автоматически». Если включена вторая опция, подключение к указанному почтовому серверу будет выполняться автоматически, при запуске консоли администрирования. Логин и пароль на подключение указывается в файле настроек сервера (%UserGate Mail%\settings.xml) и в файле настроек консоли администрирования (%UserGate Mail%\Console\console.xml).

Установка пароля на подключение

Создать логин и пароль для подключения к UserGate Mail Server можно на странице “Server Settings – Remote Admin” в разделе “Advanced Security Settings”. В этом разделе также можно указать TCP-порт для подключения к серверу. Новые настройки вступают в силу сразу после их применения, перезапуск сервера не требуется.

Установка пароля на доступ к базе статистики UserGate

Для хранения настроек сервера, а также пользовательских сообщений, UserGate Mail Server используется специальный сервис UserGate Mail Database Service. Сервис основан на СУБД PostgreSQL. По умолчанию сервис устанавливается в директорию “%UserGate Mail%\pgsql”. Подключение к базе данных выполняется через интерфейс localhost на порт 5432 TCP.



Изображение 2, Настройка параметров базы данных

При установке UserGate Mail Server инсталлятор автоматически создает три учетные записи (root, ugmailuser, ugwmuser) для работы с базой статистики. Логин и пароль пользователей, а также адрес и порт сервера UserGate Mail Database Server пользователей указываются в файлах %UserGate Mail%\pgsql\etc.

Для хранения настроек UserGate Mail Server создается база данных UGMail, доступ к базе осуществляется от имени пользователя ugmailuser. Для работы с UserGate Webmail создается отдельная база – ugwm, доступ к которой осуществляется от имени пользователя ugwmuser. Пользователь с привилегиями root используется сервисов UserGate Mail Service для создания баз данных, если таковые отсутствуют в момент запуска почтового сервера.

Настройки сервера

Основные настройки

В разделе Основных настроек указываются параметры для доступа к базе данных (БД) UserGate Mail Server. В настройках по умолчанию предполагается, что сервер БД установлен на одну с UserGate Mail Server машину, поэтому в качестве адреса БД указан адрес localhost. Почтовый сервер работает с БД от имени пользователя ugmailuser.



Изображение 1, Основные настройки

Для сильно загруженного почтового сервера, обрабатывающего несколько доменов, можно ускорить работу, включив кэширование объектов БД. В этом случае почтовый сервер будет помещать информацию о почтовых доменах и аккаунтах во внутреннюю память (кэш) снижая общее количество запросов к БД. В настройках параметров кэширования указывается время жизни записи в кэш (TTL, Time To Live). По умолчанию TTL составляет 60 секунд.

Обработка почтовых сообщений реализована в виде отдельных потоков. Администратор может указать необходимое количество потоков, занимающихся доставкой сообщений (Max. Delivery Threads), а также задать максимально допустимое количество потоков (Max. TCP threads). Дополнительно можно определить приоритет потоков (Thread Priority).

Настройка многопоточности	
Максимальное количество потоков	15
Число потоков доставки	3
Приоритет потоков	Нормальный

Изображение 2, Настройка потоков и приоритета

Внимание: не рекомендуется увеличивать общее количество потоков до максимального значения, а также выставлять наивысший приоритет (Highest), без необходимости, поскольку такой подход может увеличить объем памяти, выделяемой под процесс UGMail.exe и долю процессорного времени.

Настройка директорий для хранения сообщений

В разделе General Settings указывается расположение директории (Message Store), в которой почтовый сервер будет помещать поступающие сообщения. По умолчанию, все поступающие сообщения складываются в директорию %UserGate Mail Server%\Mail. Директория %UserGate Mail Server%\Tmp используется для хранения временных файлов, при антивирусной обработке сообщений.

Директории	
Место хранения сообщений	C:\Program Files\Entensys\UserGate Mail Server\Mail
Временная директория	C:\Program Files\Entensys\UserGate Mail Server\Tmp

Изображение 3, Настройка места хранения писем

Настройки сервера

Если почтовый сервер обрабатывает несколько доменов, администратор может указать домен по умолчанию (Default domain). В этом случае, если при авторизации пользователь указывает не полный почтовый адрес, а лишь его часть (без доменного имени), почтовый сервер автоматически подставит Default Domain.

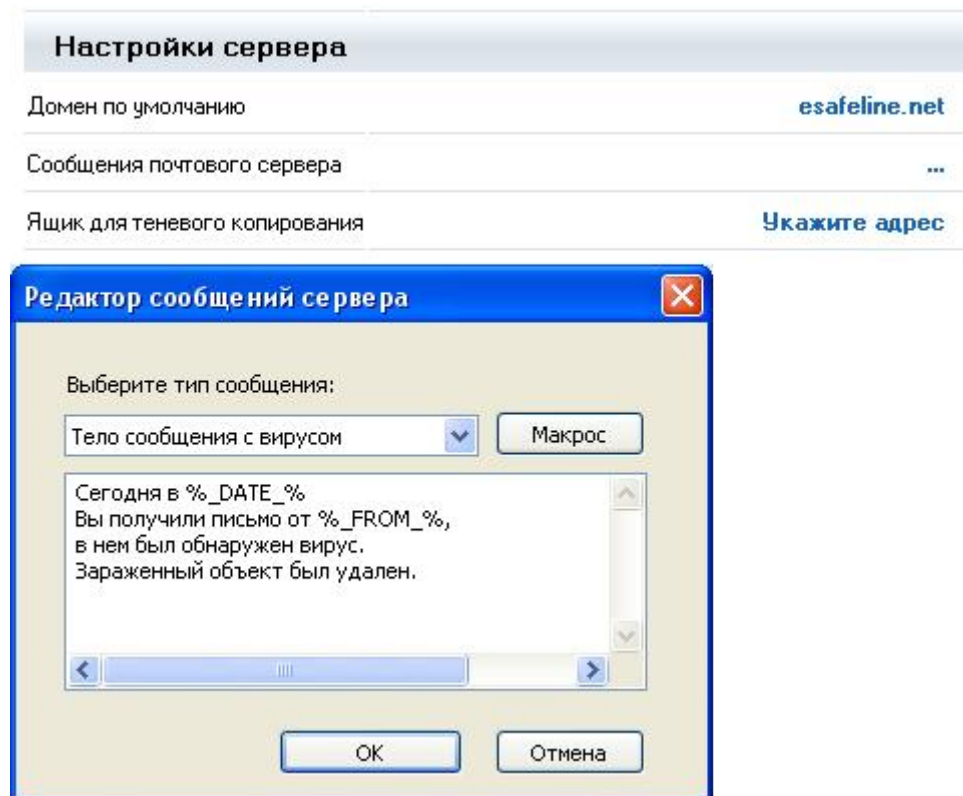
Скрытая копия (Shadow email)

UserGate Mail Server может выполнять копирование всех поступающих сообщений на указанный электронный адрес (Shadow Mail). В качестве Shadow Mail можно

указать любой, существующий почтовый адрес. Копирование почтовых сообщений выполняется, безусловно, в не зависимости от дальнейшей обработки письма фильтрами антиспама или антивируса, а также без влияния пользовательских правил обработки сообщений.

Создание шаблонов серверных сообщений

В разделе Server Messages Setup администратор может задать текст служебных сообщений почтового сервера. Для некоторых типов сообщений существуют предопределенный набор макросов, позволяющих детализировать текст сообщения. Например, макрос `%_ATTACHMENT_` обозначает имя вложенного файла. При создании уведомляющего сообщения, почтовый сервер заменит макрос на название вложенного файла.

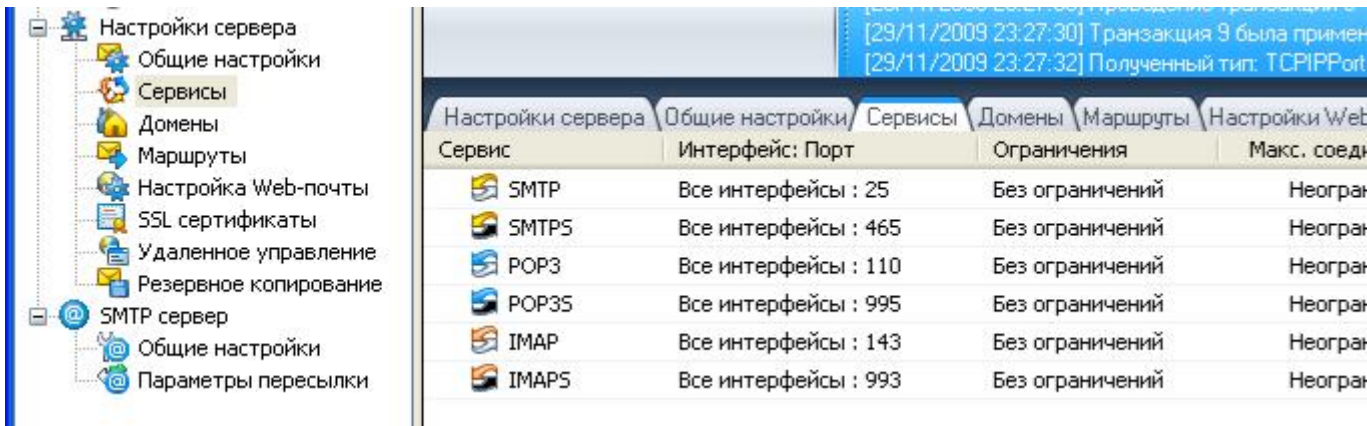


Изображение 4,5 Настройка сервера, и задание сообщений сервера

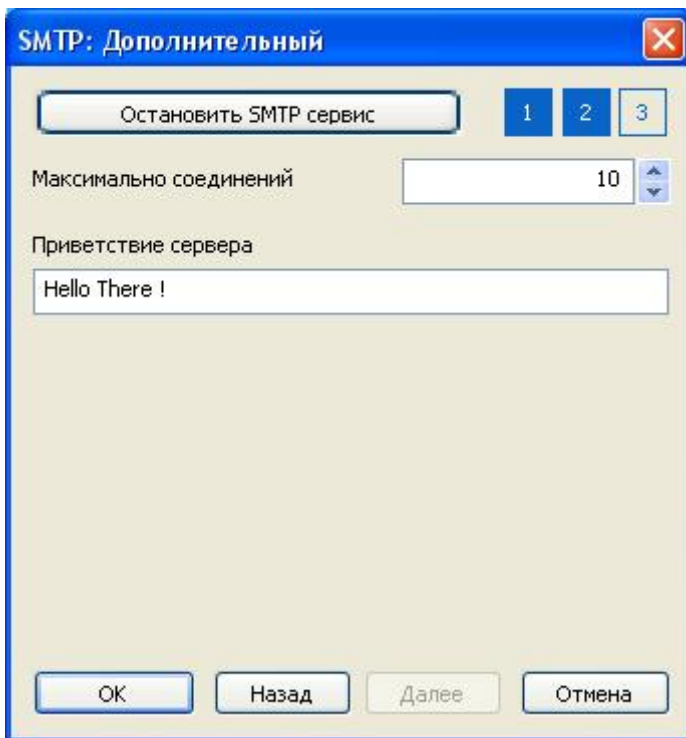
Сервисы

Обработка почтовых протоколов реализована в виде набора сервисов. Сервисы перечислены на одноименной странице консоли администрирования UserGate Mail Server. Для каждого сервиса можно указать список прослушиваемых интерфейсов и портов, задать предельное количество одновременных подключений и ограничить диапазон IP адресов, с которых разрешено подключение. По умолчанию почтовые сервисы прослушивают все доступные сетевые интерфейсы сервера. Ограничения на количество подключений не установлены. В настройках по умолчанию подключения к почтовым сервисам разрешено с любых адресов (диапазон 0.0.0.0 - 255.255.255.255).

Помимо сетевых настроек, для каждого сервиса администратор может задать т.н. Welcome Message.



Изображение 1, Сервисы.

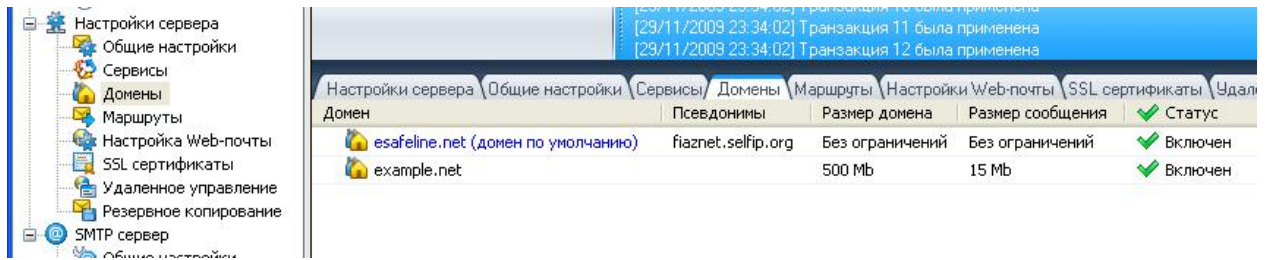


Изображение 2, Настройка сервисов.

Домены

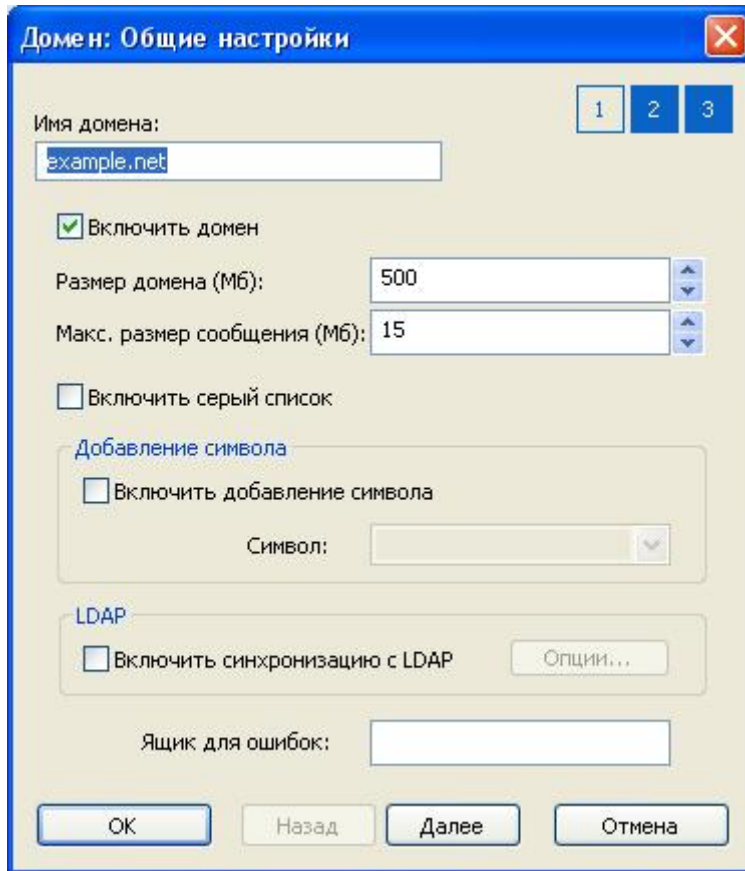
Домен является ключевой настройкой почтового сервера. Администратор может указать список доменов, обрабатываемых почтовым сервером, через одноименный пункт дерева настроек консоли администрирования. Для каждого домена указывается:

- название (в формате FQDN, Fully Qualified Domain Name)
- предельное значение размера домена
- режим Grey Listing (один из методов антиспам проверки)
- режим Plus Addressing
- адрес почтового ящика, в который будут помещаться сообщения об ошибках



Изображение 1, Домены.

Размер домена вычисляется как сумма размеров аккаунтов, входящих в домен. Если суммарный размер всех аккаунтов домена превышает установленный предел, почтовый сервер перестанет обрабатывать входящие сообщения для данного домена.



Изображение 2, Настройки домена.

Дополнительно, в свойствах домена администратор может указать "подпись домена" (Domain Signature) и режим ее добавления, а также задать одно или несколько альтернативных имен домена (alias).

Домен: Подпись

Имя домена: example.net

Использовать подпись домена

Редактировать подпись

Домен Example.net.

Использование подписи: Добавить к подписи пользо...

Добавлять при ответе

Добавлять для локальных писем

OK Назад Далее Отмена

Домен: Псевдонимы

Имя домена: example.net

Псевдонимы домена

Название
example2.net
example3.net

OK Назад Далее Отмена

Изображение 3,4 Подпись домена, Псевдонимы.

Опция LDAP Sync в настройках почтового домена предназначена для синхронизации учетных записей с каталогом LDAP, например с MS Active Directory.

LDAP синхронизация

Помимо внутренней базы учетных записей почтового домена, UserGate Mail Server поддерживает функцию импорта пользовательских учетных записей из LDAP каталога. Такой подход позволяет выполнять централизованное управление учетными записями, сокращает количество возможных ошибок и упрощает процесс администрирования. Для выполнения синхронизации с LDAP каталогом необходимо:

- включить опцию LDAP Sync в свойствах почтового домена в разделе Server Settings
- указать имя LDAP каталога (например, название домена Active Directory)
- указать логин и пароль пользователя, от имени которого будет осуществляться доступ к LDAP каталогу

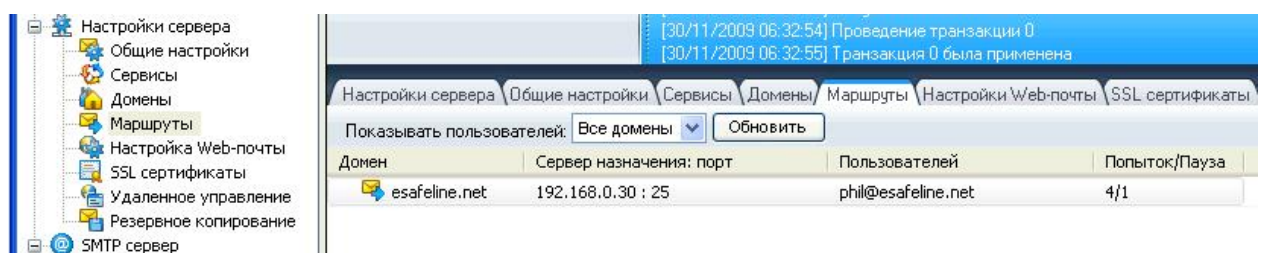
В разделе Advanced можно указать дополнительные настройки, например, название узла с которого почтовый сервер будет просматривать структуру каталогов LDAP. При синхронизации почтовый сервер будет просматривать все нижележащие узлы LDAP каталога.

При обращении к каталогу LDAP будут выбраны все включенные учетные записи, в свойствах которых указан адрес электронной почты. Доступ к каталогу осуществляется по протоколу LDAP. Безопасный вариант протокола в данный момент не поддерживается. Период повторного опроса каталога не конфигурируется и составляет две минуты.

Маршруты

Для каждого домена можно определить маршрут доставки входящих сообщений. Маршрут определяется в разделе Routes консоли администрирования. В настройках маршрута указываются следующие параметры:

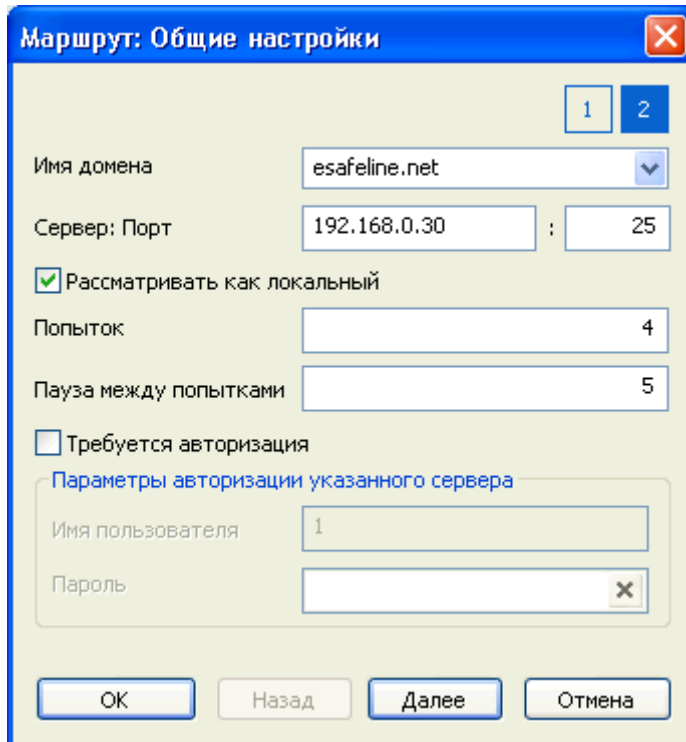
- название почтового домена
- адрес и порт удаленного SMTP сервера
- максимальное количество попыток доставки
- таймаут повторной доставки (интервал времени, через который сервер попытает доставить сообщение повторно, если предыдущая попытка была неудачной)
- параметры для авторизации на удаленном SMTP сервере



Изображение 1, Маршруты сервера.

Дополнительно, в параметрах маршрута можно определить аккаунты, для которых будет использоваться маршрут. По умолчанию предполагается, что маршрут используется для всех аккаунтов домена.

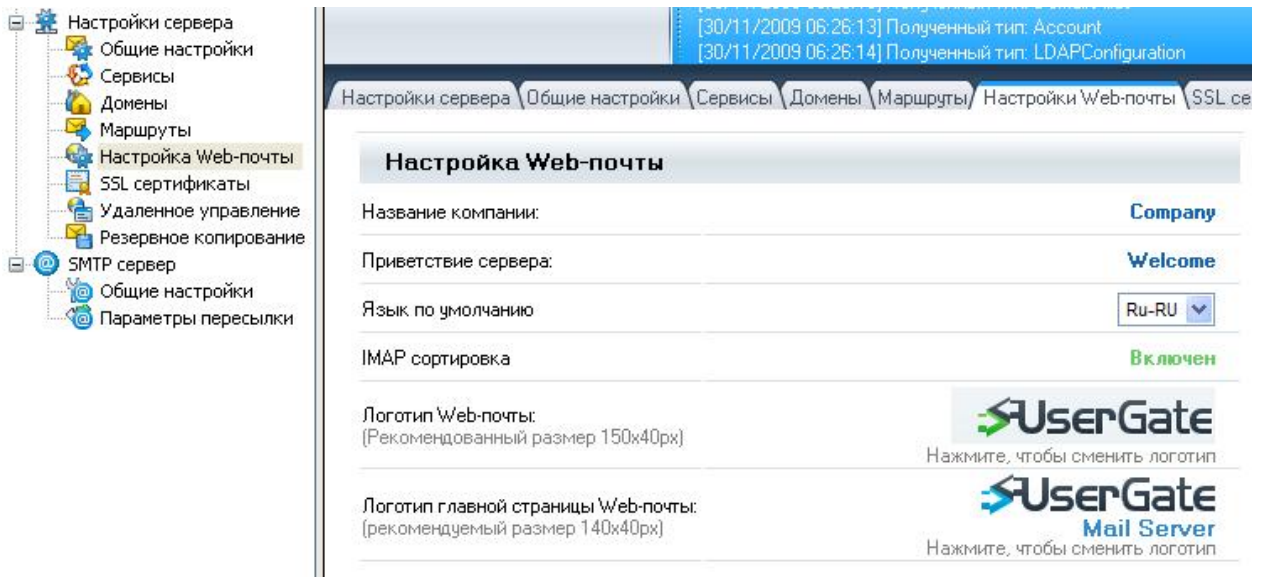
Опция «Рассматривать как локальный» во включенном состоянии позволяет рассматривать указанный в маршруте домен как локальный, т.е. избавляет от необходимости явного задания соответствующих разрешений в Relay Settings.



Изображение 2, Параметры для маршрутов.

Свойства Web-почты

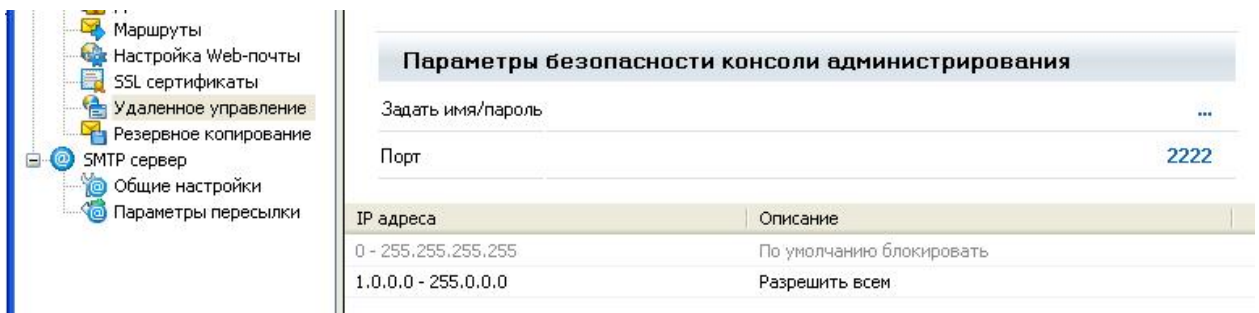
В этом разделе администратор может указать параметры UserGate Webmail, такие как "Название компании", текст приветствующего сообщения, системную локаль и логотип компании. Дополнительно можно включить режим IMAP сортировки. По умолчанию, UserGate Webmail работает на порту 5555 и доступен по адресу: <http://ugmail:5555/webmail>, где ugmail - адрес сервера, на который установлен UserGate Mail Server.



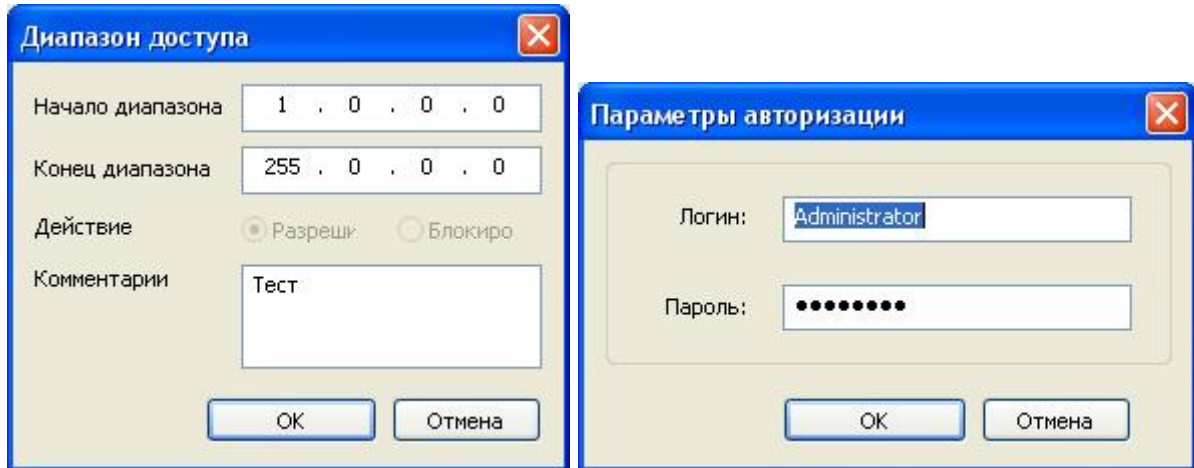
Изображение 1, Настройки Web-почты.

Настройка доступа к серверу

Администрирование почтового сервер выполняется с помощью специальной программы - консоли администратора. Консоль администратора представляется собой самостоятельное приложение, которое общается с сервером по специальному протоколу, поверх TCP. Для общения сервера и консоли, по умолчанию используется порт 2222. В разделе Remote Admin можно создать правила, разрешающие подключение консоли администратора только с определенных IP адресов. Правила обрабатываются в порядке приоритетов. Приоритет правила определяется его порядком в списке правил. Последним всегда обрабатывается default правило, запрещающее подключение консоли администратора со всех адресов. В настройках Remote admin также можно задать логин и пароль на подключение консоли администратора и переопределить номер порта.



Изображение 1, Страница с настройками доступа.



Изображение 2,3 Задание диапазона доступа и Задание имени и пароля.

Настройка резервного копирования в UserGate Mail Server

В настройках резервного копирования указываются следующие параметры:

- Директория, в которую будут складываться файлы резервных копий. По умолчанию используется директория %UGMail%\Backup.
- Максимальное количество файлов резервных копий, которые требуется сохранять в директории. Более ранние файлы копий будут удаляться автоматически
- Интервал выполнения полного резервного копирования (full backup)
- Интервал выполнения дифференциального резервного копирования (differential backup). Рекомендуется выбирать значение этого интервала, меньшее интервала для создания полных копий

Время старта системы резервного копирования.

Опционально, администратор UserGate Mail Server может выполнить резервное копирование текущих настроек сервера, через соответствующий пункт настроек (Manual Backup)

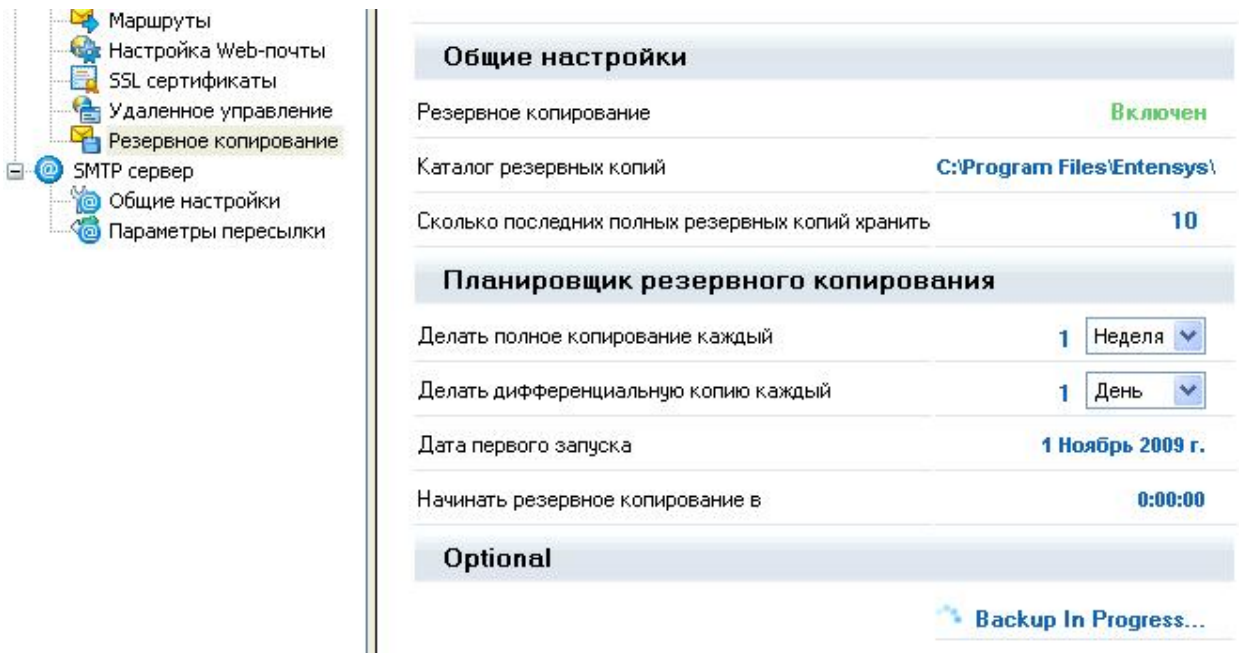
Для получения времени создания full backup, нужно прибавить целое количество интервалов для full backup к времени начала работы системы копирования. Пусть время начала работы системы копирования задано параметром Tstart и заданы периоды для полного Pfull и дифференциального копирования Pdiff, тогда, время создания i-го файла full backup определяется следующим образом:

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

Время создания differential backup:

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

При резервном копировании UserGate Mail Server сохраняет содержимое почтовой директории (по умолчанию %UGMail%\Mail), копирует файл настроек сервера (%UGMail%\settings.xml) и создает дамп используемой базы данных. В базе данных UserGate Mail Server (база - ugmail) сохраняются некоторые настройки сервера, а также информация об обработанных почтовых сообщениях.



Изображение 1, Настройки резервного копирования.

Восстановление состояния UserGate Mail Server из резервной копии

Восстановление состояния почтового сервера из резервных копий выполняется в два этапа. На первом этапе, из набора дифференциальных копий и первоначальной полной копии формируется результирующий файл копии, точнее - директория, содержащая все нужные файлы. Для создания результирующей копии используется консольная утилита BackupPrepare, расположенная в директории %UGMail%\Backup. В качестве аргумента командной строки этой утилите передается название ZIP архива, содержащее *diff* в названии. Дата, присутствующая в названии ZIP архива, указывает дату создания копии.

Для восстановления наиболее актуального состояния почтового сервера следует выбирать ZIP архив с самой последней датой. Вызов утилиты BackupPrepare может выглядеть, например, так:

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

При работе утилита BackupPrepare последовательно пройдет через всю цепочку промежуточных копий, вплоть до первого файла полной копии. Если цепочка пройдена успешно, в результате будет создана директория, содержащая итоговый backup настроек сервера на указанную дату. В данном случае, будет создана директория "2010.01.01 09.01.00".

На втором этапе имя полученной директории в качестве аргумента передается командному файлу RestoreBackup.bat. Этот файл расположен в директории %UGMail%\Backup. Перед запуском RestoreBackup.bat следует остановить почтовый сервер и закрыть любые приложения, имеющие доступ к почтовой базе данных. Запуск RestoreBackup.bat может выглядеть следующим образом:

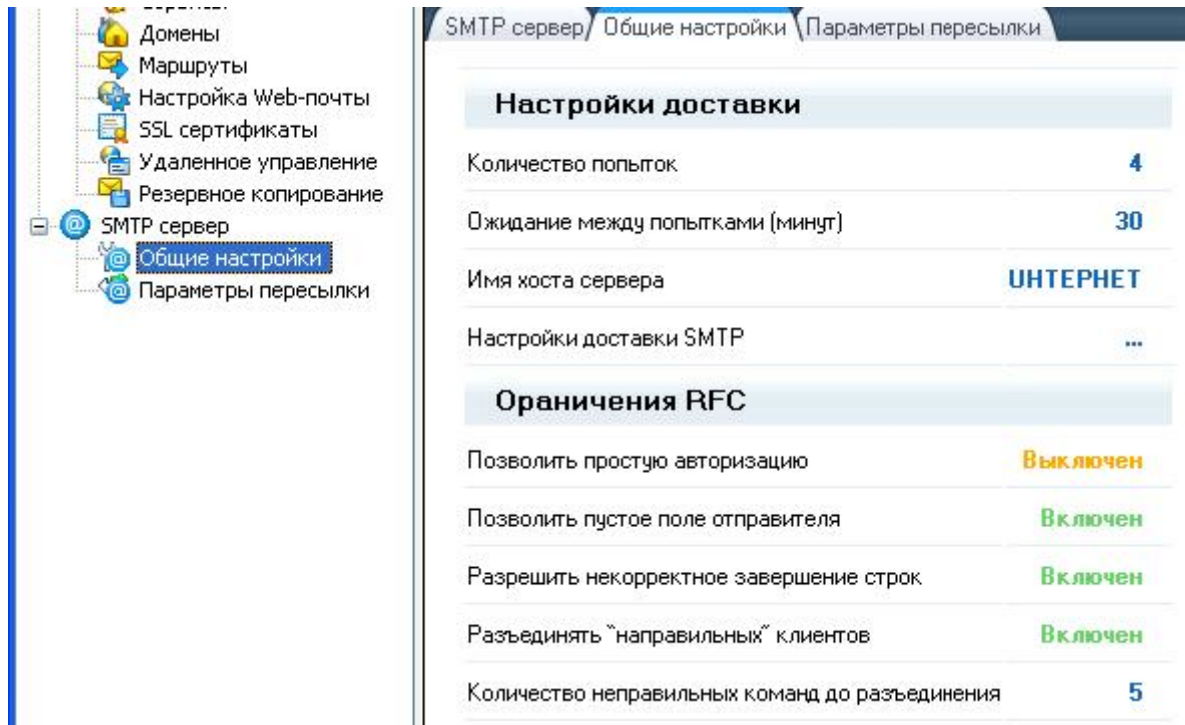
```
RestoreBackup.bat "2010.01.01 09.01.00"
```

Утилита RestoreBackup удалит текущую директорию для хранения почтовых сообщений, текущие настройки сервера и базу данных, заменив их файлами из резервной копии.

Сервер SMTP

Основные настройки

В общих настройках SMTP сервера указываются параметры доставки сообщений, режим доставки, ограничения, которые будут использоваться в соответствии с требованиями RFC на почтовые протоколы и некоторые другие параметры.



Изображение 1, Настройки сервиса SMTP.

Основными параметрами настроек SMTP сервера являются параметры очереди доставки.

Эти параметры определяют, как долго почтовое сообщение будет находиться в очереди обработки сообщений и как именно должны доставляться почтовые сообщения. К параметрам очереди относятся следующие настройки:

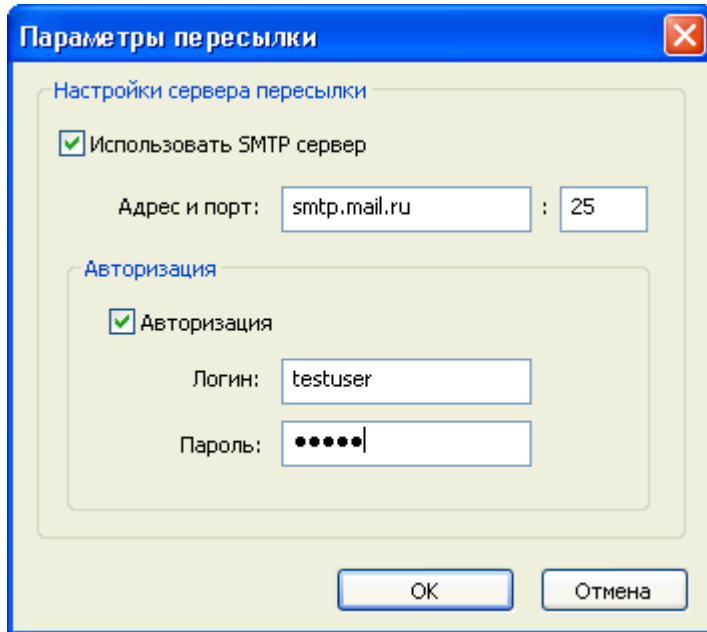
- максимально количество попыток доставки
- таймаут повторной доставки

Имя хоста (параметр Hostname) будет использоваться почтовым сервером при подключении к другим почтовым серверам при доставке сообщений.

По умолчанию полагается, что SMTP сервер работает в т.н. режиме MX - доставки, когда каждое сообщение доставляется непосредственно серверу, отвечающему за [домен](#) получателя. Тем не менее, администратор может задать промежуточный сервер (Relay Server), указав его в разделе SMTP Delivery Settings. В настройках Relay Server'a также можно указать логин и пароль, если требуется авторизация.

SMTP сервер может блокировать почтовые сообщения, если в качестве адреса получателя перечислено несколько адресов. Предельное количество получателей задается параметром Максимальное количество получателей. Также доступна опция Delivery Log, позволяющая включать подробное логирование процесса отправки сообщений.

Нелинейность стадий обработки почтовых сообщений, за счет наличия пользовательских правил, антивирусных и **антиспам** модулей, может привести к заикливанию в обработки почтового сообщения. И хотя такая ситуация маловероятна, в настройки вынесен такой параметр как "Максимальная глубина пересылки"



Изображение 2, Настройки пересылки.

Параметры пересылки

Администратор почтового сервера может разрешить или запретить некоторые виды обработки почтовых сообщений для определенных IP адресов или их диапазонов. В правилах настройки relay указываются:

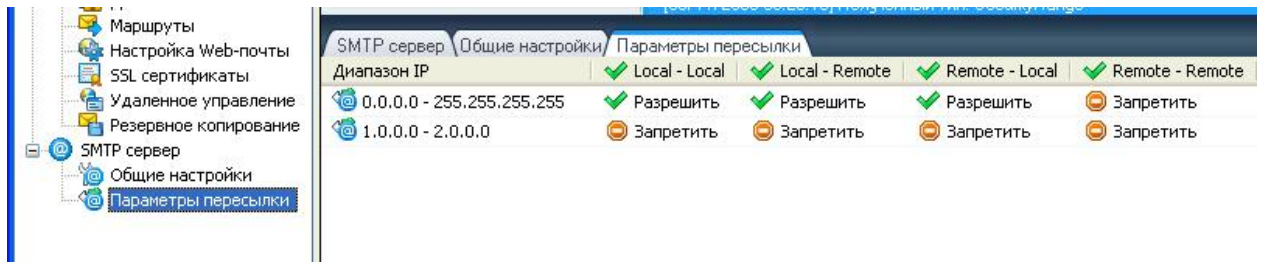
- начальный и конечный IP адреса диапазона
- опции пересылки
- комментарий

Опции пересылки позволяют разрешить пересылку сообщений внутри собственного почтового **домена** (направление Local - Local), отправку сообщений на внешние **домены** от имени собственного (направление Local - Remote), а также прием сообщений, адресованных к нашему **домену**, от внешних **доменов** (направление Remote - Local).

Включенная опция Remote - Remote позволяет использовать UserGate Mail Server в качестве сервера пересылки. Категорически не рекомендуем включать этот режим, т.к. открытые релейы были признаны сообществом по развитию интернета как ошибочные конфигурации почтовых серверов. Если к серверу имеется доступ из интернета никогда не включайте эту опцию.

Внимание: Если сервер предназначен для работы с внешней почтой, не стоит включать опцию Remote - Remote для всего диапазона IP адресов. В этом случае ваш почтовый сервер превратится в т.н. open relay.

Правила в разделе Relay Settings обрабатываются в соответствии с приоритетами.

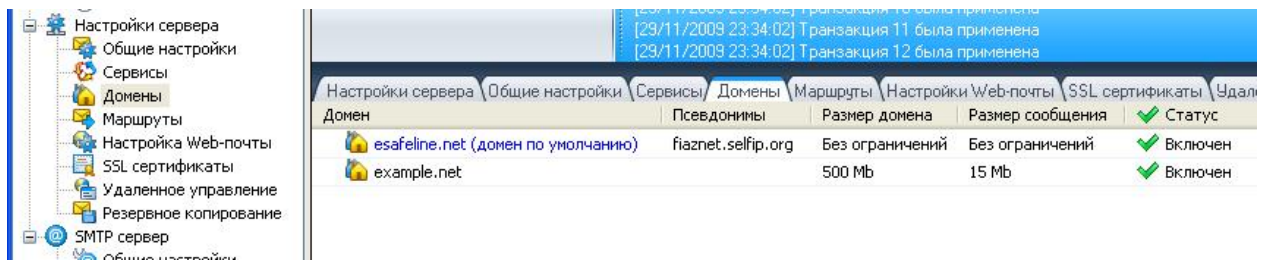


Изображение 3, Настройка разрешений, для пересылки.

Домены

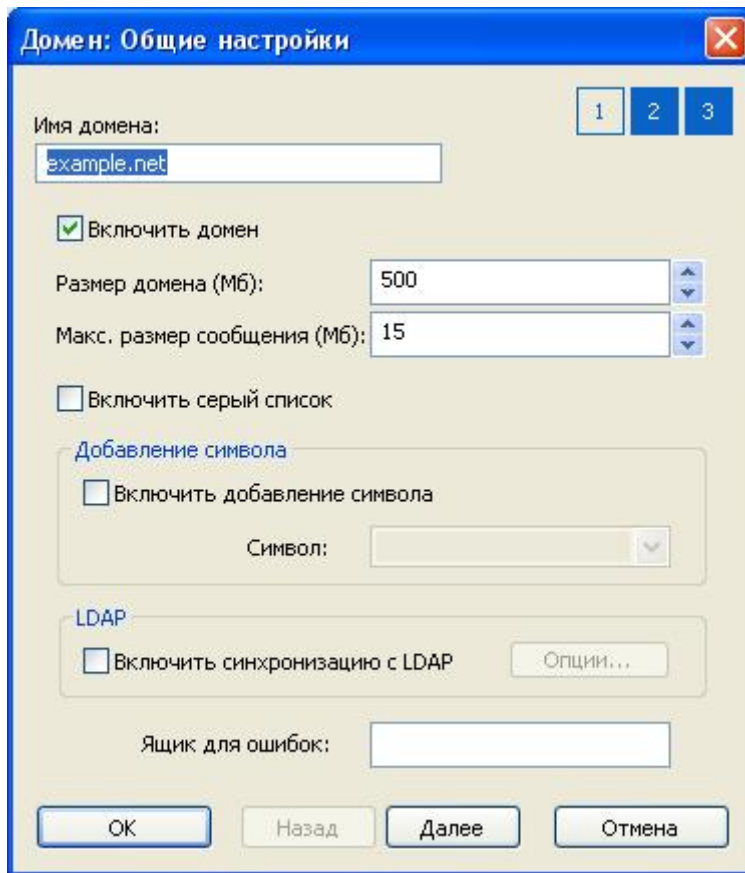
Домен является ключевой настройкой почтового сервера. Администратор может указать список доменов, обрабатываемых почтовым сервером, через одноименный пункт дерева настроек консоли администрирования. Для каждого домена указывается:

- название (в формате FQDN, Fully Qualified Domain Name)
- предельное значение размера домена
- режим Grey Listing (один из методов антиспам проверки)
- режим Plus Addressing
- адрес почтового ящика, в который будут помещаться сообщения об ошибках



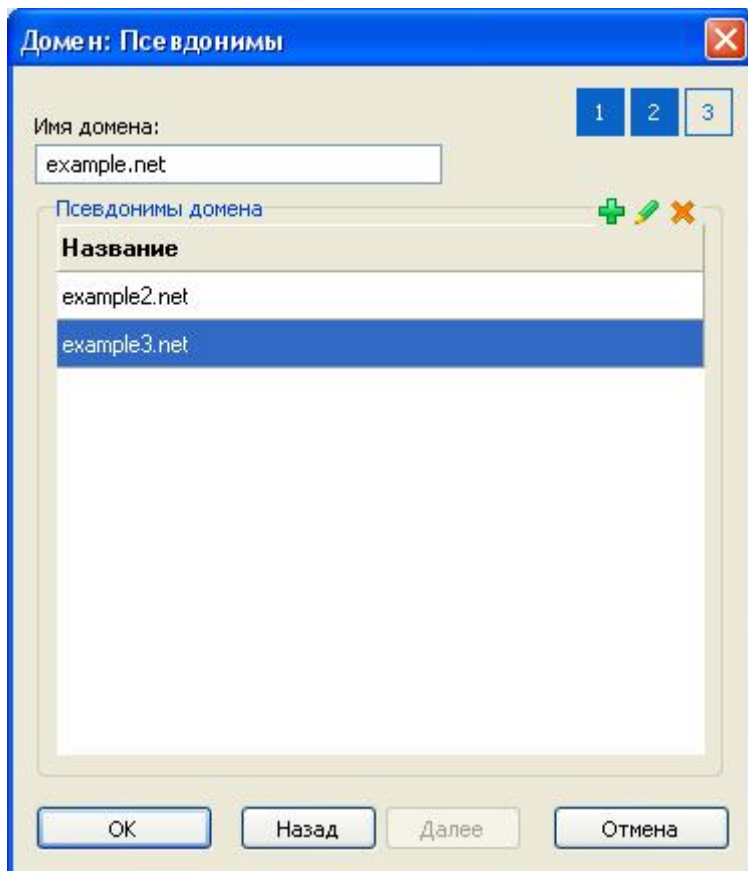
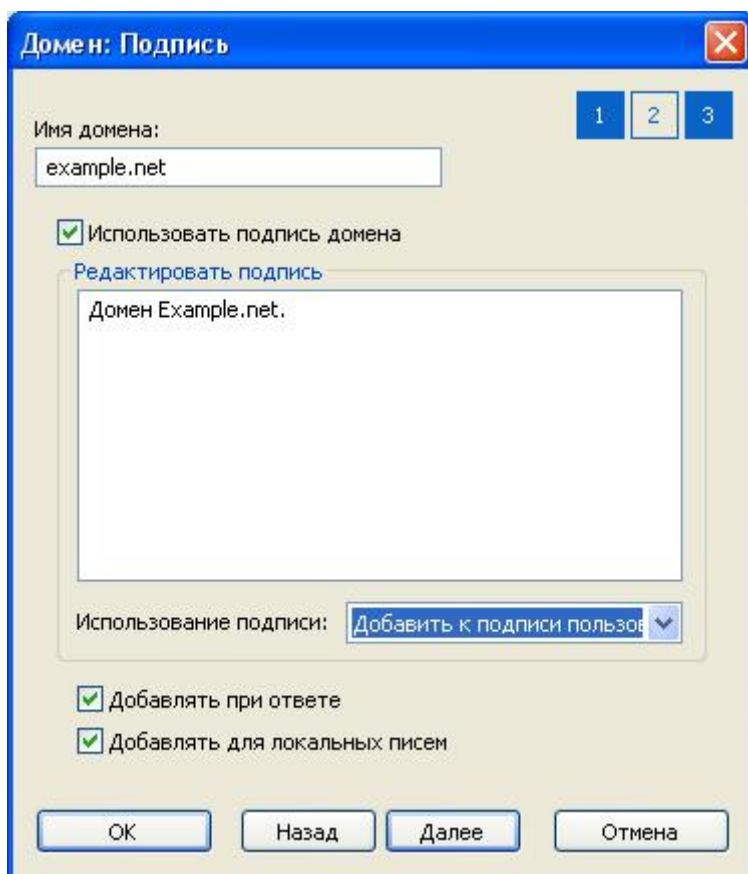
Изображение 1, Домены.

Размер домена вычисляется как сумма размеров аккаунтов, входящих в домен. Если суммарный размер всех аккаунтов домена превышает установленный предел, почтовый сервер перестанет обрабатывать входящие сообщения для данного домена.



Изображение 2, Настройки домена.

Дополнительно, в свойствах домена администратор может указать "подпись домена" (Domain Signature) и режим ее добавления, а также задать одно или несколько альтернативных имен домена (alias).



Изображение 3,4 Подпись домена, Псевдонимы.

Опция LDAP Sync в настройках почтового домена предназначена для синхронизации учетных записей с каталогом LDAP, например с MS Active Directory.

LDAP синхронизация

Помимо внутренней базы учетных записей почтового домена, UserGate Mail Server поддерживает функцию импорта пользовательских учетных записей из LDAP каталога. Такой подход позволяет выполнять централизованное управление учетными записями, сокращает количество возможных ошибок и упрощает процесс администрирования. Для выполнения синхронизации с LDAP каталогом необходимо:

- включить опцию LDAP Sync в свойствах почтового домена в разделе Server Settings
- указать имя LDAP каталога (например, название домена Active Directory)
- указать логин и пароль пользователя, от имени которого будет осуществляться доступ к LDAP каталогу

В разделе Advanced можно указать дополнительные настройки, например, название узла с которого почтовый сервер будет просматривать структуру каталогов LDAP. При синхронизации почтовый сервер будет просматривать все нижележащие узлы LDAP каталога.

При обращении к каталогу LDAP будут выбраны все включенные учетные записи, в свойствах которых указан адрес электронной почты. Доступ к каталогу осуществляется по протоколу LDAP. Безопасный вариант протокола в данный момент не поддерживается. Период повторного опроса каталога не конфигурируется и составляет две минуты.

Настройки домена

Локальные пользователи

Для каждого домена в разделе Local Accounts создаются пользовательские учетные записи. В настройках учетной записи указываются следующие параметры:

- логин
- имя почтового домена
- уровень доступа к консоли администрирования
- пароль
- имя пользователя
- персональные ограничения на размер сообщений
- одно или несколько альтернативных имен (alias)
- почтовый ящик для перенаправления сообщений

Авторизация пользователей через LDAP

Для авторизации на почтовом сервере, в свойствах почтовой учетной записи необходимо указать пароль. Однако, если почтовый сервер установлен на

машину, входящую в домен Active Directory и в свойствах почтового домена включена опция LDAP Sync, указывать пароль в свойствах почтового аккаунта не обязательно. В этом случае, для проверки подлинности пользователя будет использован доменный пароль.

Пользователь: Общие настройки

Логин пользователя: 1 2 3

Включить пользователя

Домен:

Пароль:

Размер ящика (МБ):

Переопределить максимальный размер сообщения

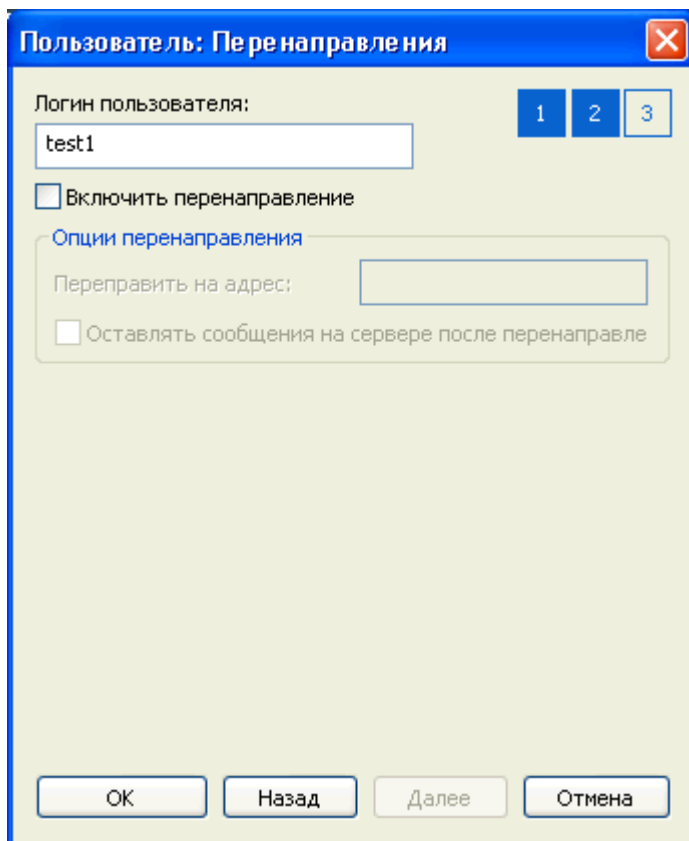
Отменить настройки домена

Макс. размер письма (КБ):

Пользователь: Псевдонимы

Логин пользователя: 1 2 3

Псевдонимы пользователя

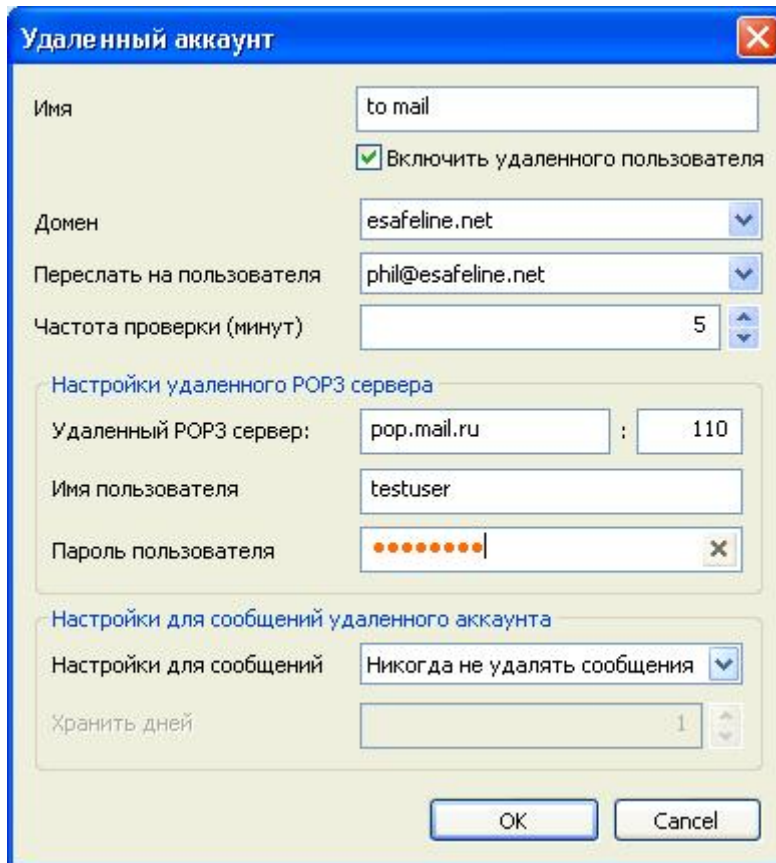


Изображение 1,2,3 Настройка пользователей.

Удаленные аккаунты

Каждой локальной учетной записи в UserGate Mail Server можно сопоставить некоторый удаленный аккаунт. Удаленный аккаунт используется, когда необходимо выполнять периодический опрос внешнего почтового ящика. При наличии сообщений во внешнем почтовом ящике, сообщения будут автоматически скачены и помещены в локальный аккаунт и, в зависимости от настроек, могут быть удалены на удаленном почтовом ящике. Если локальный аккаунт или соответствующий ему **домен** не активны, то скачивание из удаленных аккаунтов не производится. В настройках удаленного аккаунта указываются следующие параметры:

- почтовый адрес
- адрес удаленного сервера
- логин и пароль для авторизации на POP3 сервере
- локальные аккаунты, которые должны получать почту с удаленного аккаунта



Удаленный аккаунт

Имя: to mail

Включить удаленного пользователя

Домен: esafeline.net

Переслать на пользователя: phil@esafeline.net

Частота проверки (минут): 5

Настройки удаленного POP3 сервера

Удаленный POP3 сервер: pop.mail.ru : 110

Имя пользователя: testuser

Пароль пользователя: [masked]

Настройки для сообщений удаленного аккаунта

Настройки для сообщений: Никогда не удалять сообщения

Хранить дней: 1

OK Cancel

Изображение 1, Настройка удаленных пользователей.

Списки рассылки

Рассылка есть механизм, который позволяет отправлять одно письмо группе участников рассылки. Она представляет собой адрес, при получении писем на который, они дублируются и рассылаются всем участникам рассылки. В настройках рассылки указывается:

- почтовый адрес рассылки
- режим, которые определяет, с каких адресов письма будут приниматься для этой рассылки
- почтовые адреса участников рассылки

UserGate Mail Server поддерживает три режима рассылки сообщений. Режим Общий представляет собой обычный адрес групповой рассылки. В этом режиме на указанный адрес сообщения можно отправлять с любых адресов.

В режиме Групповой отправлять сообщения на адрес групповой рассылки могут только участники группы, т.е. только те пользователи, которые перечислены в свойствах рассылки. При попытке отправить сообщение на указанный адрес с любых прочих аккаунтов, почтовый сервер будет возвращать сообщение "550 Not authorized".

Информационный предназначен для случая, когда один определенный аккаунт должен иметь возможность отправки сообщений сразу всем участникам группы. При попытке отправить сообщение на адрес групповой рассылки с любого другого аккаунта, почтовый сервер вернет сообщение "550 Not authorized".

Список рассылки: Общие настройки

Адрес 1 2
testaddress

Включить список

Опции

Список для домена: example.net

Режим: Общий





Информационный адрес:

Подсказка
Общий или открытый режим: Любой пользователь будет иметь доступ к этому списку рассылки.

OK Назад Далее Отмена

Список рассылки: Получатели

Адрес 1 2
testaddress

Получатели    

Получатели

phil@esafeline.net

Требуется авторизация

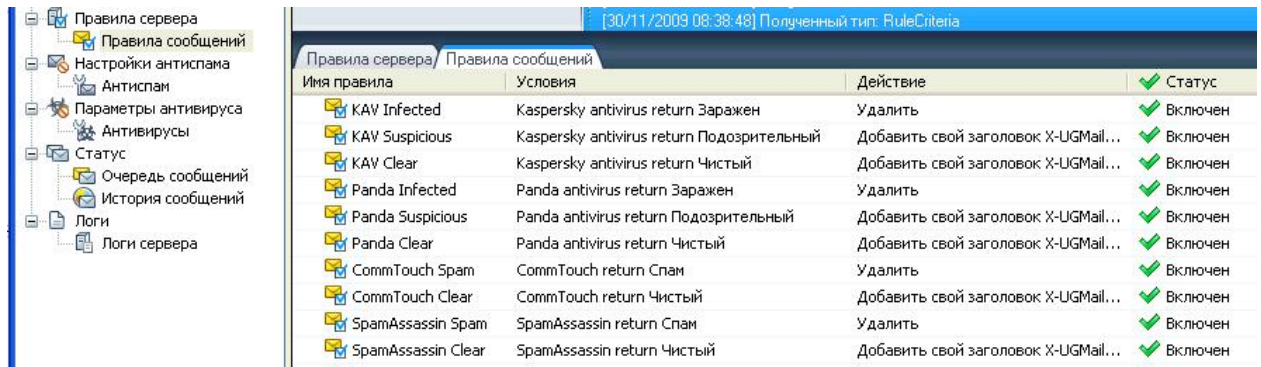
OK Назад Далее Отмена

Изображение 1,2 Списки рассылки.

Правила для сообщений

Обработка сообщений в UserGate Mail Server реализована на основе правил (Message Rules). Правила представляют собой набор условий, объединяемых по логическому И/ИЛИ и одно или несколько действий, которые должны быть выполнены, если указанное условие выполняется. Правила обрабатываются последовательно сверху вниз, таким образом, каждое сообщение может быть

обработано несколькими правилами. Для нелинейной обработки сообщений предусмотрены такие действия как “Stop Processing”, в этом случае нижележащие правила не рассматриваются, и “Jump to Rule” – переход на определенное правило, расположенное ниже по списку правил.



Имя правила	Условия	Действие	Статус
KAV Infected	Kaspersky antivirus return Заражен	Удалить	Включен
KAV Suspicious	Kaspersky antivirus return Подозрительный	Добавить свой заголовок X-UGMail...	Включен
KAV Clear	Kaspersky antivirus return Чистый	Добавить свой заголовок X-UGMail...	Включен
Panda Infected	Panda antivirus return Заражен	Удалить	Включен
Panda Suspicious	Panda antivirus return Подозрительный	Добавить свой заголовок X-UGMail...	Включен
Panda Clear	Panda antivirus return Чистый	Добавить свой заголовок X-UGMail...	Включен
CommTouch Spam	CommTouch return Спам	Удалить	Включен
CommTouch Clear	CommTouch return Чистый	Добавить свой заголовок X-UGMail...	Включен
SpamAssassin Spam	SpamAssassin return Спам	Удалить	Включен
SpamAssassin Clear	SpamAssassin return Чистый	Добавить свой заголовок X-UGMail...	Включен

Изображение 1, Правила для сообщений.

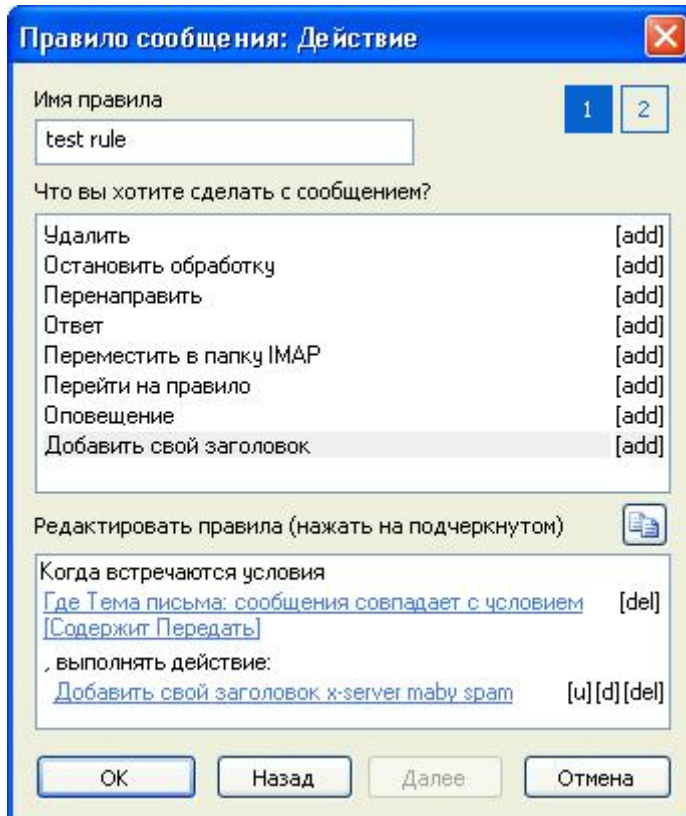
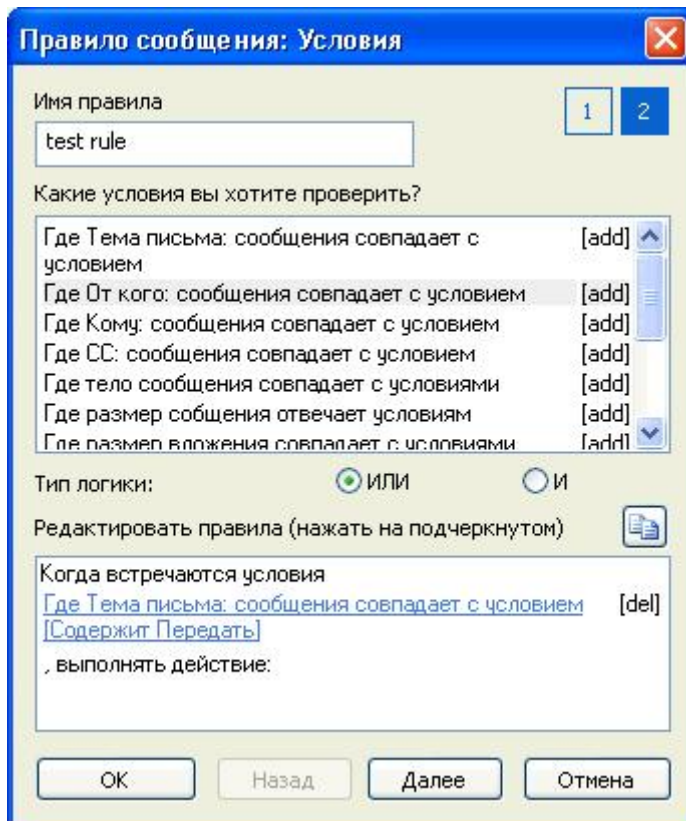
Доступны следующие условия:

- Поле Subject [Equals, Contains, RegEx, Not Contains, Not Equals]
- Поле From [Contains, RegEx, Not Contains]
- Поле To [Contains, RegEx, Not Contains]
- Поле CC [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]

Доступны следующие действия:

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

Фильтрация сообщений по Custom Header не предусмотрена и предназначена главным образом для обработки на стороне почтового клиента. Правила можно применять ко всем или только к указанным аккаунтам домена.



Изображение 2,3 Правила.

Антивирусы

В UserGate Mail Server интегрированы два антивирусных модуля: антивирус Kaspersky Lab и Panda Security. Оба антивирусных модуля предназначены для

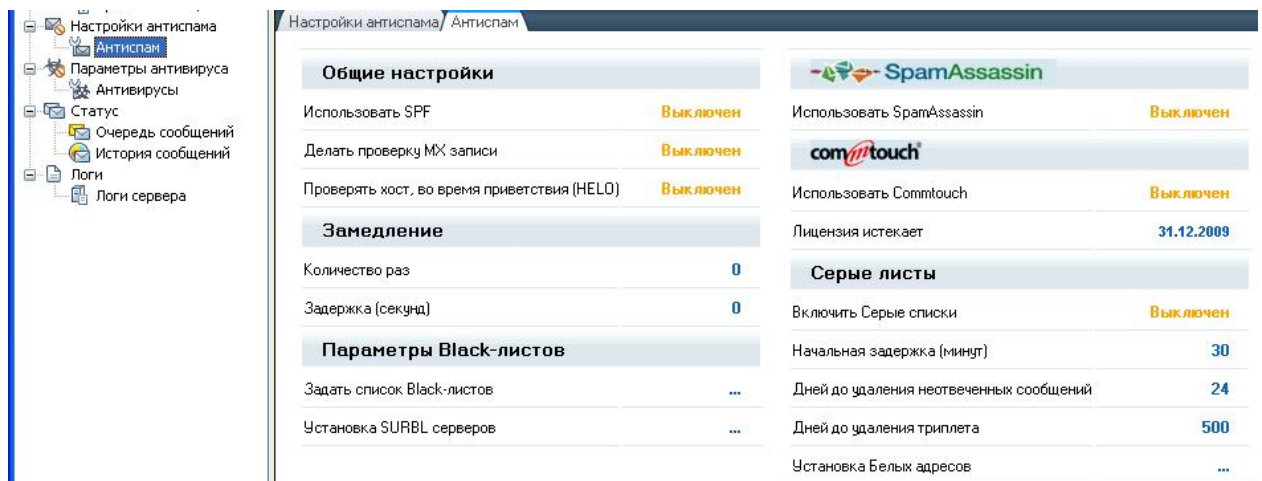
проверки SMTP трафика. Настройки антивирусных модулей доступны в разделе Antivirus консоли администрирования. Администратор может указать предельный размер сообщения, которое будет проверяться антивирусными модулями, действие, выполняемое сервером при обнаружении вируса, а также включить режим оповещений отправителя и/или получателя сообщения.

Перед запуском антивирусных модулей необходимо запустить обновление антивирусных баз и дождаться его завершения. В настройках по умолчанию базы антивируса Касперского обновляются с сайта Kaspersky Lab, а для антивируса Panda скачиваются с <http://www.usergate.ru>.

UserGate Mail Server поддерживает одновременную работу двух антивирусных модулей. В этом очередность проверки определяется правилами Message Rules, задаваемыми администратором UserGate Mail Server.

Антиспам

В UserGate Mail Server реализована поддержка нескольких методов антиспам фильтрации. Антиспам фильтрация может выполняться на основе DNSBL (DNS blacklist), SURBL (Spam URI blacklist), Greylisting и Tarpitting.



Изображение 1, Антиспам.

Серые списки

Серые списки (Greylisting) реализуют механизм отсрочки получения писем. Это механизм подразумевает, что входящее письмо сразу не принимается, а отправителю отсылается сообщение с просьбой повторить попытку через некоторое время. При этом сохраняется информационный триплет (информация о том – кто, откуда и куда посылал). Если же триплет входящего письма совпадает с одним из триплетов, уже хранящимся в списке, то письмо принимается (это означает, что письмо пытаются доставить повторно). Таким образом, отсекаются спамеры, которые обычно не предпринимают повторных попыток отсылки писем на один и тот же адрес.

Черные списки (DNSBL)

Динамический «черный список» представляет собой сетевую службу, предоставляемую провайдером «черных списков». Эти провайдеры отслеживают адреса IP (иногда и имена доменов), скомпрометированные спамерами. Почтовые фильтры, поддерживающие применение динамических «черных списков», формируют запрос к провайдеру «черного списка», содержащий адрес

отправителя, а также адреса почтовых серверов, через которые проходило письмо по пути к получателю. Если при выполнении запроса выяснится, что адрес содержится в «черном списке» провайдера услуги, то высока вероятность того, что письмо представляет собой обычный спам. Некоторые провайдеры «черных списков» наряду со списками спаммеров отслеживают адреса, с которых происходит рассылка вирусов, «троянцев», сетевых «червей», программ несанкционированного удаленного управления и другого вредоносного контента. Обращение к службам динамических «черных списков» осуществляется через службу DNS для проверки, не содержатся ли в списках спаммеров адреса IP, перечисленные в заголовке письма (в поле адреса отправителя или адреса почтовых ретрансляторов в полях Received: в некоторых случаях наряду с адресами IP могут использоваться символьные имена [доменов](#)).

Замедление

Замедление получения писем с удаленного сервера, который подозревается в рассылке спама. Подозрения основываются на большом количестве адресатов в одном письме. Если это количество превышает установленный порог, то последующие получения с этого сервера начинают происходить с заданной задержкой.

SURBL фильтрация

SURBL фильтрация применяется для обнаружения спама на основе URL содержащихся в теле письма (проверка присутствия их в Black-листах). Модуль делает следующее: для каждого из URL, найденных в сообщении, извлекает [доменный](#) компонент (2-го или 3-го уровня), добавляет суффикс имени SURBL и выполняет DNS запрос на адрес SURBL сервера(ов). Пример работы:

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

Для [доменов](#), для которых необходимо проверять не два уровня [доменного](#) имени, а три, используется отдельный список - файл 2tld . Например, это актуально для виртуальных хостингов или же специальных зон для [доменов](#) третьего уровня, например [org.ru](#) или [pp.ru](#).

SpamAssassin

SpamAssassin - это расширяемый почтовый фильтр, используемый для идентификации спама. Полученные почтовые сообщения последовательно прогоняются через набор тестов. Каждый тест имеет некоторую «стоимость». Если сообщение успешно проходит тест, эта «стоимость» добавляется к общему балу. Стоимость может быть положительной или отрицательной, положительные значения называются «spam», отрицательные «ham». Сообщение проходит через все тесты, подсчитывается общий бал. Чем выше бал, тем больше вероятность, что сообщение является спамом.

У SpamAssassin'a есть настраиваемый порог, при превышении которого письмо будет классифицировано как спам. Обычно порог таков, что письмо должно подойти по нескольким критериям; срабатывание только одного теста недостаточно для превышения порога.

Commtouch

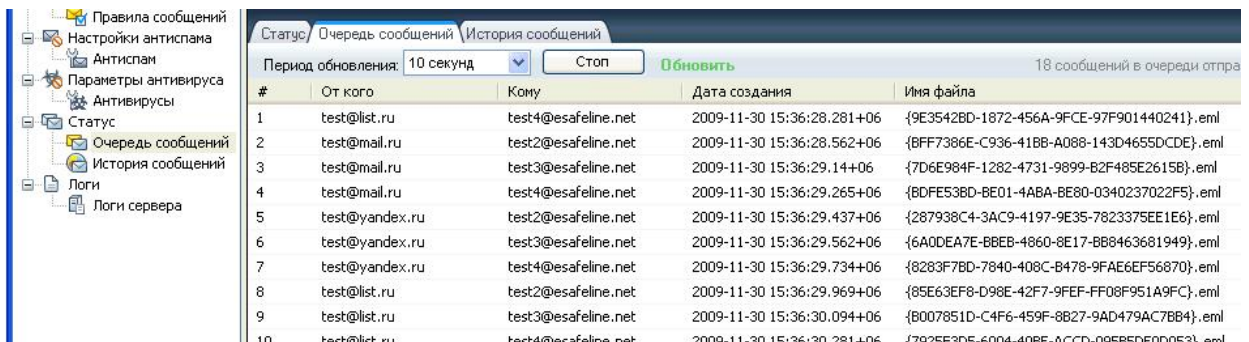
Commtouch's Anti-Spam Gateway - это запатентованное решение для защиты от спама систем для почтовых серверов и SMTP-шлюзов. Пакет компании Commtouch использует уникальный фильтр, основанный на фирменном алгоритме RPD (Recurrent-Pattern Detection), идентифицирующем спам по его основному признаку — по его распространенности. В отличие от многих производителей спам-фильтров компания Commtouch не обновляет базу данных типовых определений фильтров контента, ее продукт отыскивает паттерны в почтовом трафике.

Когда шлюз Anti-Spam Enterprise получает электронное сообщение, он пытается найти релевантное правило локальной политики, определенное либо для всего предприятия, либо для конкретных пользователей. Если сообщение не подходит ни под одно из правил, то ПО Commtouch начинает просматривать локальный кэш с ранее полученными из центра Anti-Spam Detection Center ответами. Если он по-прежнему не может найти какое-нибудь правило, соответствующее сообщению, то ПО шлюза запрашивает центр Anti-Spam Detection Center, размещаемый на территории компании Commtouch. Если центр недоступен, сообщение отправляется во входящий почтовый ящик пользователя.

Классифицировав сообщение как спам, шлюз принимает соответствующие меры, определенные администратором при его конфигурировании. Легитимное сообщение доставляется в почтовый ящик конечного пользователя.

Очередь сообщений

В разделе Message Queue отображается очередь почтовых сообщений сервера. Администратор почтового сервера может удалить какое – либо сообщение из очереди, остановить или снова запустить очередь сообщений. По умолчанию в очереди сообщений отображается 20 последних сообщений, обрабатываемых почтовым сервером.



#	От кого	Кому	Дата создания	Имя файла
1	test@list.ru	test4@esafeline.net	2009-11-30 15:36:28.281+06	{9E3542BD-1872-456A-9FCE-97F901440241}.eml
2	test@mail.ru	test2@esafeline.net	2009-11-30 15:36:28.562+06	{BFF7386E-C936-418B-A088-143D4655DCDE}.eml
3	test@mail.ru	test3@esafeline.net	2009-11-30 15:36:29.14+06	{7D6E984F-1282-4731-9899-B2F485E2615B}.eml
4	test@mail.ru	test4@esafeline.net	2009-11-30 15:36:29.265+06	{BDFE53BD-BE01-4ABA-BE80-0340237022F5}.eml
5	test@yandex.ru	test2@esafeline.net	2009-11-30 15:36:29.437+06	{287938C4-3AC9-4197-9E35-7823375EE1E6}.eml
6	test@yandex.ru	test3@esafeline.net	2009-11-30 15:36:29.562+06	{6A0DEA7E-BBEB-4860-8E17-BB8463681949}.eml
7	test@yandex.ru	test4@esafeline.net	2009-11-30 15:36:29.734+06	{8283F7BD-7840-408C-B478-9FAE6EF56870}.eml
8	test@list.ru	test2@esafeline.net	2009-11-30 15:36:29.969+06	{85E63EF8-D98E-42F7-9FEF-FF08F951A9FC}.eml
9	test@list.ru	test3@esafeline.net	2009-11-30 15:36:30.094+06	{B007851D-C4F6-459F-8B27-9AD479AC7BB4}.eml
10	test@mail.ru	test4@esafeline.net	2009-11-30 15:36:30.281+06	{7925F305-A004-408F-8C7D-09585D000053}.eml

Изображение 1, Очередь сообщений.

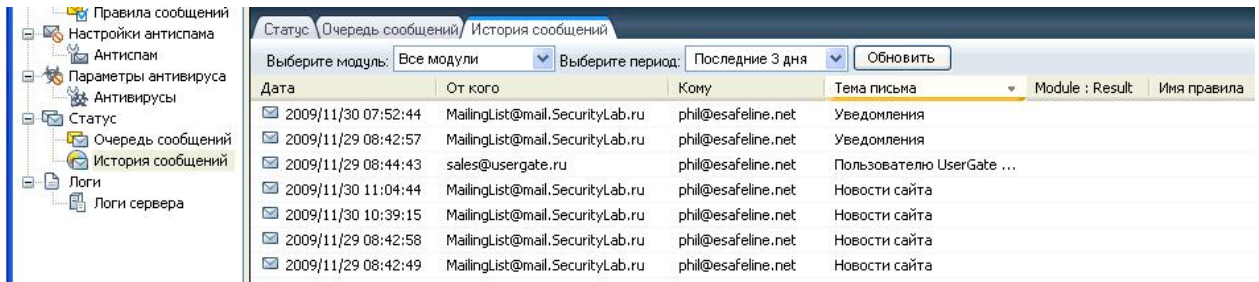
История сообщений

История сообщений отображает результат работы почтового сервера. На странице агрегирована вся полезная информация об электронных письмах обработанных почтовым сервером. Так же на этой странице содержится некоторая информация о работе Антиспам и Антивирусных модулей встроенных в почтовый сервер. Здесь можно увидеть когда сообщение было обработано, От кого и Куда направлялось, какими модулями было обработано.

Реализованна сортировка данных по Дате, Источнику, Назначению, Теме сообщения, или по отдельному модулю (Антиспам, Антивирус).

Дополнительно отображается информация о сработанных правилах для сообщений, т.е. когда сообщение было обработано правилом, это событие будет отображено на странице Истории сообщений.

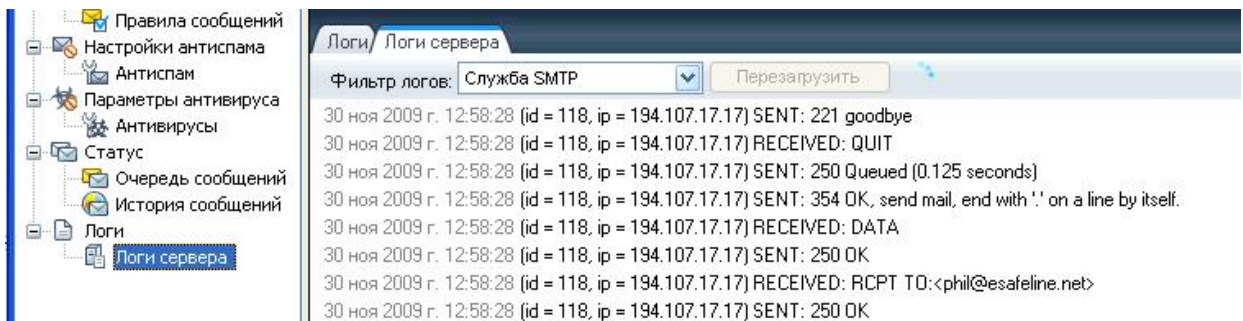
По замыслу страница истории сообщений служит главным помощником, и источником информации, об обработанных почтовым сервером писем. Помогает решить проблемы с доставкой писем при их возникновении. У каждого письма есть несколько действий, которые могут быть произведены над сообщением. Либо переслать сообщение адресату, либо добавить в список белых адресов (в следующей версии), если письмо было ошибочно детектировано как "спам", одним из Антиспам модулей.



Изображение 1, История сообщений.

Журнал сервера

Страница предназначена для отображения логов работы модулей почтового сервера, с возможностью фильтрации. Администратор почтового сервера может просматривать лог каждого отдельного модуля UserGate Mail Server.



Изображение 1, Логи сервера.