НАСТОЙКА МЕХАНИЗМОВ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕРВЕРОВ ЭЛЕКТРОННОЙ ПОЧТЫ

Безопасная настройка почтовой службы SMTP

E-mail сервер

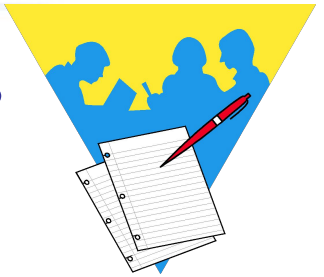
Безопасная настройка SMTP сервера

С точки зрения безопасности интерес представляют следующие возможности конфигурирования:

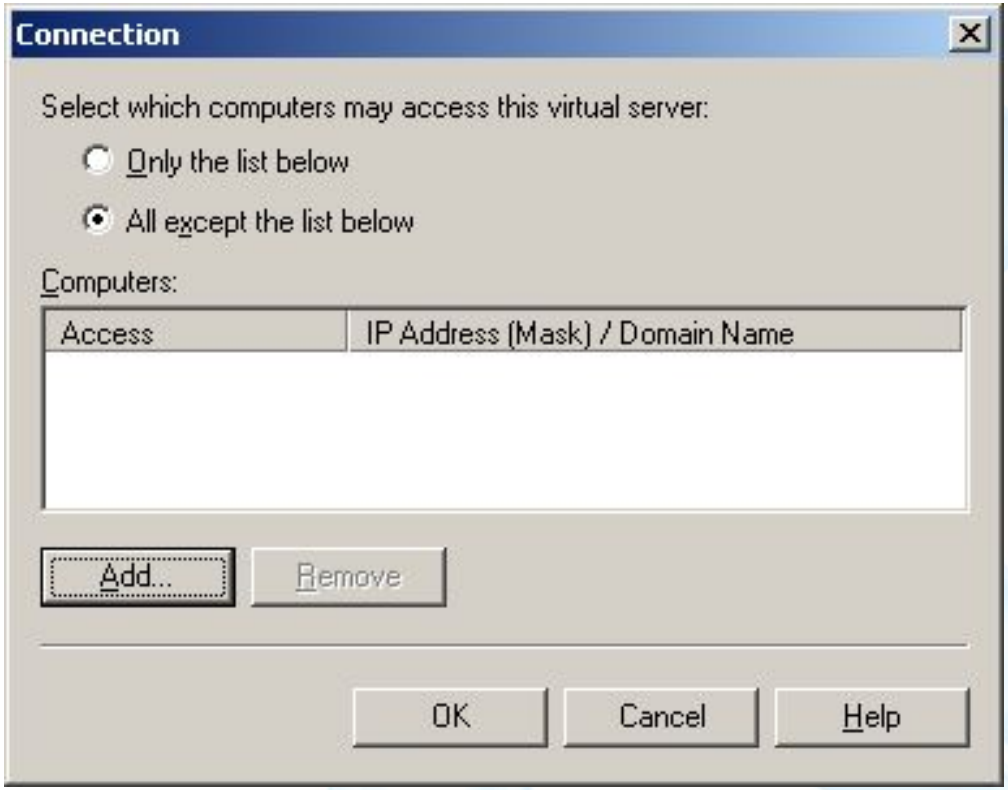
- Разграничение доступа к SMTP серверу в зависимости от IP-адресов хостов, сетей или имен доменов
- Настройка вариантов аутентификации на сервере SMTP
- Настройка ретрансляции почтовых сообщений через сервер
- Фильтрация сообщений по адресу отправителя
- Удаление информации о версии из заголовка службы SMTP
- Управление автоматической генерацией ответов
- Управление регистрацией событий в логах на сервере
- Введение ограничений на почтовые сообщения

Безопасная настройка SMTP сервера

Разграничение доступа к SMTP серверу в зависимости от IP-адресов хостов, сетей или имен доменов

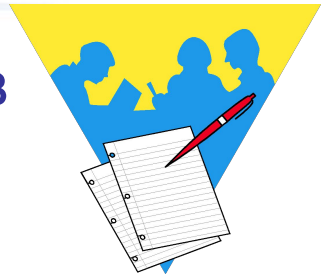


Эта возможность защищает от угрозы маскировки нарушителя под другого пользователя (клиента), когда нарушителю отказывают в обслуживании по SMTP по критерию почтового адреса отправителя.



Безопасная настройка SMTP сервера

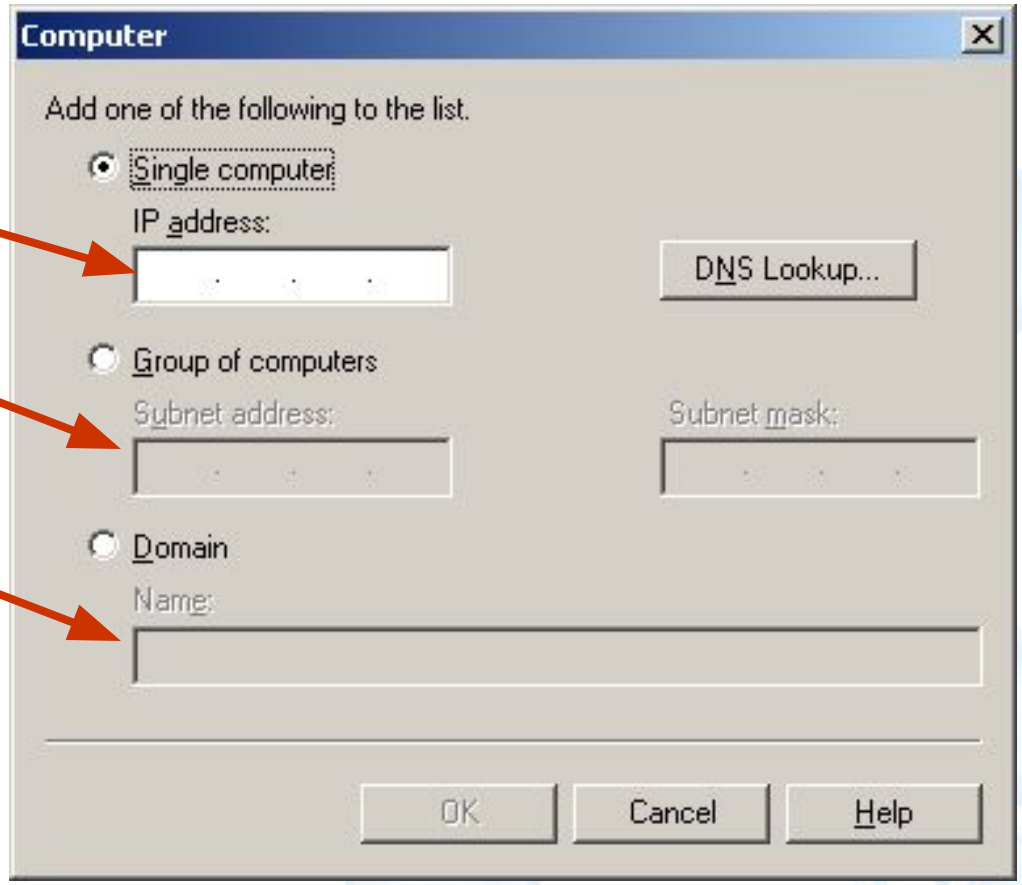
Разграничение доступа к SMTP серверу в зависимости от IP-адресов хостов, сетей или имен доменов



IP адрес узла

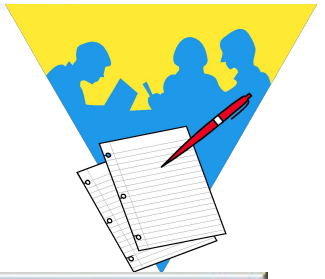
IP адрес и маска сети

Полное имя домена
(нужен обратный DNS)



Безопасная настройка SMTP сервера

Настройка вариантов аутентификации клиентов на SMTP сервере



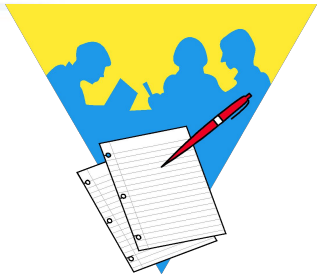
Анонимный доступ

Базовая аутентификация (имя и пароль в открытом виде)

Аутентификация по правилам Windows

Безопасная настройка SMTP сервера

Outbound security



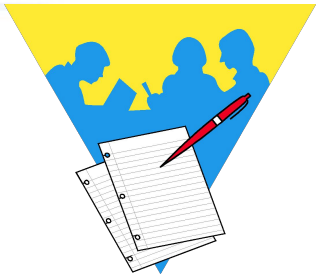
Анонимный доступ

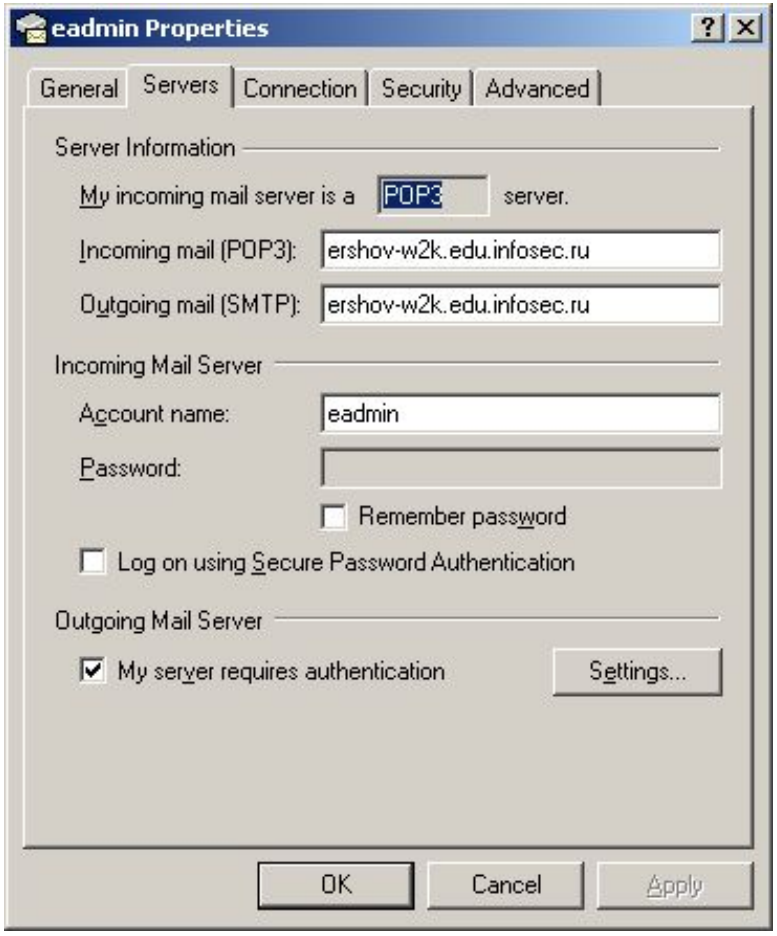
Базовая аутентификация (имя и пароль в открытом виде)

Аутентификация по правилам Windows

Безопасная настройка SMTP сервера

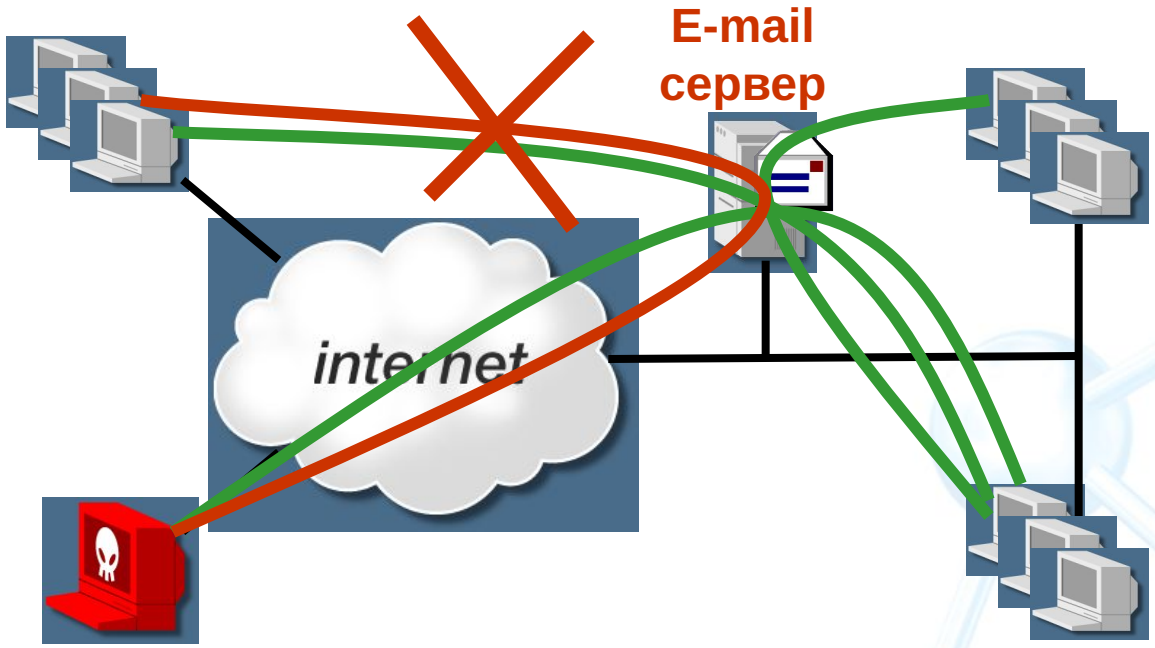
Выбор соответствующих вариантов аутентификации на клиенте





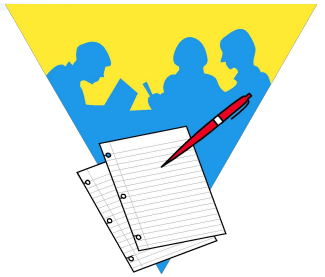
Безопасная настройка SMTP сервера

Настройка ретрансляции (RELAY) почтовых сообщений через сервер

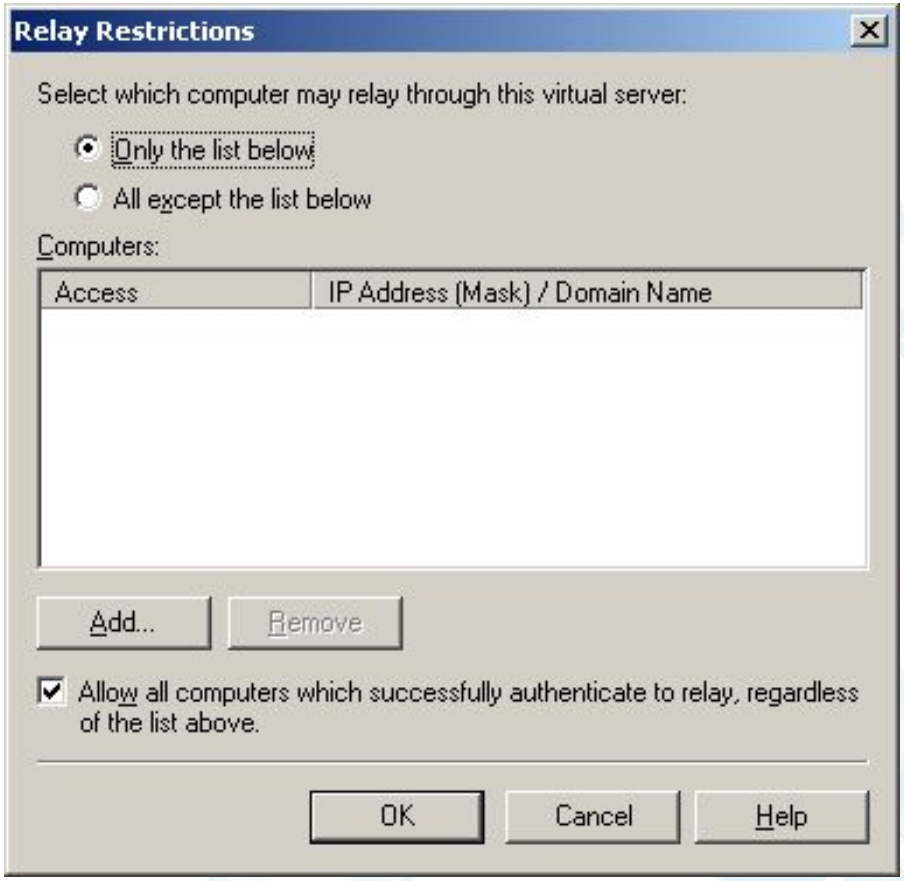


Безопасная настройка SMTP сервера

Настройка ретрансляции (RELAY) почтовых сообщений через сервер

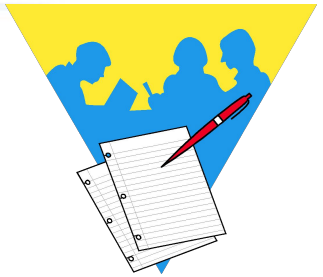


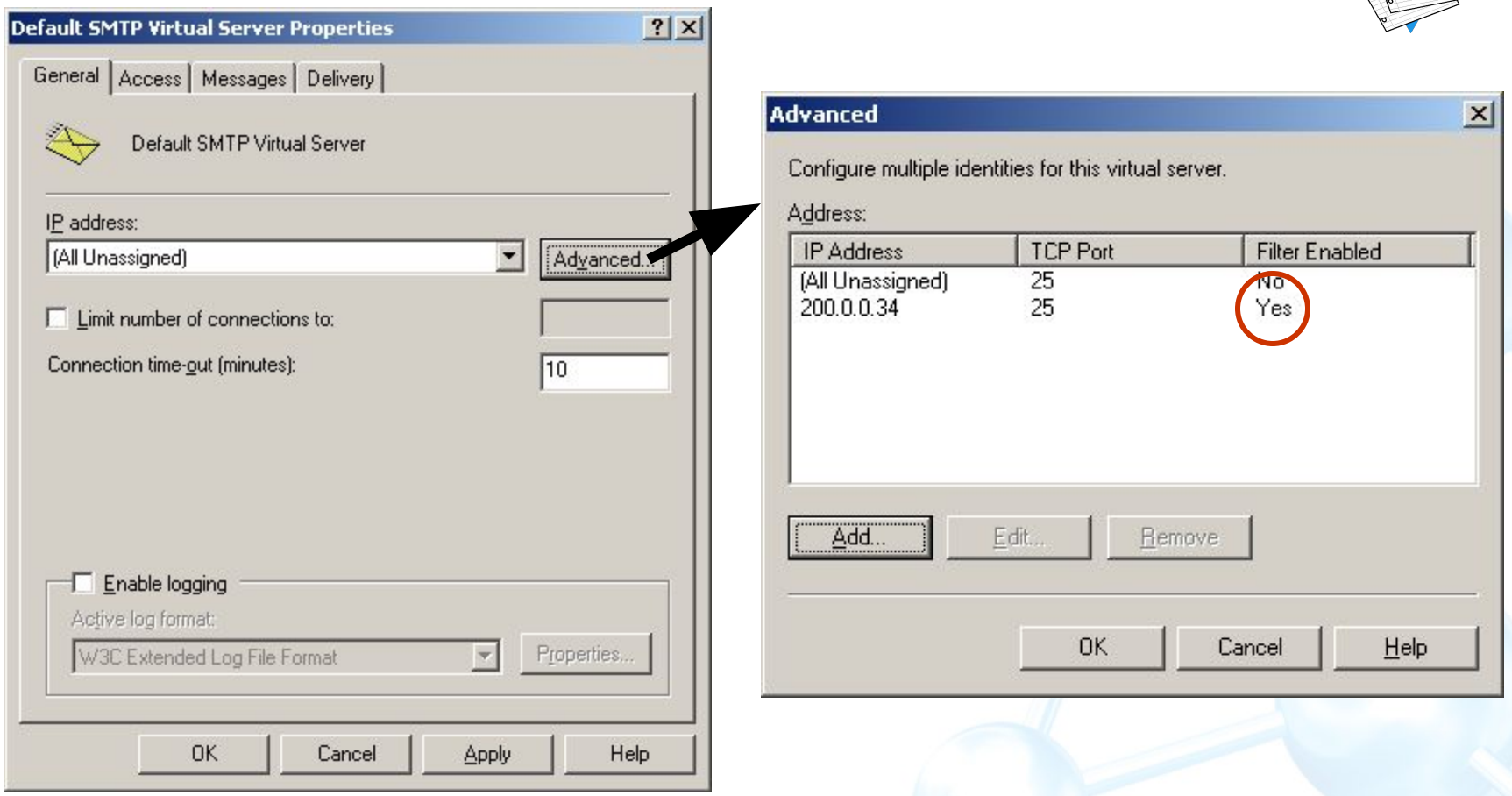
Для предотвращения использования сервера в целях рассылки спама следует выбрать вариант указания списка разрешенных отправителей, поскольку только вполне определенным внешним компьютерам необходимо предоставить возможность отправки сообщений с вашего сервера.



Безопасная настройка SMTP сервера

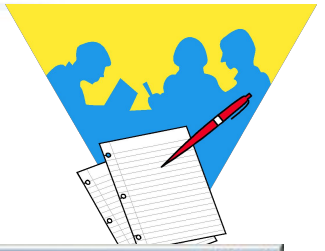
Фильтрация входящих сообщений по адресу отправителя



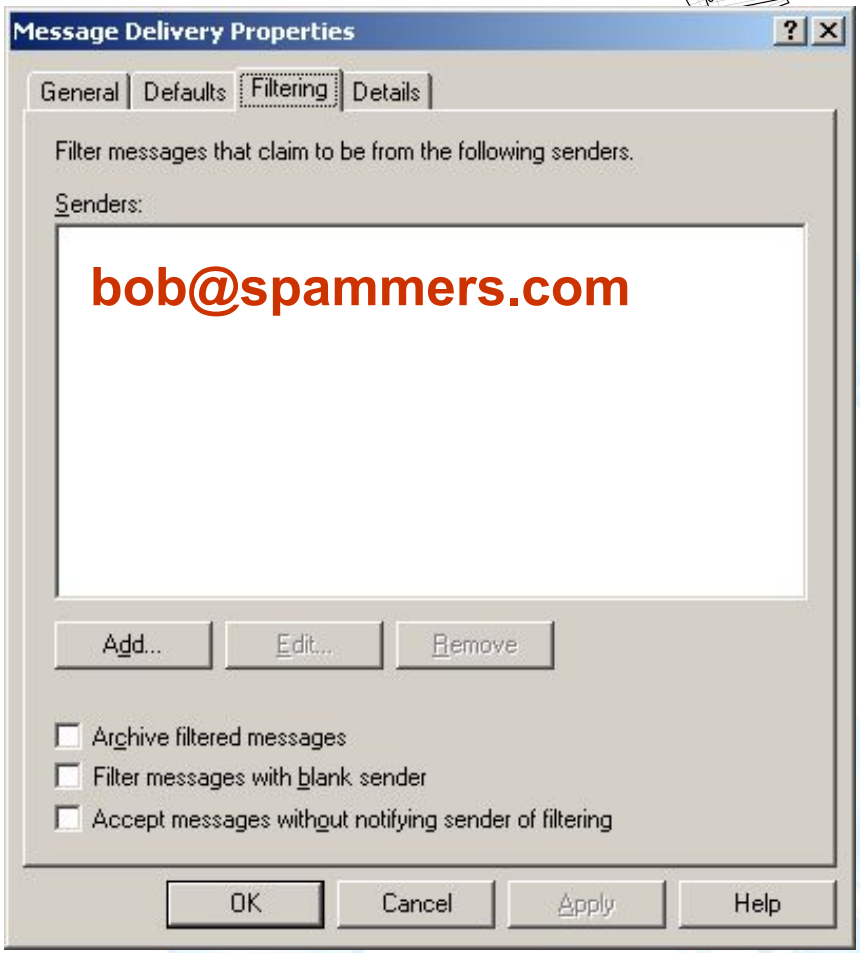


Безопасная настройка SMTP сервера

Фильтрация входящих сообщений по адресу отправителя

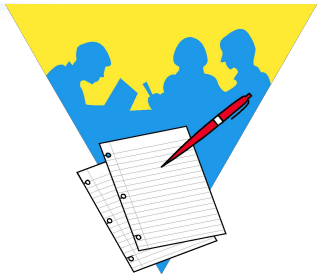


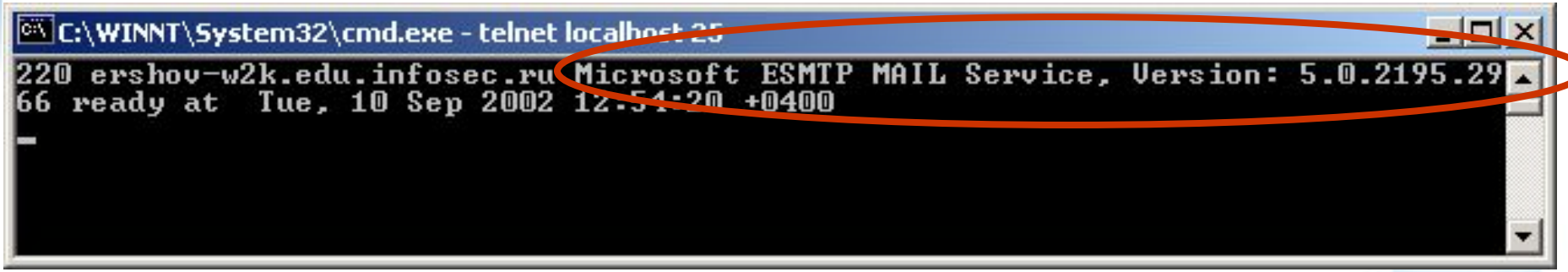
В контейнере Organization Global Settings > Message Delivery > закладка Filtering.



Безопасная настройка SMTP сервера

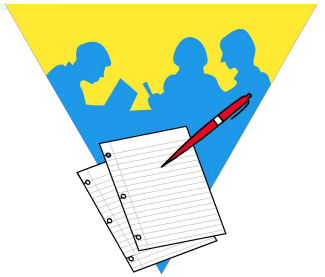
Удаление информации о версии из заголовка службы SMTP

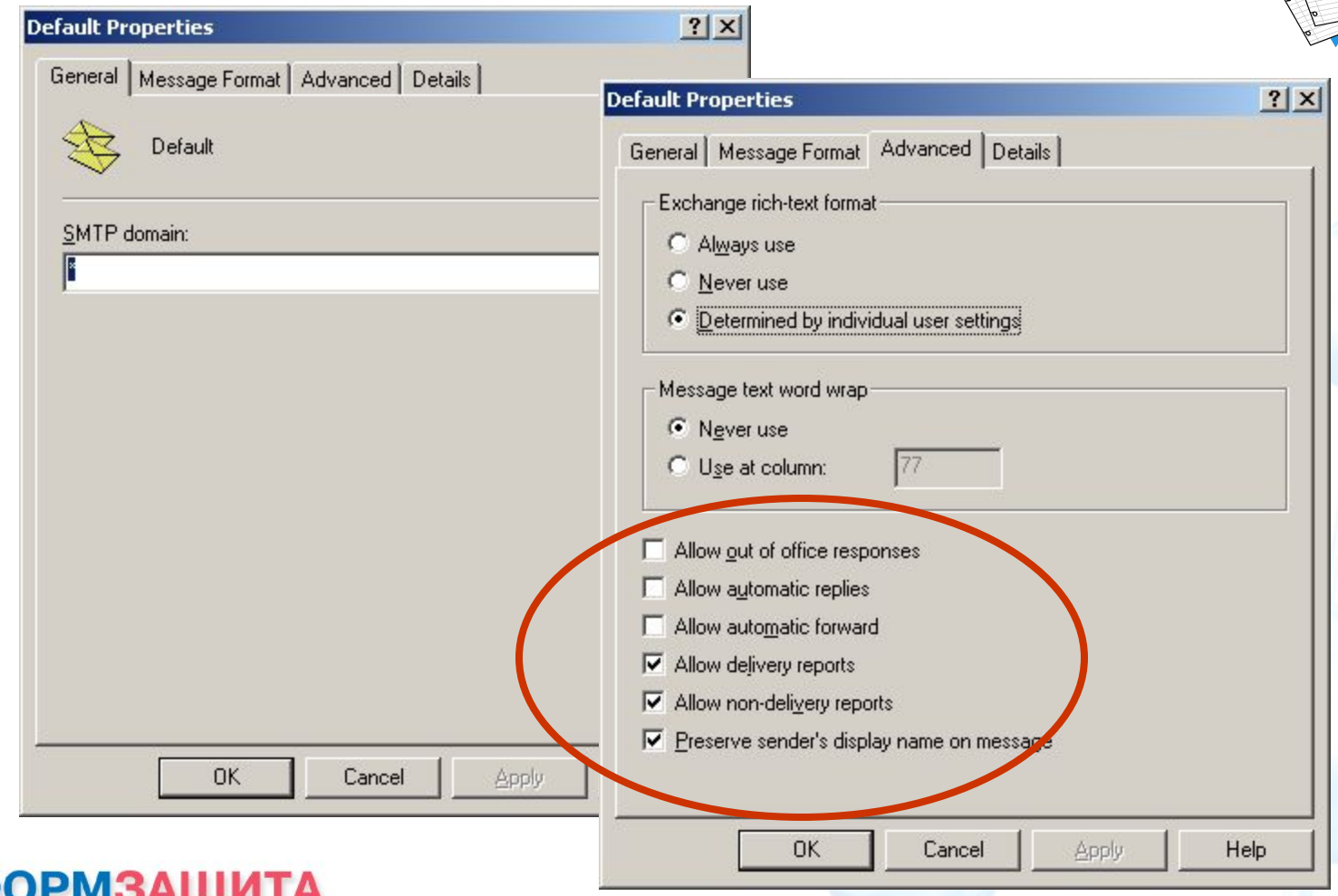




Безопасная настройка SMTP сервера

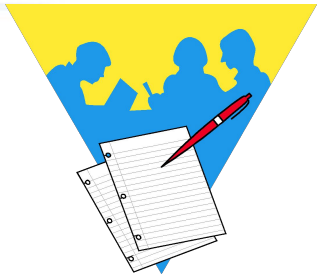
Управление автоматической генерацией ответов на почтовые сообщения

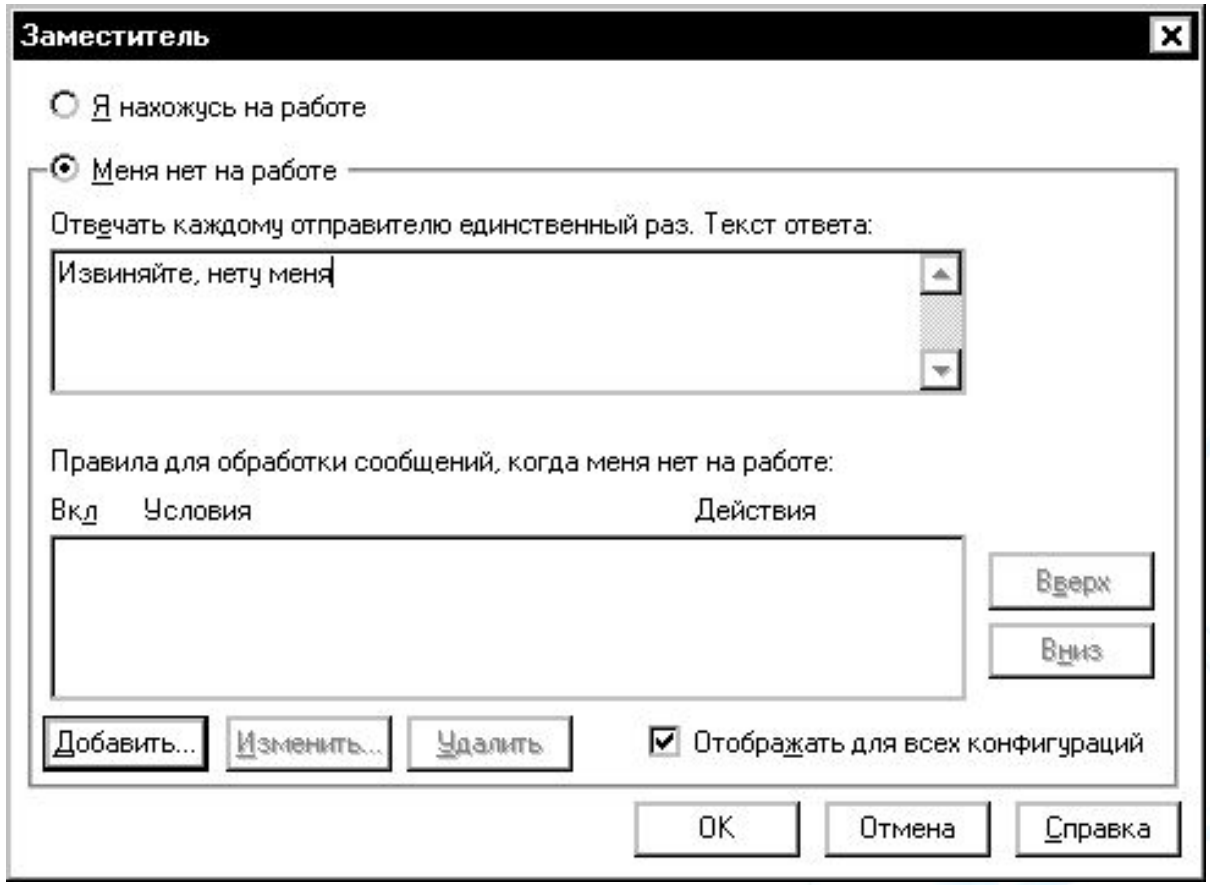




Безопасная настройка SMTP сервера

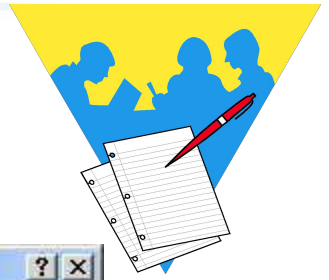
Управление автоматической генерацией ответов на почтовые сообщения





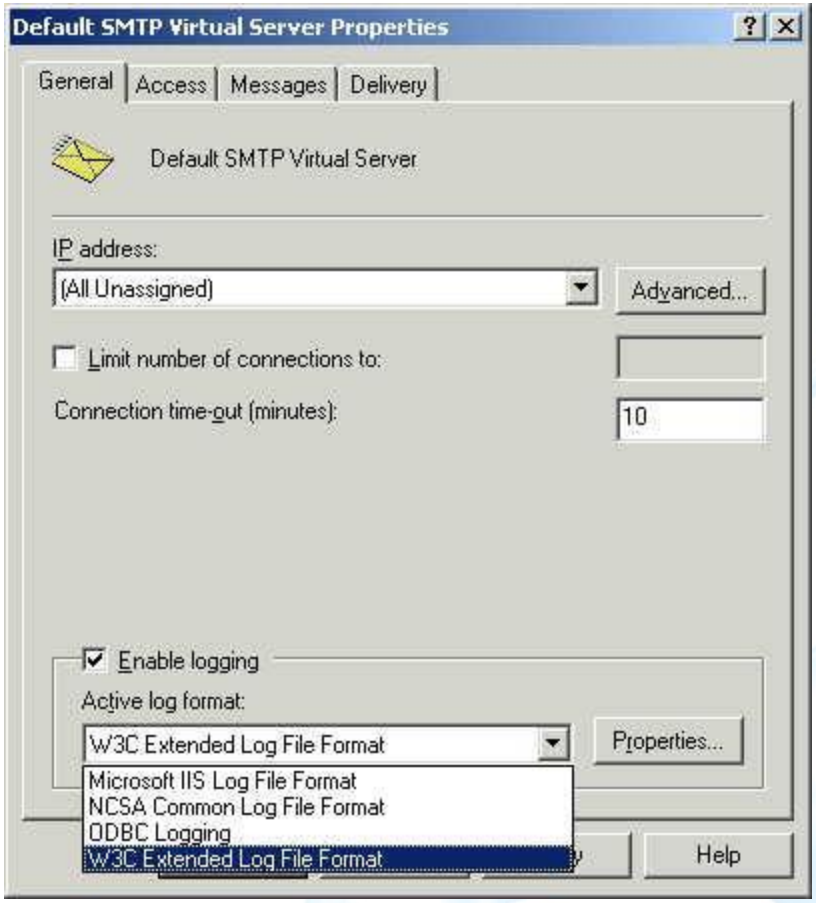
Безопасная настройка SMTP сервера

Управление регистрацией событий в лог-файлах на сервере



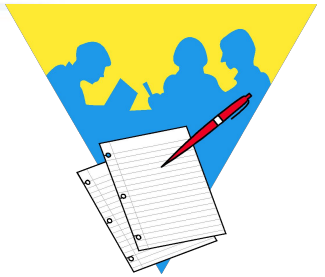
Журналы сохраняются в файлах либо в базе данных ODBC

Три типа текстовых журналов



Безопасная настройка SMTP сервера

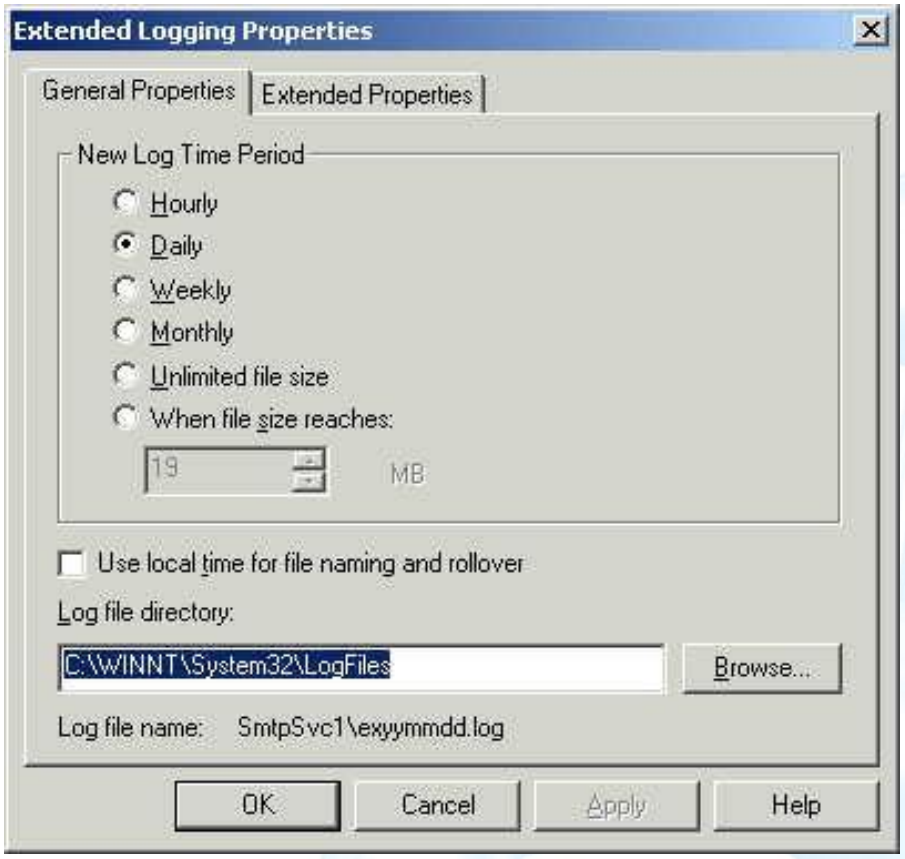
Управление регистрацией событий в лог-файлах на сервере



Параметры обработки

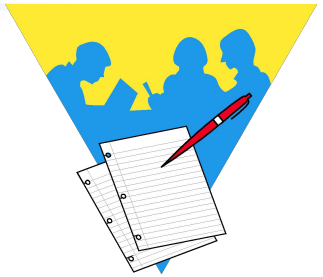
Место хранения журналов

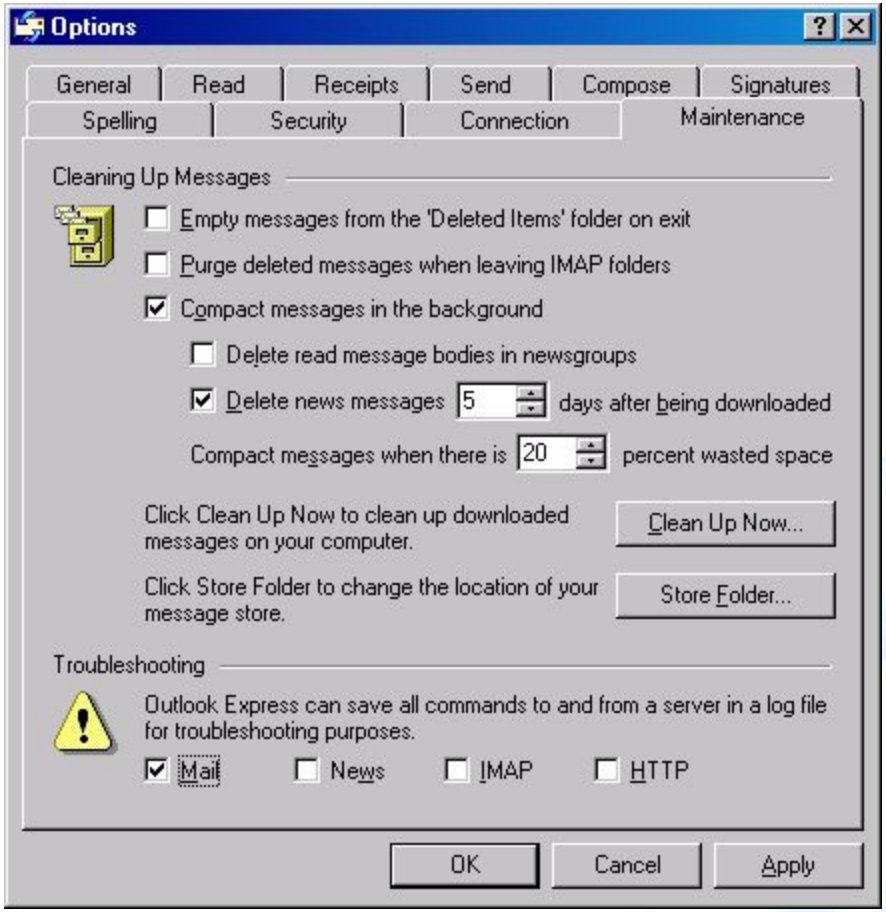
Поля, сохраняемые в журналах



Безопасная настройка SMTP сервера

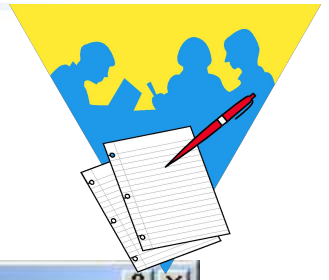
Управление регистрацией событий в лог-файлах на клиентах





Безопасная настройка SMTP сервера

Введение ограничений на почтовые сообщения

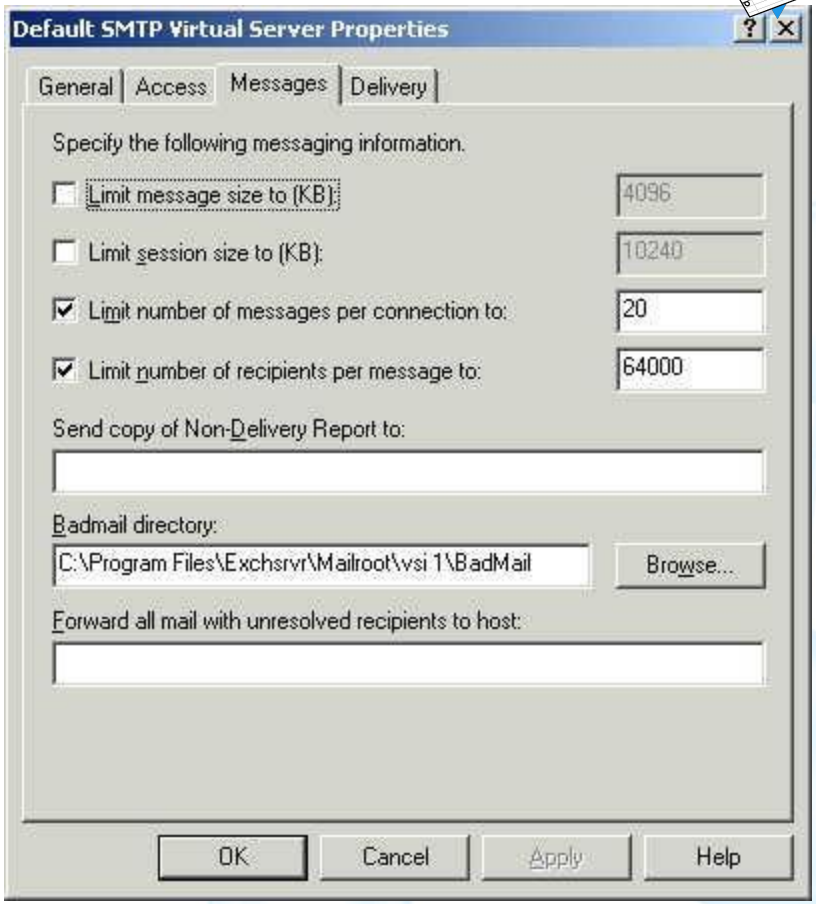


Максимальный размер сообщения

Максимальный размер сессии

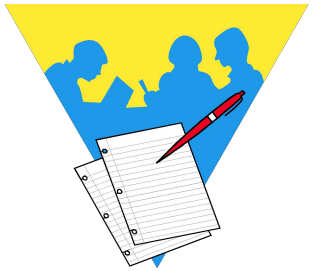
Максимальное количество сообщений в сессии

Максимальное количество получателей сообщения



Практическая работа 10

Безопасная настройка SMTP сервера



Безопасная настройка почтовой службы POP3

E-mail сервер

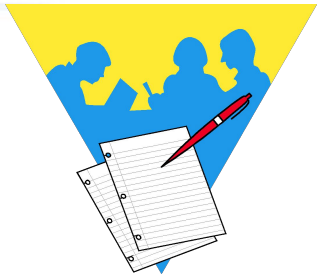
Безопасная настройка POP3 сервера

С точки зрения безопасности интерес представляют следующие возможности конфигурирования:

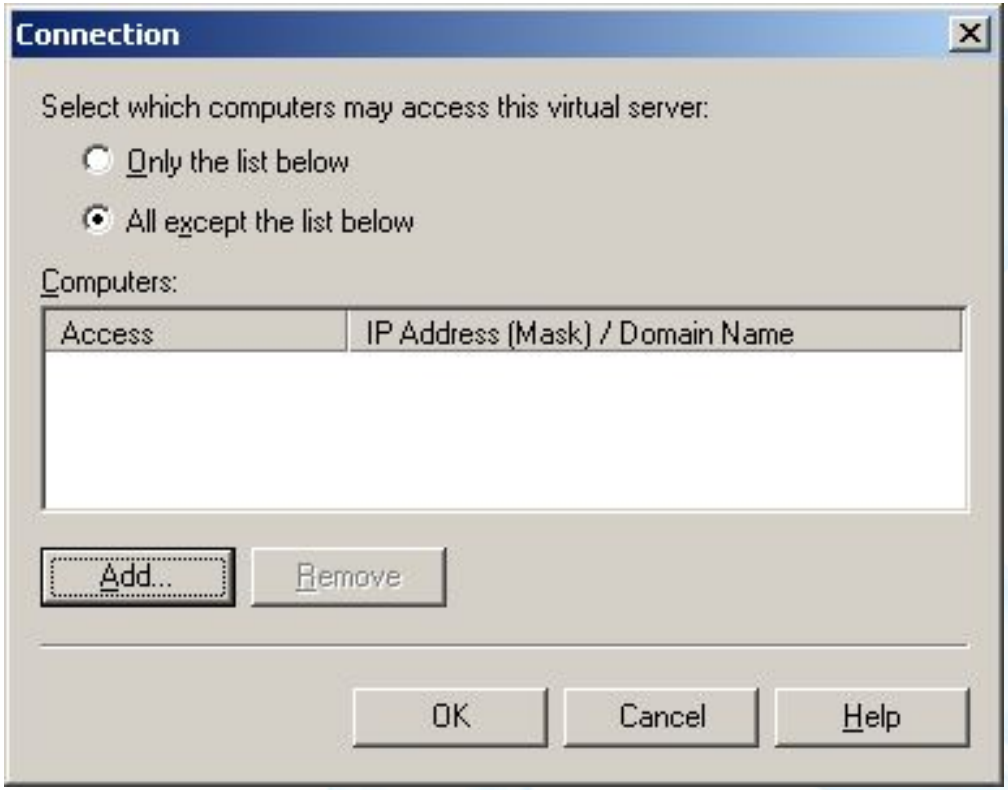
- Разграничение доступа к POP3 серверу в зависимости от IP-адресов хостов, сетей или имен доменов
- Настройка вариантов аутентификации на сервере POP3
- Удаление информации о версии из заголовка и хвостовика службы POP3
- Управление регистрацией событий в логах на сервере

Безопасная настройка POP3 сервера

Разграничение доступа к POP3 серверу в зависимости от IP-адресов хостов, сетей или имен доменов

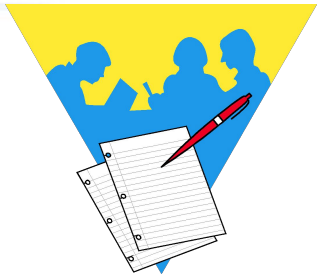


Ограничивает круг лиц, которые могут соединится с сервером. Поскольку сервер POP используется для получения почты, диапазон адресов обычно известен. Защита от взлома из «чужой» сети.



Безопасная настройка POP3 сервера

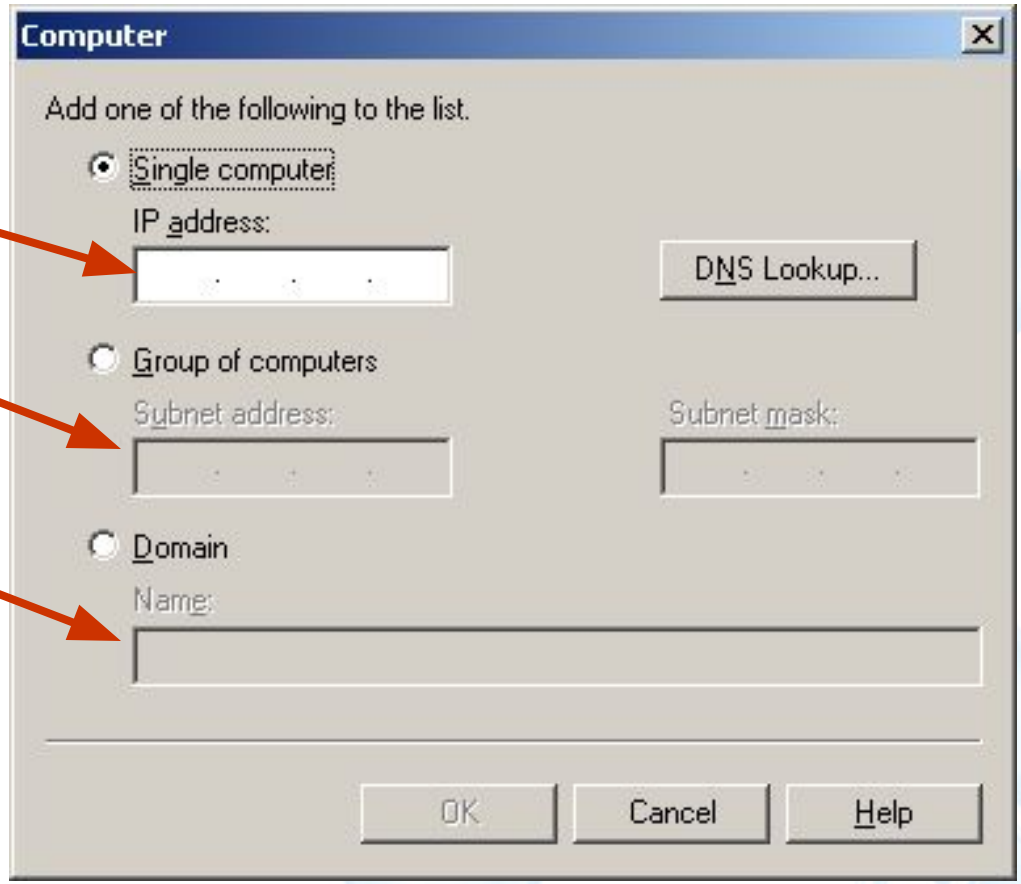
Разграничение доступа к POP3 серверу в зависимости от IP-адресов хостов, сетей или имен доменов



IP адрес узла

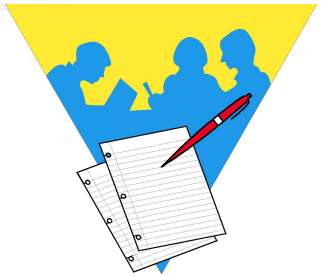
IP адрес и маска сети

Полное имя домена
(нужен обратный DNS)



Безопасная настройка POP3 сервера

Настройка вариантов аутентификации клиентов на POP3 сервере

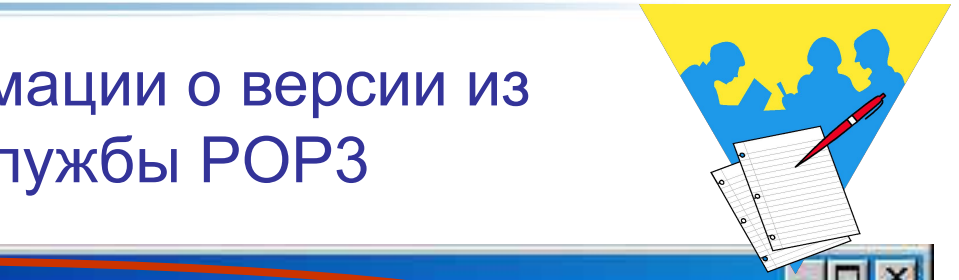


Базовая аутентификация (имя и пароль в открытом виде)

Аутентификация по правилам Windows (NTLM)

Безопасная настройка POP3 сервера

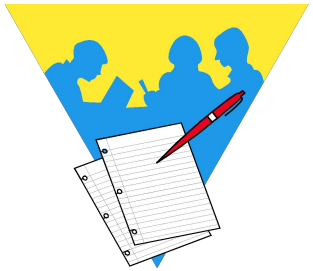
Удаление информации о версии из заголовка службы POP3



```
C:\WINNT\System32\cmd.exe
+OK Microsoft Exchange 2000 POP3 server ready.
user user1
+OK
pass 1111
+OK User successfully logged on.
stat
+OK 3 7138
retr 1
+OK
Received: from w2kas ([200.1.1.100]) by w2kas.dom.isec with Microsoft SMTPSVC(5.
0.2195.5329);
quit
+OK Microsoft Exchange 2000 POP3 server version 6.0.6249.0 signing off.
```

Практическая работа 11

Безопасная настройка POP3 сервера



Безопасная настройка почтовой службы IMAP4

E-mail сервер

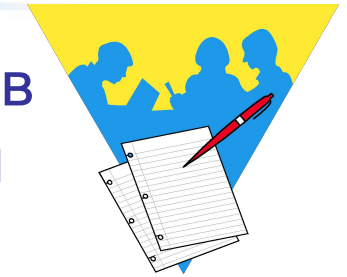
Безопасная настройка IMAP4 сервера

С точки зрения безопасности интерес представляют следующие возможности конфигурирования:

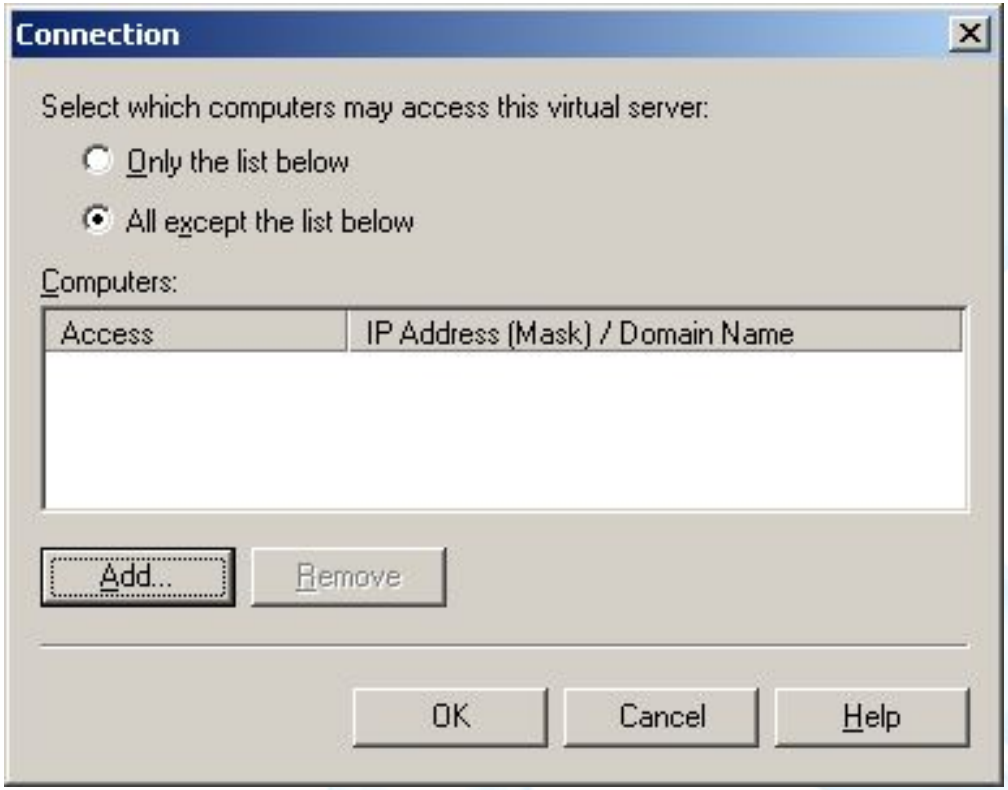
- Разграничение доступа к IMAP4 серверу в зависимости от IP-адресов хостов, сетей или имен доменов
- Настройка вариантов аутентификации на сервере IMAP4
- Удаление информации о версии из заголовка и хвостовика службы IMAP4
- Управление регистрацией событий в логах на сервере

Безопасная настройка IMAP4 сервера

Разграничение доступа к IMAP4 серверу в зависимости от IP-адресов хостов, сетей или имен доменов

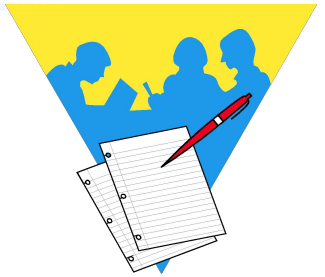


Ограничивает круг лиц, которые могут соединится с сервером. Поскольку сервер IMAP4 используется для получения почты, диапазон адресов обычно известен. Защита от взлома из «чужой» сети.



Безопасная настройка IMAP4 сервера

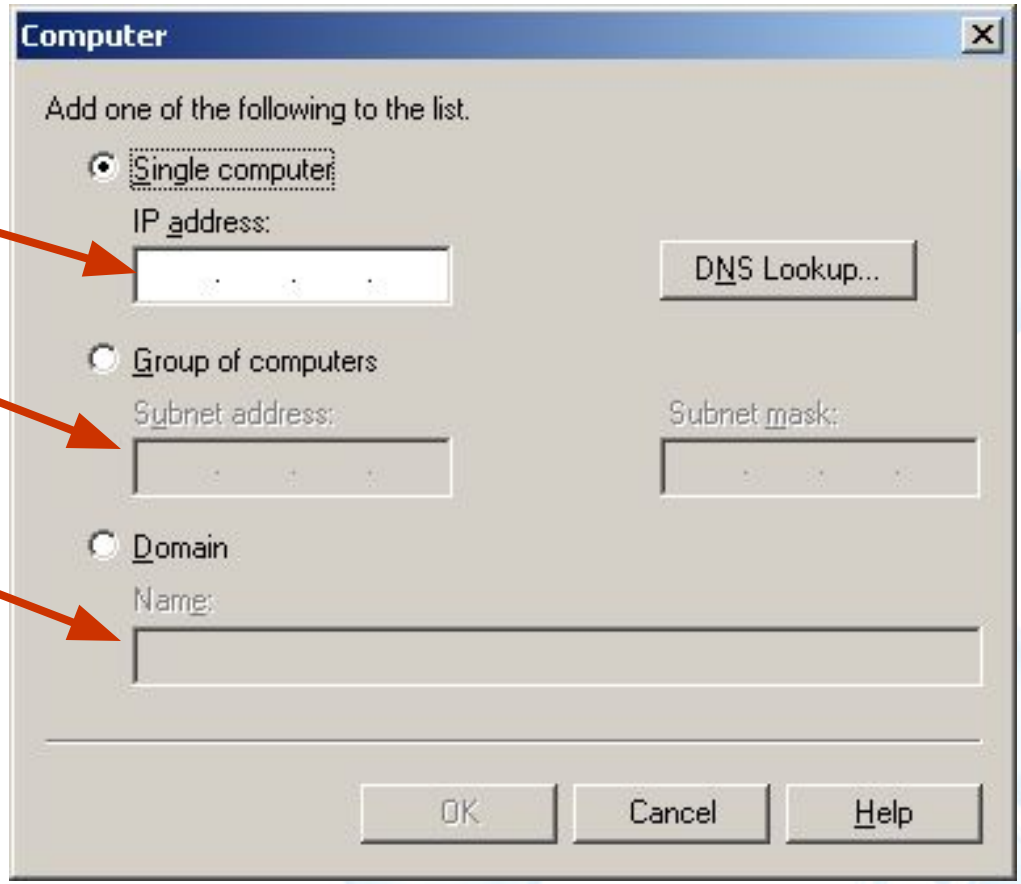
Разграничение доступа к IMAP4 серверу в зависимости от IP-адресов хостов, сетей или имен доменов



IP адрес узла

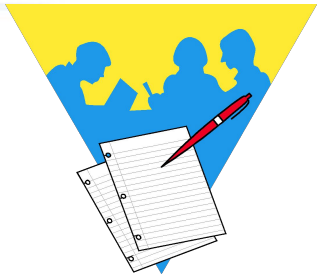
IP адрес и маска сети

Полное имя домена
(нужен обратный DNS)



Безопасная настройка IMAP4 сервера

Настройка вариантов аутентификации клиентов на IMAP4 сервере

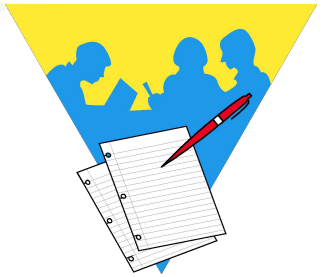


Базовая аутентификация (имя и пароль в открытом виде)

Аутентификация по правилам Windows (NTLM)

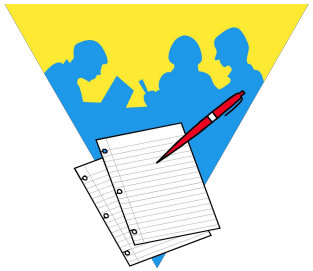
Безопасная настройка IMAP4 сервера

Удаление информации о версии из заголовка службы IMAP4



Практическая работа 12

Изменение заголовков служб POP3 и IMAP4



Вопросы ?