BatPost

Administrator's Manual

General Information about the Server

Currently, the server supports the following protocols: SMTP and POP3. IMAP protocol support will be added later. Data structure was developed for operation through all the three protocols. Default data storage directory is DB.

Structure of the Directories

The working directory of the program contains the following files:

- BatPost.exe — the server proper
- BatPostC.exe — server configuration module
- BatPostM.exe — server monitoring module
- HaltNtfy.exe — module used to inform administrator of critical errors when the log-keeping subsystem is inoperable
- Server.ini — file with server settings

And the following subdirectories:

- DB — the server database where the information about groups, domains, users, folders, messages, as well as rules, blacklists and acceptlists is stored.
- Drivers — subdirectory used to store data access drivers.
- Logs — subdirectory used to store the server logs
  - ERROR.LOG — this log keeps information about errors occurred during the server operation. Entries appearing in this file are of great importance, as they may indicate to inner problems of the server. Inform the developer of any unusual entries appearing in the log.
  - POP.LOG — log for operation through the POP3 protocol
  - POST.LOG — message sending log
  - Session.LOG — all the data received through SMTP and POP3 protocols are written to this log (except messages themselves, to avid disk space wasting)
  - SMTP.LOG — log for operation through the SMTP protocol
  - DrvErr.LOG — log for data access driver errors
  - AppErr.LOG — application error log
  - BatPostLog.mdb — MS Access database used to store the logs. Provides for compiling any desired samples and convenient log analysis.
- Spool — server spool. Used for temporary storage of messages and message queue status information (until they are written to the relevant database or sent out).

User Data Structure on the Server

By user data we mean data directly related to mail server operation and visible from the outside (groups, domains, users, folders, messages).

The data structure can be presented as a tree: the upper level (the root) contains domains (domains.cfg), and domains contain users (users.cfg). Each user has a folder tree (folders.cfg). Folders contain messages.
Groups (groups.cfg) are used to manage user privileges. Each user can be included into several groups. So, it is possible to specify for each folder what privileges each group in that folder has. User privileges are only sensible for IMAP, so this with the other two protocols this information is ignored.

Default name of the subdirectory used to store all the information about a domain is similar to the domain name.

Default name of the subdirectory used to store all the information about a user is similar to the user name.

Auxiliary message information is stored in files named “xxxxxxxx.cfg”, where x is a hexadecimal number. Message text is stored in file with the same name, but the extension is “lfr”. Separate message database is used for each folder.

Auxiliary Data Structure on the Server

By auxiliary data we mean data used to organize internal operation of the server that cannot be seen from outside (rules, blacklists and acceptlists).

- ruleset1.cfg — rules for IP-addresses and hosts
- ruleset2.cfg — rules for mail address received through MAIL FROM and RCPT TO
- IP_BL.cfg — blacklist for IP-addresses
- Host_BL.cfg — blacklist for host names
- Addr_BL.cfg — blacklist for mail addresses from MAIL FROM
- IP_AL.cfg — acceptlist for IP-addresses

- Host_BL.cfg — acceptlist for host names
- Addr_BL.cfg — acceptlist for mail addresses from MAIL FROM

To for flexible management of permitting and prohibiting of varied actions, the priorities from 0 to 3 are introduced in addition to the notions Enable, Disable. When priority values are different, the greater one prevails. When priorities are equal, Disable has the preference. So, we have the following sequence with ascending priority: Enable 0, Disable 0, Enable 1, Disable 1, Enable 2, Disable 2, Enable 3, Disable 3. Hereinafter such values are referred to as flags.

Once connection is established IP-address and host name are processed ruleset1. After that, the system checks whether connection via that protocol is permitted, and if it is not, the negative return code is sent back and the channel is closed. Besides, IP-address and host name are checked by relevant blacklists and acceptlists. Thus, the result is determined by a combination of default flags, flags for each match in ruleset1, and flags used with blacklist and acceptlist.

All further checks are done only for the SMTP protocol.

Once a sender's address is received (through MAIL FROM) it is processed by the ruleset2 and checked by relevant blacklist and acceptlist. Besides, the address is checked for belonging to the server. If so, the final result may be combined with additional flags. If no operations are permitted, the negative return code is sent back.

Recipient addresses (RCPT TO) are processed by the ruleset2 upon receipt. Depending on whether the recipient is local or remote, the messages are checked for permission to be added to the local databases or for permission of relay, and if there is no permission, the negative return code is sent back.

The settings also specify if previous calculation results are to be used for flag calculation. Depending on this, the decision on sending the negative response is taken, as any negative flags except Disable 3 can be "redeemed" into positive.

Initial Setting of the Rules

Since relay is prohibited by default, it is necessary to add entries permitting it to desired users into the Ruleset 1 (Database|Rule sets/BL/AL…). This can be done in several ways:

- Using regular expression describing the relevant sub-network
- Using regular expression describing host names for which relay is permitted
- Using individual rules for each of the hosts relay is permitted from

Mail-Lists and Aliases

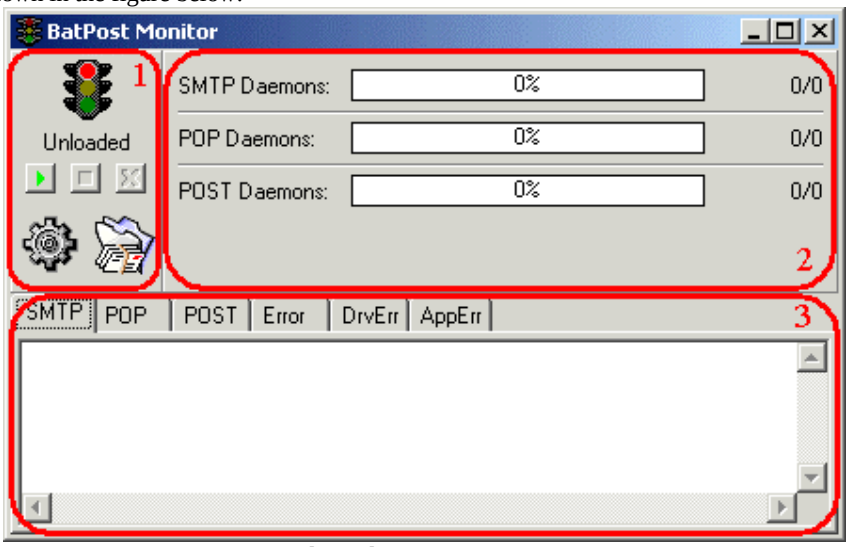
Both mail-lists and aliases use one and the same format: a list of lines, one mail address in each line. Empty lines and lines beginning with “#” are ignored.

Lines beginning with “$” are called directives. The following directives are possible:

- `$include` filename — include addresses from file

Monitor

The monitor module is used to control the server operation, watch its activity, and view logs. The monitor appearance is shown in the figure below:



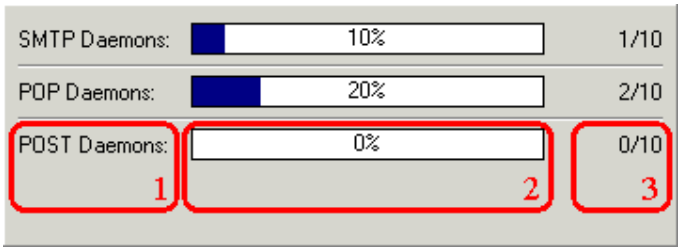
1. Server control panel
2. Server activity panel
3. Log viewing panel

Server Control Panel

1. The red light means that the server is unloaded from memory. Yellow means it is loaded into the memory and stopped. Green means that server is loaded into the memory and working.
2. Shows the same information as the element 1 does, but in the text form. Respectively: Unloaded, Stopped and Started.
3. Server start button. If the server is not loaded into the memory, it will be loaded and started. If the server was stopped, it will be started again.
4. Server stop button. The server will stop working, but remain in the memory.

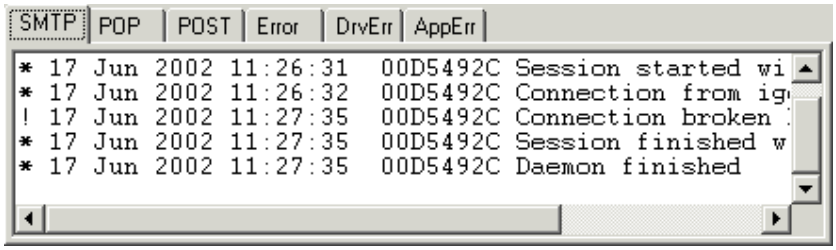
5. Server unload button. If the server is working, it will be stopped and unloaded from the memory. If the server is stopped, it will be unloaded from memory.
6. Open the configurator. Click on this button will launch the configurator module.
7. Open the Spool Monitor. Click on this button will open the form used to monitor messages currently in the spool.

Server Activity Panel



1. Daemon type
2. Percent of the server load by that daemon type
3. Active_daemon_number/Maximum_daemon_number

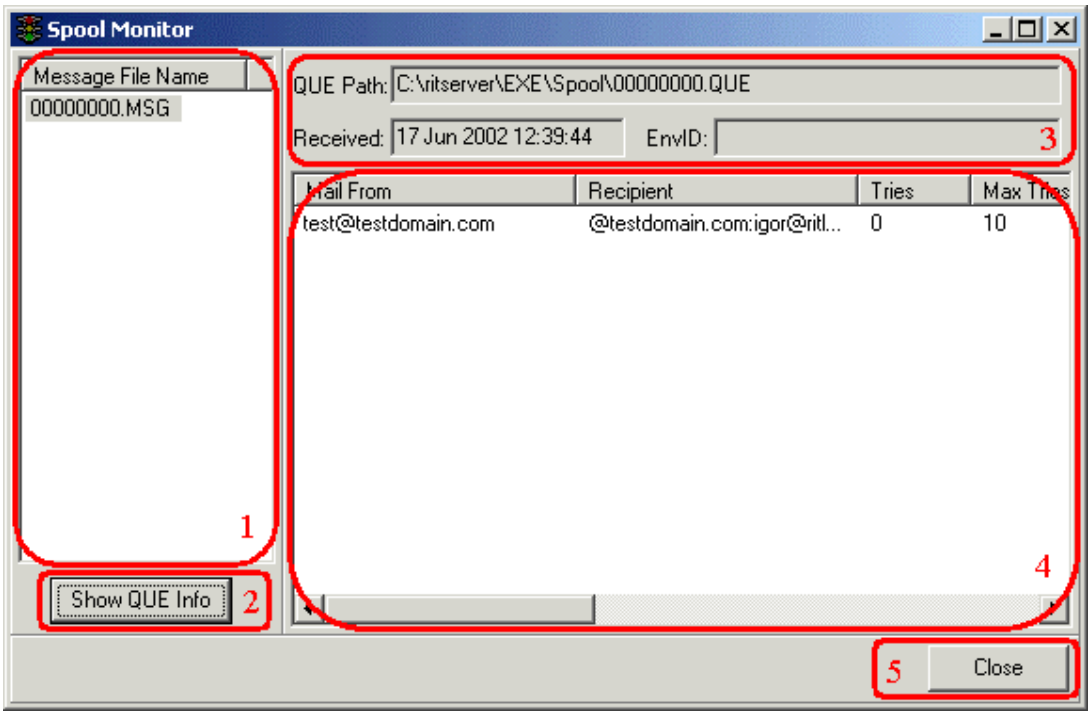
Log Viewing Panel



This panel is used to view event logs from the following files: SMTP.LOG, POP.LOG, POST.LOG, ERROR.LOG, DrvErr.LOG, and AppErr.LOG. Since log size may easily be up to tens and even hundreds of MB on a rather heavily used server, only the recent entries are displayed (a few hundreds) to save the memory space.

Spool Monitor

Message texts are stored in *.MSG files. Auxiliary information about the message is stored in a *.QUE file which name is similar to name of the file with the relevant message.

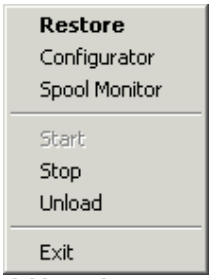


1. Message file list
2. Button used to display the auxiliary information for selected message. Since the spool has to be blocked while auxiliary information is being viewed, which may have negative effect on operation rate of the server, it was decided not to display the auxiliary information automatically but to show it on manual request.
3. Auxiliary information about a message in general
   - QUE Path — specification of the file which contains the auxiliary information
   - Received — date and time of the message receipt on the server
   - EnvID — the identifier line used in the extended SMTP protocol
4. Auxiliary information about each of the destination addresses
   - Mail From — message sender address
   - Recipient — message recipient address
   - Tries — number of attempts to send the message done
   - Max Tries — maximum possible number of attempts to send the message
   - Last Try — date and time of the last attempt to send the message
   - Next Try — date and time of the next attempt to send the message
   - Flags — flags (for internal use)
   - Last Error — text message about the last error
   - Original Recipient — original message recipient. Used in the extended SMTP protocol
   - Action — the action done with the address in the last send attempt (DSN extension rfc1894)
     - None — no complete sending attempts so far
     - Failed — the message cannot to delivered to the recipient. Every attempt taken to send the message failed
     - Delayed — there was an unsuccessful delivery attempt, but the server will keep trying to deliver the message
     - Delivered — the message has been delivered to a local recipient
     - Relayed — the message has been relayed for delivery to a remote recipient
     - Expanded — the alias list behind the address has been successfully expanded
   - Status — the text code of message delivery status (DSN extension rfc1894)
5. Spool monitor close button

The Tray Icon

For more convenient operation, the monitor puts its icon into the system tray:

Meaning of the traffic light signals is the same as in the main window of the monitor. Right-clicking the tray icon opens the context menu:

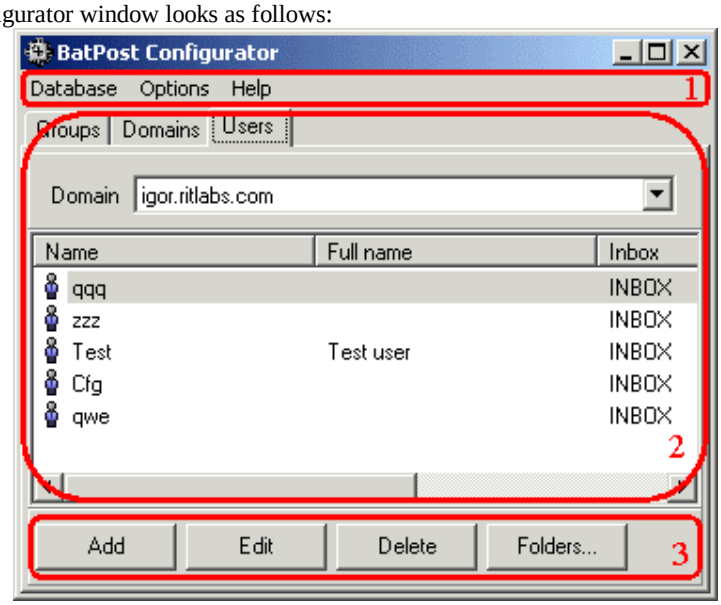


which can be used to access some functions available in the main window of the monitor: start, stop, and unload the server from the memory; launch of the configurator; open the spool monitor and exit and monitor module.

The Configurator

The configurator module is used to change server settings. Changes in some settings only take effect after relaunch of the server, while changes in other settings don't require server relaunch. Any changes in the “Options” window require the server to be relaunched. Changes related to domains may also require relaunch. Always relaunch the server if you are not sure the change you have made to the settings don't require that.

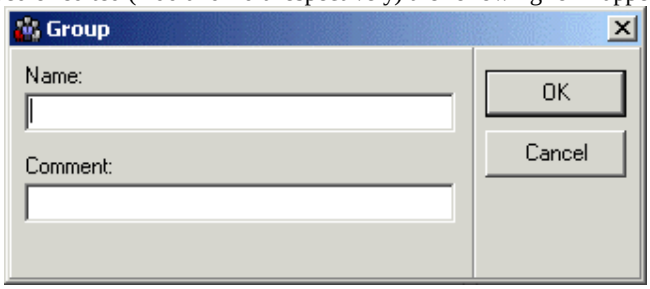
The main configurator window looks as follows:



1. The configurator module main menu
2. Group, domain, and user lists. With users there is the additional control for choosing the domain which users are of interest to us.
3. The buttons used to add (Add), modify (Edit) and delete (Delete) entities. On the Users tab there is the additional button “Folders…” used to edit the user folders.

Groups

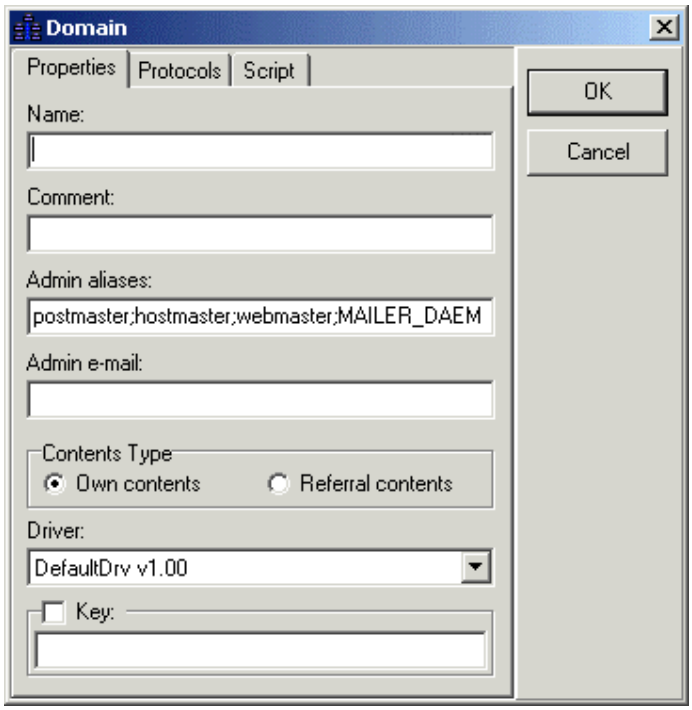
User groups are used by the IMAP protocol to specify user privileges in each particular folder. A user may be a member of several groups simultaneously and have respective privileges to perform certain actions in a folder. When a group is being added or edited (Add and Edit respectively) the following form appears:



where the group name is to be entered into the “Name” field and comment into the “Comment” field. To save the changes click “OK”, to quit without saving – “Cancel”.

Domains

By domains we mean names of the host the server will receive mail for. When a domain is being added or edited (Add and Edit respectively) the following form appears:

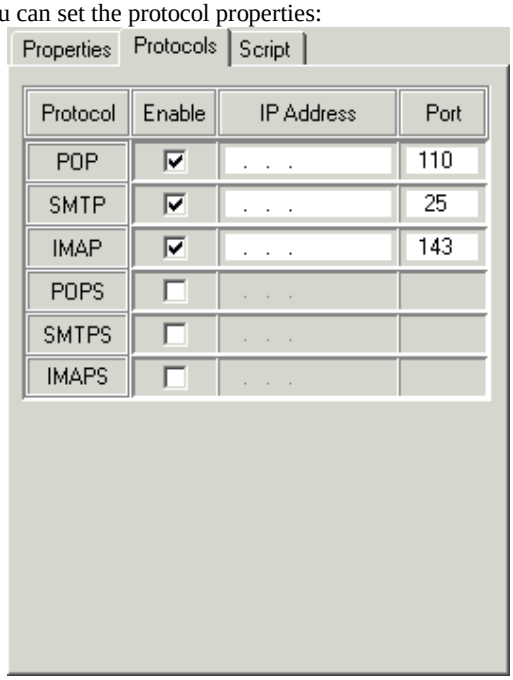


name

- Name — domain name
- Comment — comment
- Admin aliases — domain administrator aliases. Messages addressed to the names listed with semicolon as a separator will be delivered to the domain administrator
- Admin e-mail — mail address of the domain administrator
- Contents Type — domain content type
  - § Own contents — domain will have its own users. Here it is also possible to choose desired data access driver to be used to access domain users
  - § Referral contents — domain content will be taken from another domain via a link

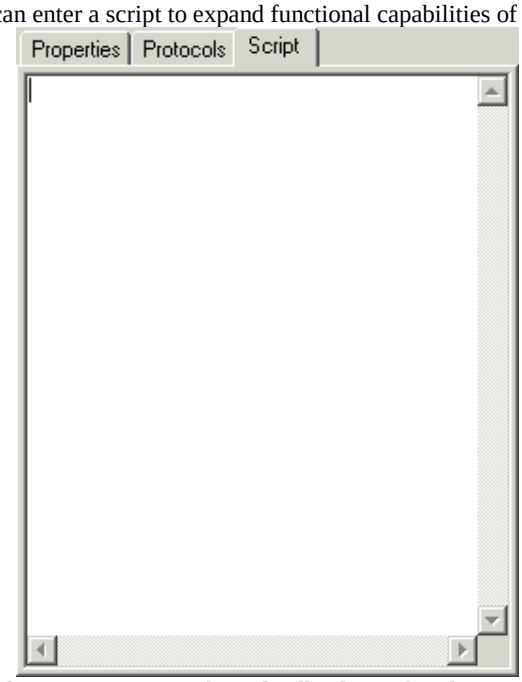
the link (domain name) can be either entered manually or chosen from the list. The latter method is preferable, as misspelling is impossible.

On the “Protocols” tab you can set the protocol properties:



currently, POP and SMTP protocols are supported (IMAP is coming soon). A protocol may be deactivated, then no connection will be accepted via that protocol for the chosen domain. If the server host is multi-address, you can specify the IP address connections via that protocol will be accepted on. You can also specify number of the port to be used for that protocol. **We don't recommend** changing any of these settings unless you have a very good understanding of their meaning.

On the “Script” tab you can enter a script to expand functional capabilities of the server:



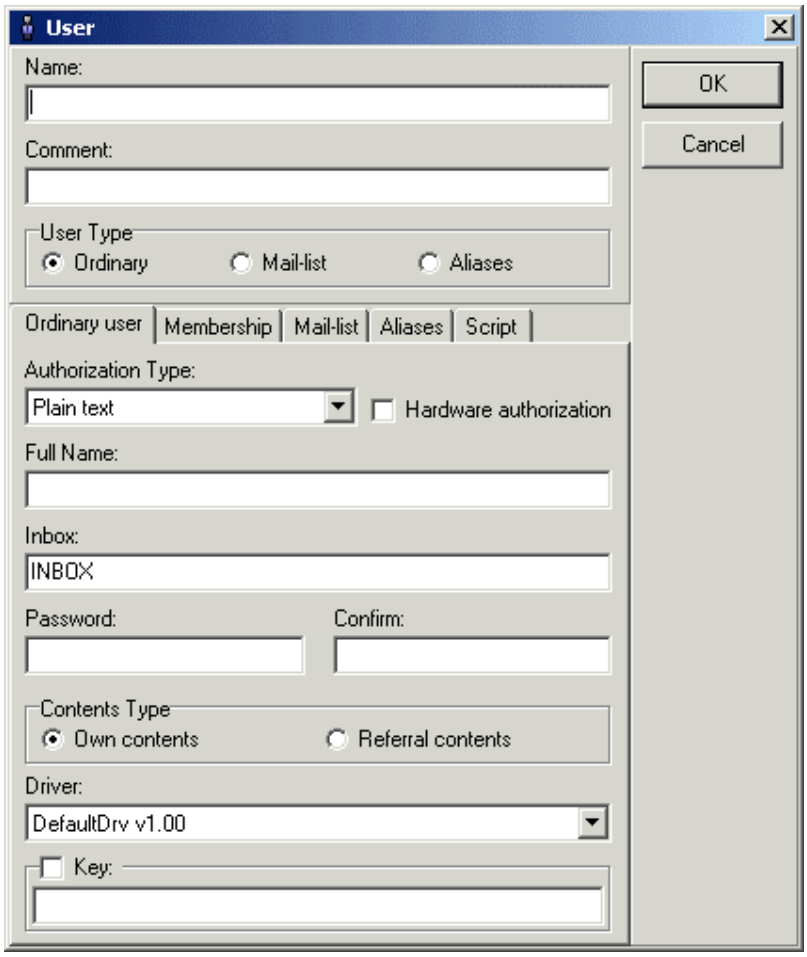
currently this feature doesn't work, moreover, it may be radically changed in the nearest future.

To save the changes click “OK”, to quit without saving click “Cancel”.

When a domain is being deleted (the “Delete” button in the main form) you will be first requested to confirm deleting and then you will be requested about deleting domain content. If domain content is used by another domain via a link, in most instances it is not to be deleted.

Users

By users we mean names of the mailboxes inside a domain (the part of the address before “@”), mail-lists and aliases. Messages received on a mailbox are put in it. Messages addressed to a mail-list or an alias will be sent to all addresses in the list. The difference between a mail-list and an alias is that with the former sender's address in replaced by address of the mail-list owner. When a user is being added or edited (Add and Edit respectively) the following form appears:



where

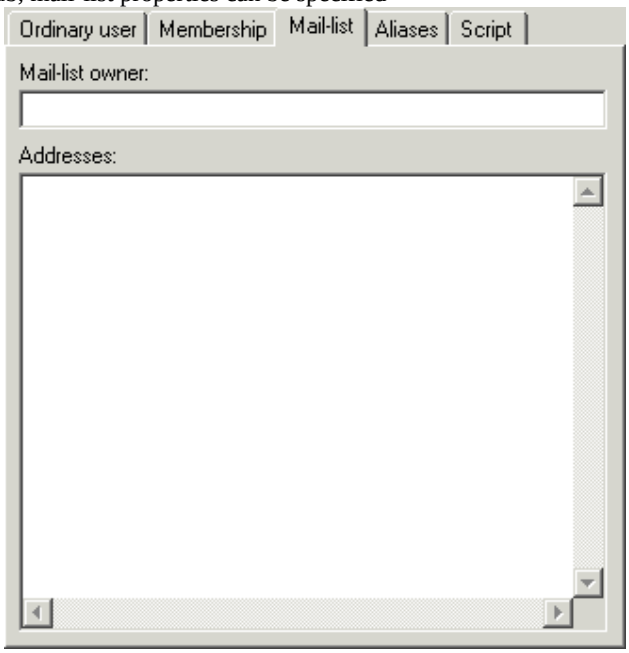
- Name — user name (the part of a mail address before "@")
- Comment — comment
- User Type — type of the user
  - § Ordinary — "standard" mail box
  - § Mail-list — mail-list
  - § Aliases — alias
- Authorization Type — authorization type
  - § Plain text — plain text authorization
  - § Digest MD5 — authorization through the Digest MD5 protocol (APOP command)
  - § CRAM MD5 — authorization through the CRAM MD5 protocol (AUTH command)
- Hardware authorization — authorization through hardware (not used so far)
- Full Name — user's full name
- Inbox — the home folder where messaged will be put by default under the SMTP protocol and which will be used by the POP3 protocol. It is not recommended to change the default name "INBOX" unless really necessary, as this might affect the system operation negatively when IMAP protocol is introduced.
- Password — user's password
- Confirm — confirmation of the user's password
- Contents Type — user's content type
  - § Own contents — a user will have own folders. Here it is also possible to choose desired data access driver to be used to access user's folders
  - § Referral contents — user's content will be taken from another domain via a link

the link (mail address) can be either entered manually or chosen from the list. The latter method is preferable, as misspelling is impossible.

In the "Membership" tab you can specify which groups each user belongs to:

the upper list contains the groups the user doesn't belong to, and the lower list contains the groups the user does belong to. You can use both the mouse and the keyboard to select groups. To select a range of groups, place the cursor on the first group in the range, press and hold "Shift", and move the cursor to the last group in the range, or vice a versa. You can also select desired groups one by one: click them with the "Ctrl" key pressed; clicking on a selected group will deselect it. Then you can click the “Add” button to add a user into all highlighted groups, or the “Remove” button to remove a user from all highlighted groups.

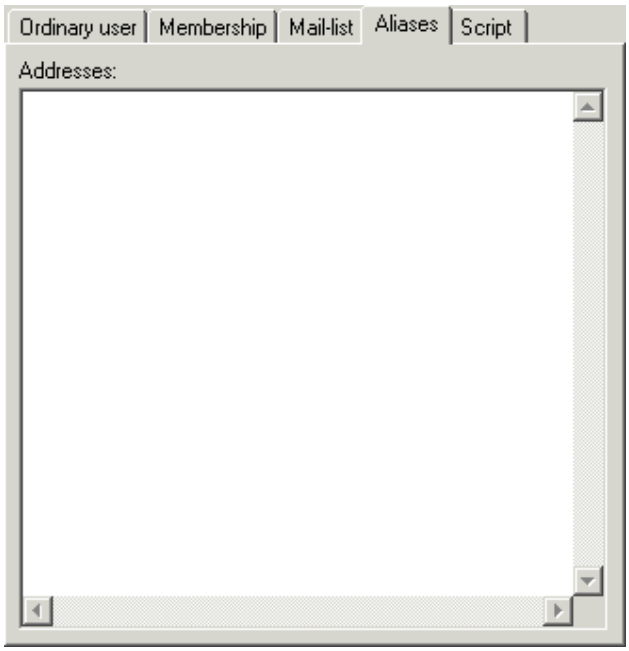
On the “Mail-list” tab, mail-list properties can be specified



where

- Mail-list owner — owner of the mail-list. This address will be shown instead of sender's address
- Addresses — the set of addresses included in the list

In the “Aliases” tab you can specify the addresses messages addressed to certain user will be forwarded to

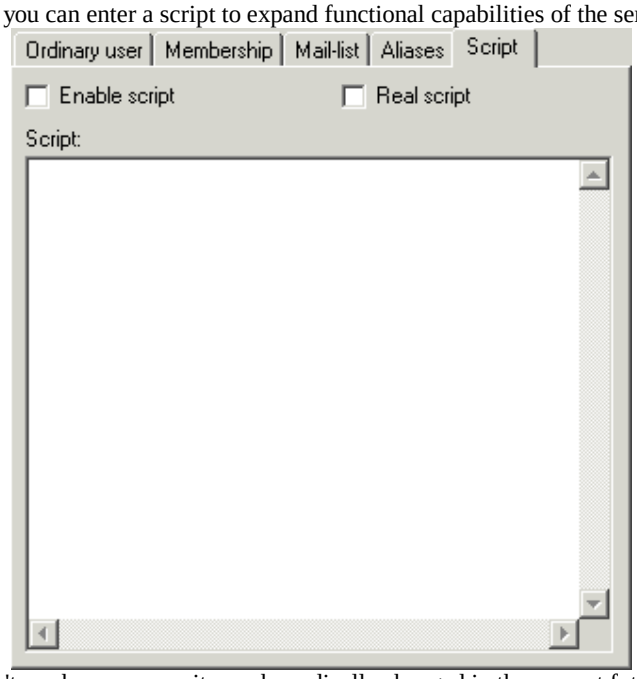


where

- Addresses — the list of addresses behind the alias

For more details about mail-lists and aliases, see the respectively named sections.

On the “Script” tab you can enter a script to expand functional capabilities of the server:



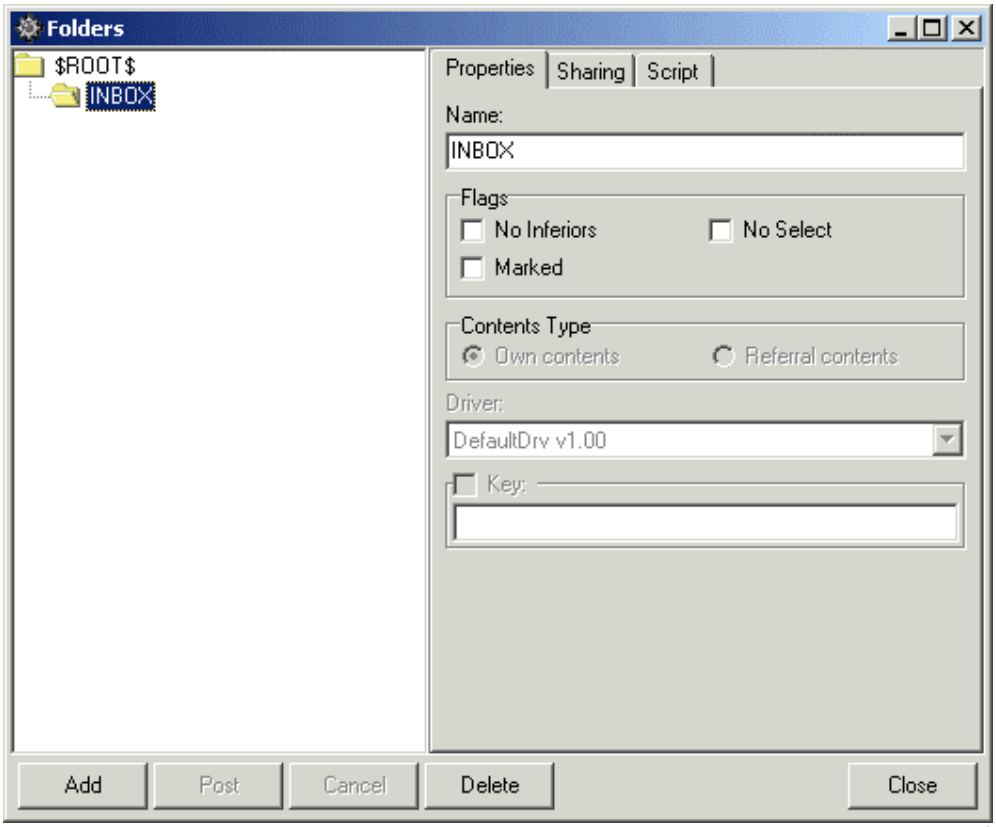
currently this feature doesn't work, moreover, it may be radically changed in the nearest future.

To save the changes click “OK”, to quit without saving click “Cancel”.

When a user is being deleted (the “Delete” button in the main form) you will be first requested to confirm deleting and then you will be requested about deleting user content. If user content is used by another user via a link, in most instances it is not to be deleted.

Folders

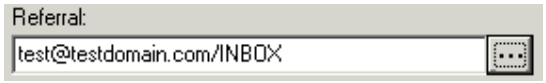
Each user has a tree of folders. By default, a user has only one folder: the home folder (INBOX). You can create any number of additional folders if necessary, however, this is only sensible when the IMAP protocol is used, as the rest protocols use the home folder solely. To view user's folders, open the “Users” tab in the main form, select desired user and click the “Folders…” button. You will see the following form:



The tree of folders belonging to the selected user is shown in the left. There is the special folder “$ROOT$” which is the root of the tree and which properties cannot be changed.

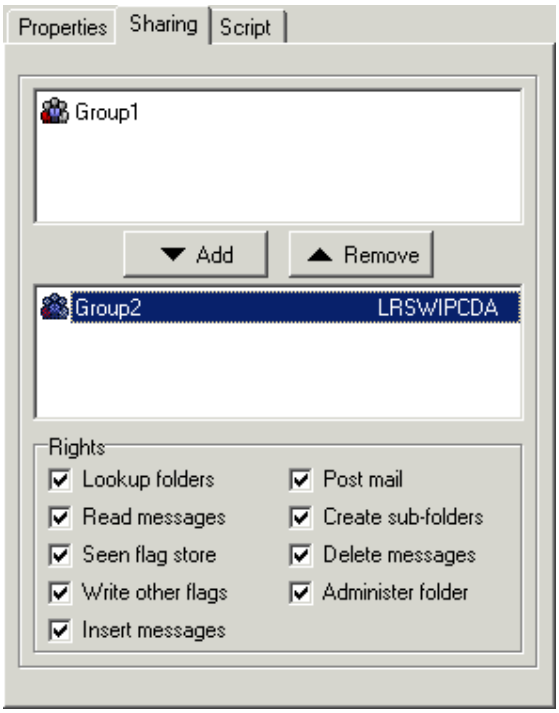
Folder properties are shown on the right:

- Name — folder name
- Flags — folder flag
  - No Inferiors — a folder can have no inferiors
  - No Select — a folder is unselectable (under the IMAP protocol)
  - Marked — a folder is marked as one that contains something "interesting", probably messages
- Contents Type — type of the folder content
  - Own contents — a folder will have its own messages. Here it is also possible to choose desired data access driver to be used to access messages inside the folders
  - Referral contents — user's content will be taken from another domain via a link



the link (mail address/Folder/Subfolder) can be either entered manually or chosen from the list. The latter method is preferable, as misspelling is impossible.

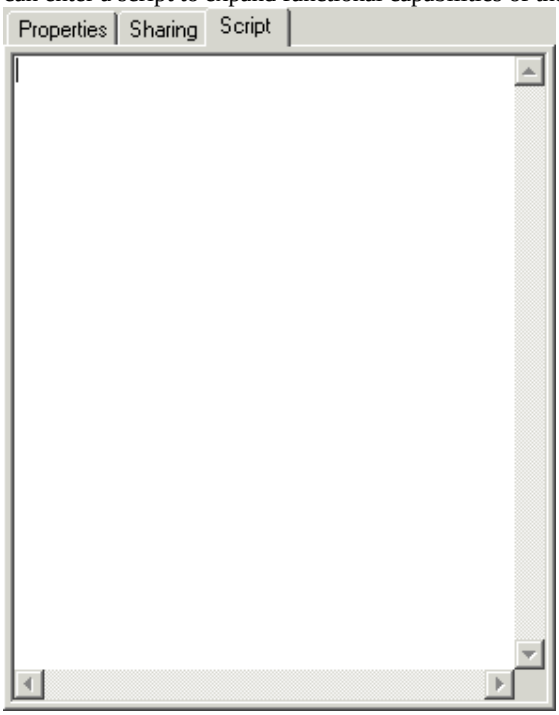
On the “Sharing” tab, group rights in a folder can be specified:



The upper list contains the groups that have no rights in the folder, and the lower list contains the groups which rights are specified. You can add groups by clicking the “Add” button and remove them by clicking the “Remove” button. The lower list also shows the rights of the groups designated by the code letters:

- (L) Lookup folders — the right to look through subfolders inside the folder
- (R) Read messages — the right to read message inside the folder
- (S) Seen flag store — the right to keep the "seen message" flag
- (W) Write other flags — the right to write other flags
- (I) Insert messages — the right to add messages into the folder
- (P) Post mail — The right to send messages
- (C) Create sub-folders — The right to create subfolders inside the folder
- (D) Delete messages — the right to delete messages from the folder
- (A) Administer folder — the right to administer the folder, i.e. to specify user rights

On the “Script” tab you can enter a script to expand functional capabilities of the server:



currently this feature doesn't work, moreover, it may be radically changed in the nearest future.

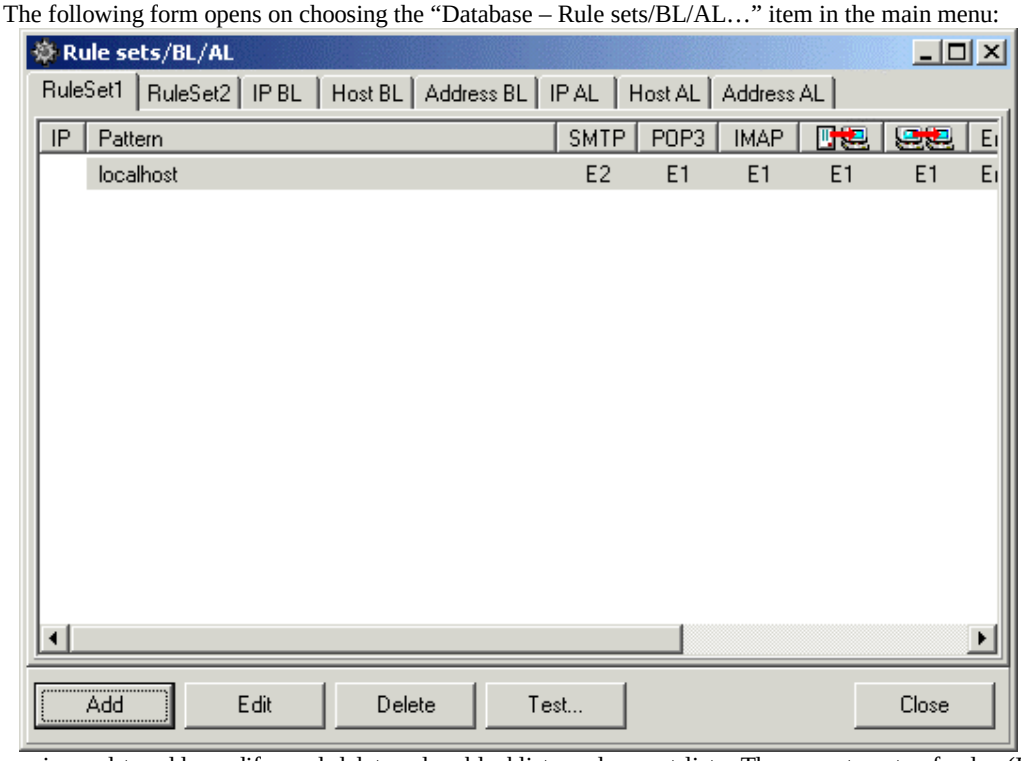
All folder properties concern only the IMAP protocol, as in the rest protocols the notion of folder is not used at all.

There is a number of buttons with the following functions at the bottom of the form:

- Add — add subfolder into the selected folder
- Post — save changes in properties of the folder being added or modified
- Cancel — cancel changes in properties of the folder being added or modified
- Delete — delete a folder. you will be first requested to confirm deleting and then you will be requested about deleting folder content. If the folder content is used by another folder via a link, in most instances it is not to be deleted.
- Close — close the folder form

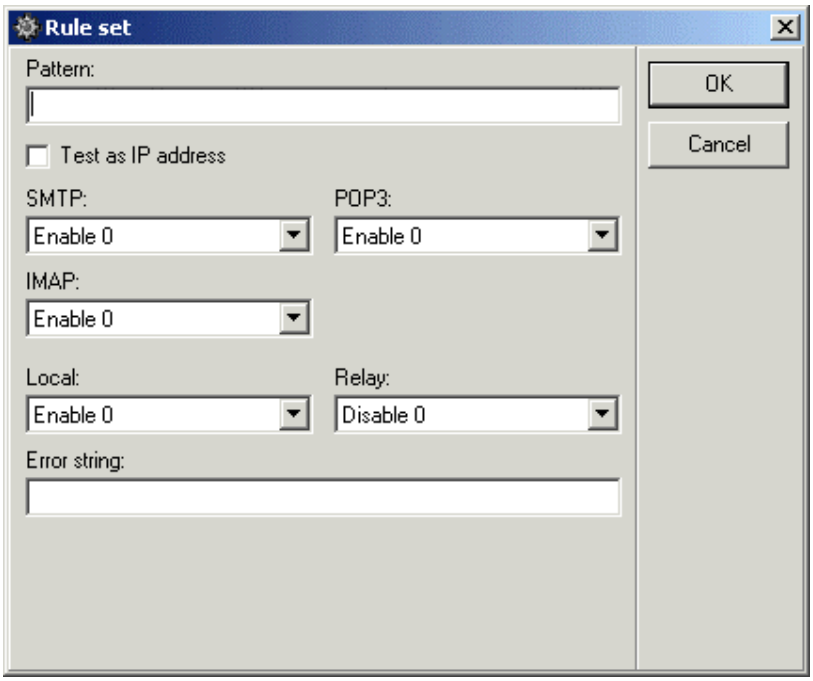
Rules, black-lists and accept-lists

The following form opens on choosing the “Database – Rule sets/BL/AL…” item in the main menu:



This form is used to add, modify, and delete rules, blacklists and accept-lists. There are to sets of rules (RuleSet1 and RuleSet2), three blacklists (IP BL, Host BL and Address BL), and three accept-lists (IP BL, Host BL and Address BL).

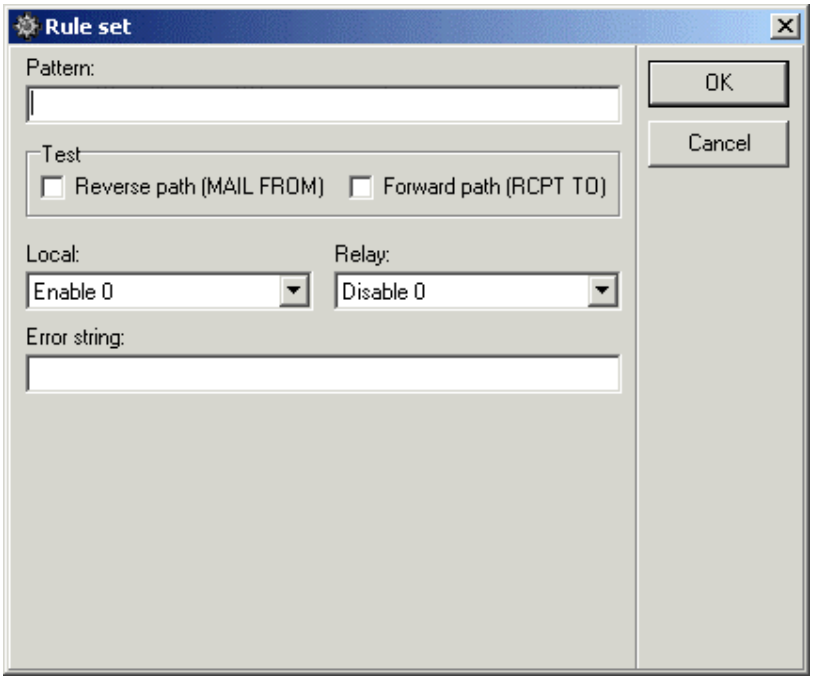
When the first rule set is being added or modified (the “Add” and “Edit” buttons respectively), the following form appears:



where

- Pattern — regular expression describing the rule template
- Test as IP address — if the box is checked, the template will be used to check IP address, otherwise it will be used to check the host name
- SMTP — whether connection via the SMTP protocol is permitted
- POP3 — whether connection via the POP3 protocol is permitted
- IMAP — whether connection via the IMAP protocol is permitted
- Local — whether the local message delivery is permitted
- Relay — whether the message relay is permitted
- Error string — the text line that will be displayed if the rule prohibits an action

When the first rule set is being added or modified (the “Add” and “Edit” buttons respectively), the following form appears:



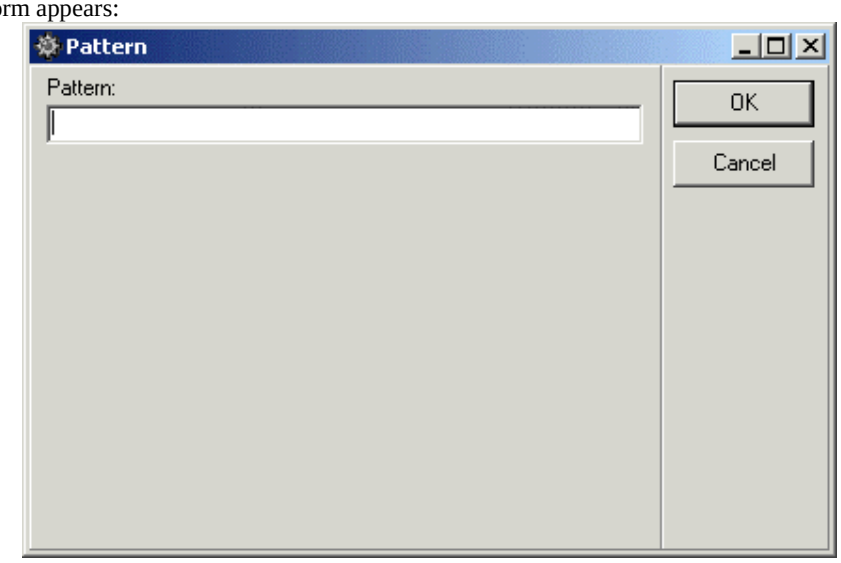
where

- Pattern — regular expression describing the rule template
- Test — to test addresses:
  - Reverse path (MAIL FROM) — return address

§ Forward path (RCPT TO) — destination address

- Local — whether the local message delivery is permitted
- Relay — whether the message relay is permitted
- Error string — the text line that will be displayed if the rule prohibits an action

When black-lists and accept-lists are being added or modified (the “Add” and “Edit” buttons respectively), the following form appears:

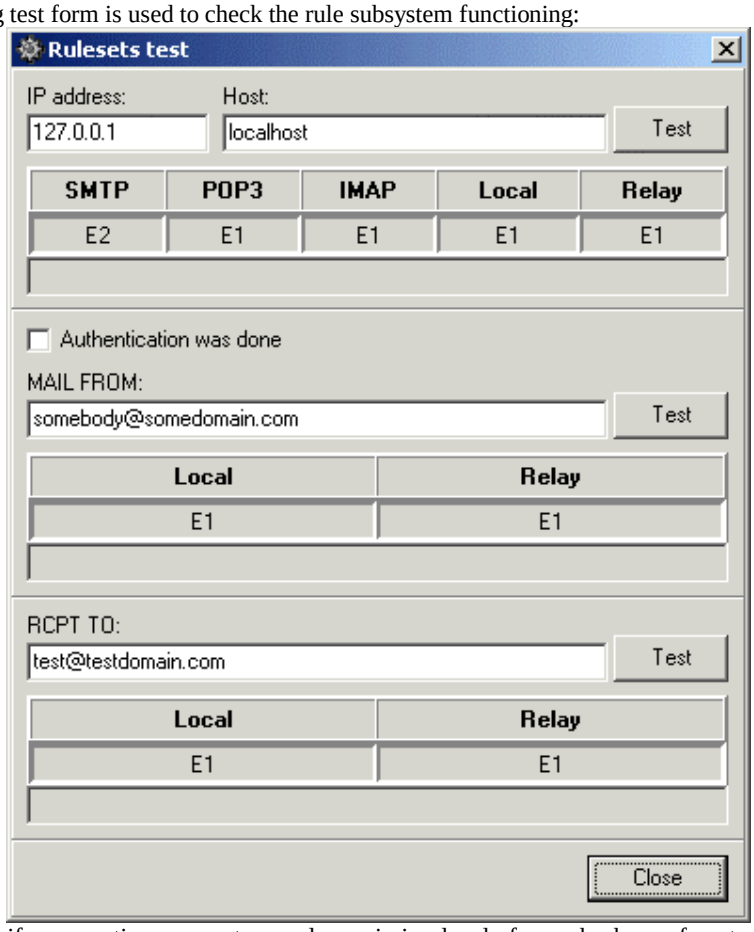


where

- Pattern — regular expression describing the black-list or accept-list pattern

For the detailed description of rule, blacklist and accept-list usage, see the sections “Introduction to the Rules”.

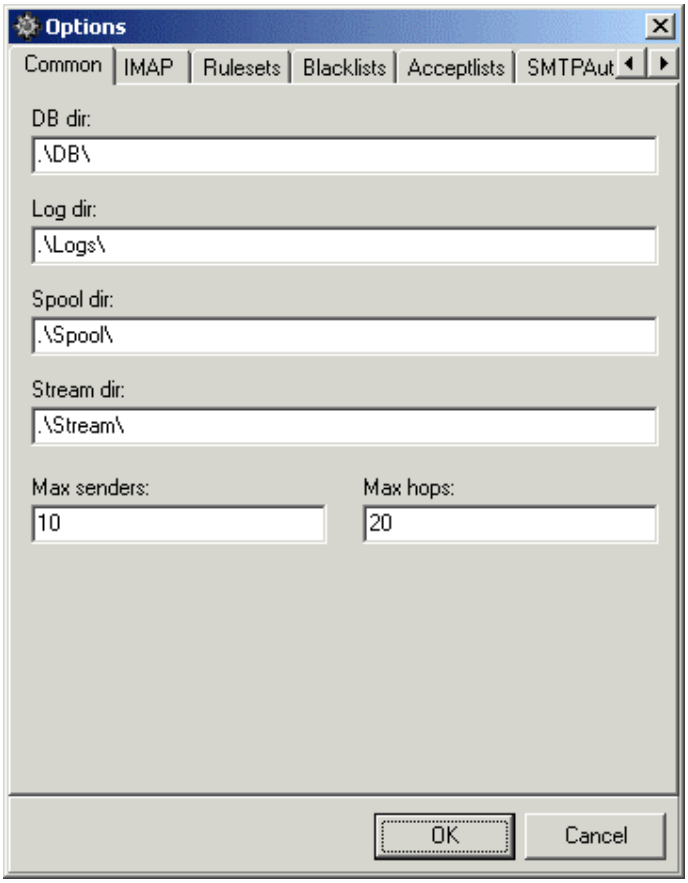
The following test form is used to check the rule subsystem functioning:



which allows to specify connection parameters and permission levels for each phase of protocol operation. This is especially helpful when the server "refuses" to perform some actions, e.g. to send messages.

Options

To set up the server options, choose the “Options” item in the main menu. The following form will appear on the screen:



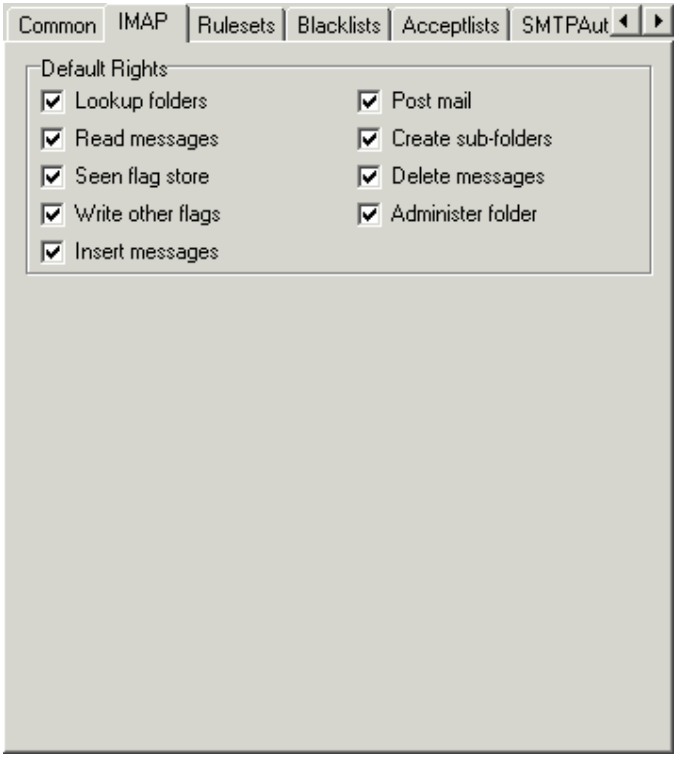
At the top of the form there is a set of tabs used to switch between option groups. Click on the “OK” button will result in saving of the changes done. To cancel the changes, the “Cancel” button is used. Of note, any changes in the options take effect only after relaunch of the server.

Common properties (The “Common” tab)

- DB dir — the directory where the server configuration is stored (groups, domains, users, folders, etc.)
- Log dir — the directory where the server logs are stored
- Spool dir — the directory where the server spool is stored
- Stream dir — the directory where the temporary stream files are stored (currently not used)
- Max senders — the maximum number of remote delivery domains (POST)
- Max hops — the maximum number of intermediate hosts a message may come through. Used to break endless message sending loops

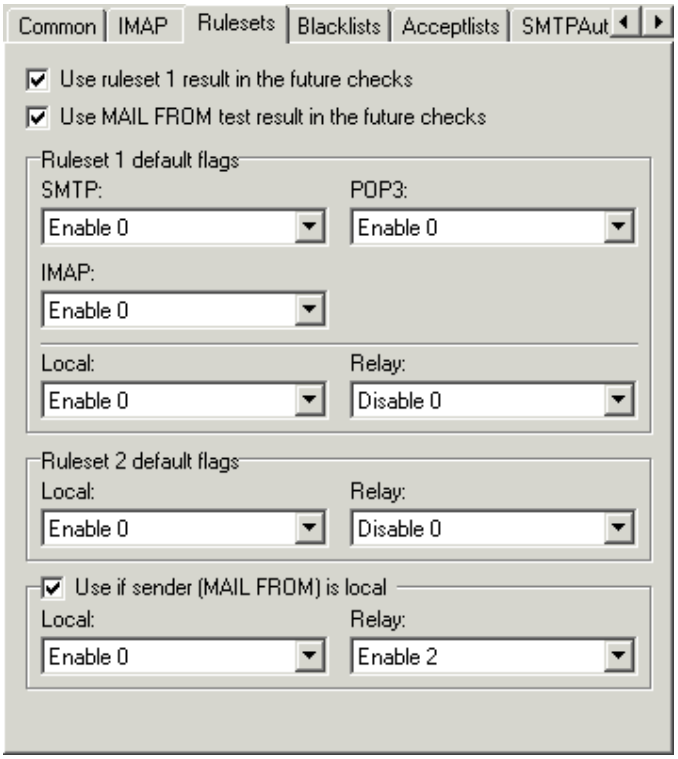
IMAP Properties (The “IMAP” tab)

Describes the default rights inside folders:



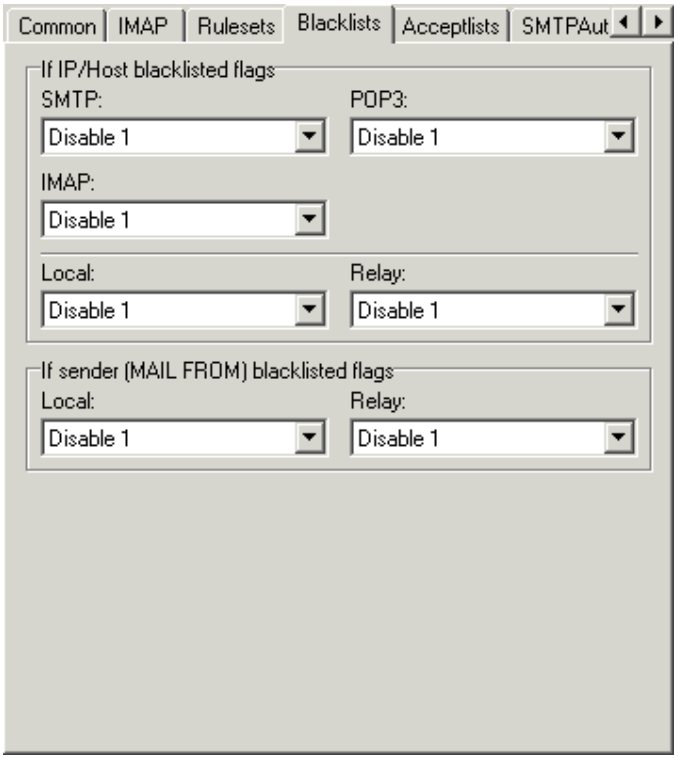
- Lookup folders — the right to look through subfolders inside the folder
- Read messages — the right to read message inside the folder
- Seen flag store — the right to keep the "seen message" flag
- Write other flags — the right to write other flags
- Insert messages — the right to add messages into the folder
- Post mail — the right to send messages
- Create sub-folders — the right to create subfolders inside the folder
- Delete messages — the right to delete messages from the folder
- Administer folder — the right to administer the folder, i.e. to specify user rights

Ruleset Properties (the “Rulesets” tab)



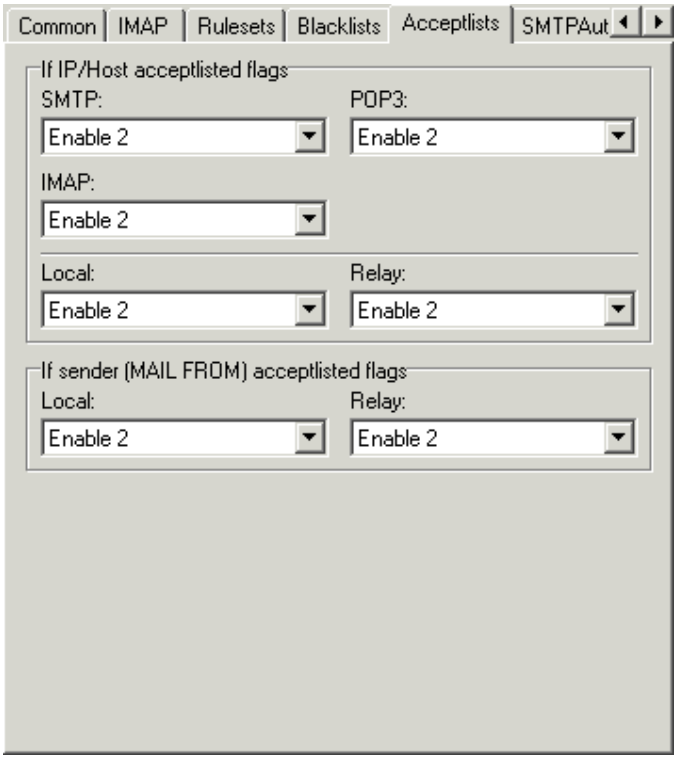
- Use ruleset 1 result in the future checks — the result obtained after running the fist set of the rules will be used in further calculations
- Use MAIL FROM test result in the future checks — the sender check result (MAIL FROM) will be used in further calculations
- Ruleset 1 default flags — default flag values before running the first set of the rules
  - SMTP — whether connection via the SMTP protocol is permitted
  - POP3 — whether connection via the POP3 protocol is permitted
  - IMAP — whether connection via the IMAP protocol is permitted
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted
- Ruleset 2 default flags — default flag values before running the second set of the rules
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted
- Use if sender (MAIL FROM) is local — flag values to be added to the calculation results if a sender is local to the server (the address in the “MAIL FROM” belongs to the server)
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted

Black-list Properties (the “Blacklists” tab)



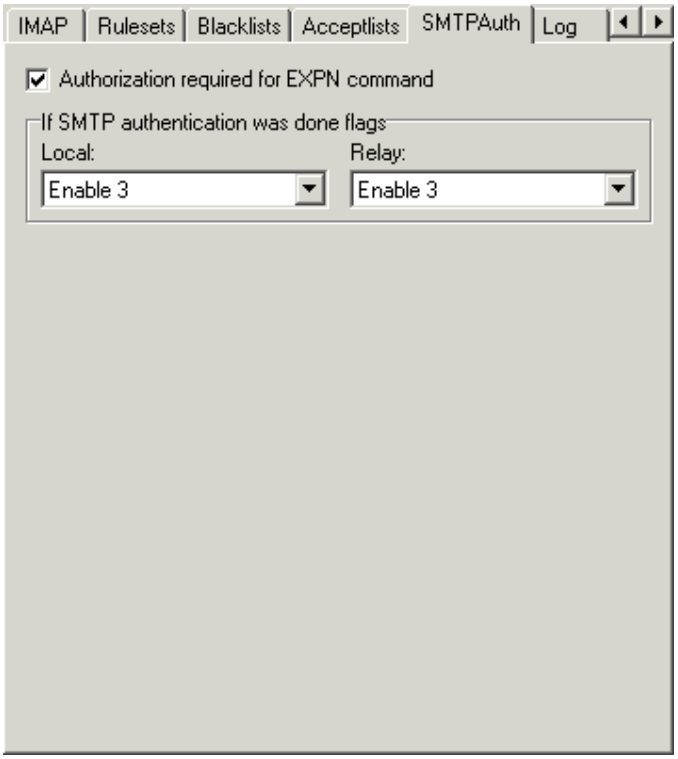
- If IP/Host blacklisted flags — flag values to be added to the calculation result, if IP address or host name found in black-list
  - SMTP — whether connection via the SMTP protocol is permitted
  - POP3 — whether connection via the POP3 protocol is permitted
  - IMAP — whether connection via the IMAP protocol is permitted
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted
- If sender (MAIL FROM) blacklisted flags — flag values to be added to the calculation result, if sender's address found in black-list
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted

Accept-list Properties (the “Acceptlists” tab)



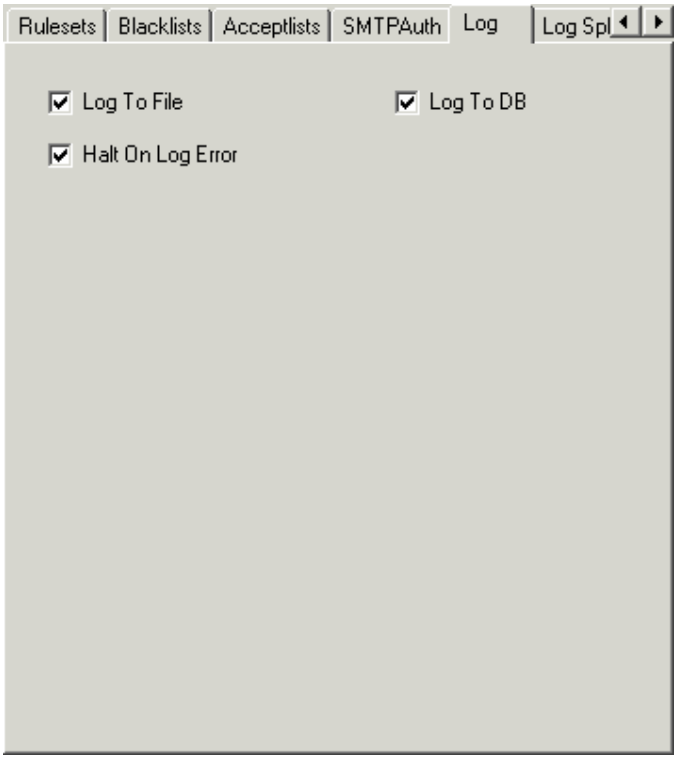
- If IP/Host acceptlisted flags — flag values to be added to the calculation result, if IP address or host name found in accept-list
  - SMTP — whether connection via the SMTP protocol is permitted
  - POP3 — whether connection via the POP3 protocol is permitted
  - IMAP — whether connection via the IMAP protocol is permitted
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted
- If sender (MAIL FROM) acceptlisted flags — flag values to be added to the calculation result, if sender's address found in accept-list
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted

SMTP Protocol Authorization Properties (the “SMTPAuth” tab)



- Authorization required for EXPN command — Authorization is required to perform the EXPN command (mail-list expanding in the SMTP protocol)
- If SMTP authentication was done flags — flag values to be added to the calculation result, if authorization was done in the SMTP protocol
  - Local — whether the local message delivery is permitted
  - Relay — whether the message relay is permitted

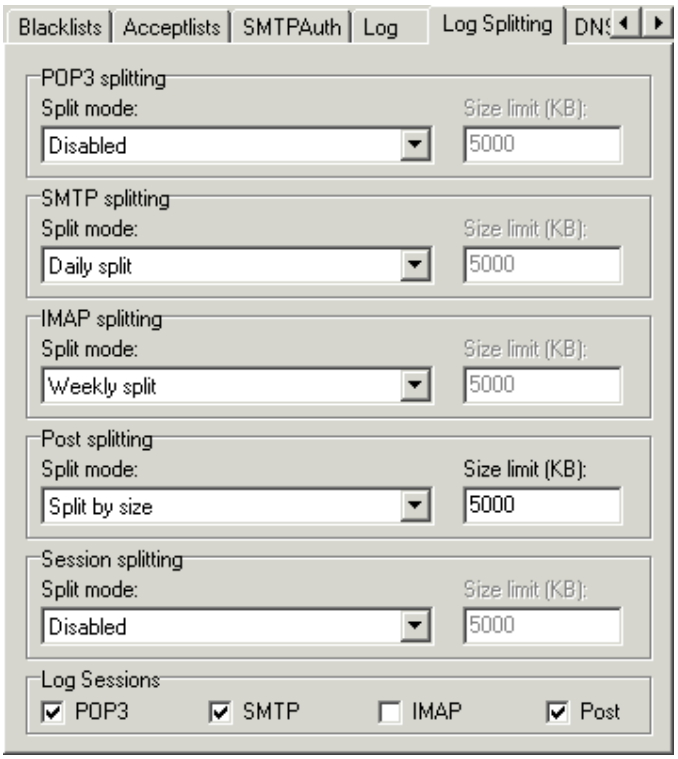
Log Subsystem Properties (the “Log” tab)



- Log To File — event logs are written to text files

- Log To DB — event logs are written to database. This provides for convenient analysis of the server operation later
- Halt On Log Error — stop operation of the server on error in the log subsystem. Sometimes it is very important that all events occurring with the server were registered. So, if the log subsystem doesn't work, the server must be stopped.

Log Splitting Properties (the “Log Splitting” tab)

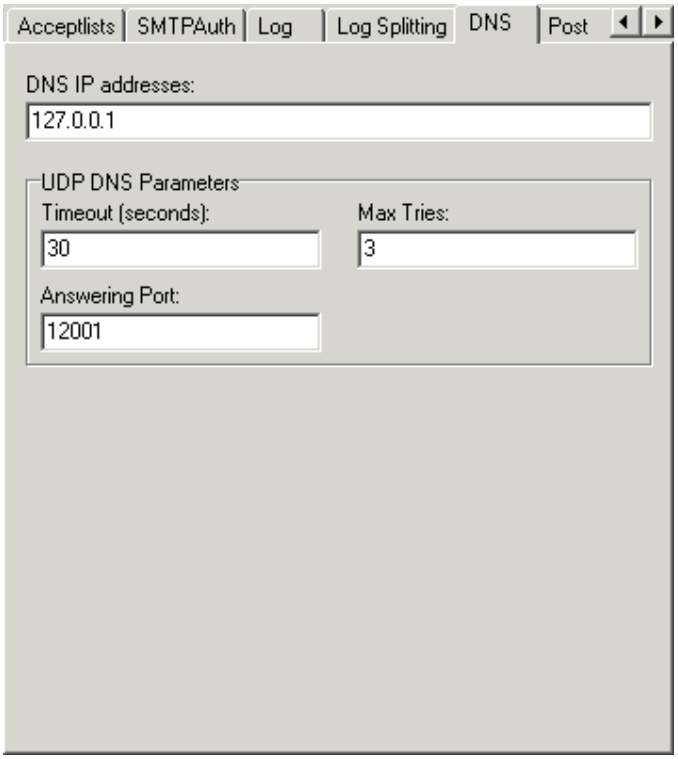


- POP3 splitting — log splitting mode for the POP3 protocol
- SMTP splitting — log splitting mode for incoming SMTP connections
- IMAP splitting — log splitting mode for the IMAP protocol
- Post splitting — log splitting mode for outgoing SMTP connections
- Session splitting — log splitting mode for session protocols
- Log Sessions — session types to be logged

There are the following log splitting modes:

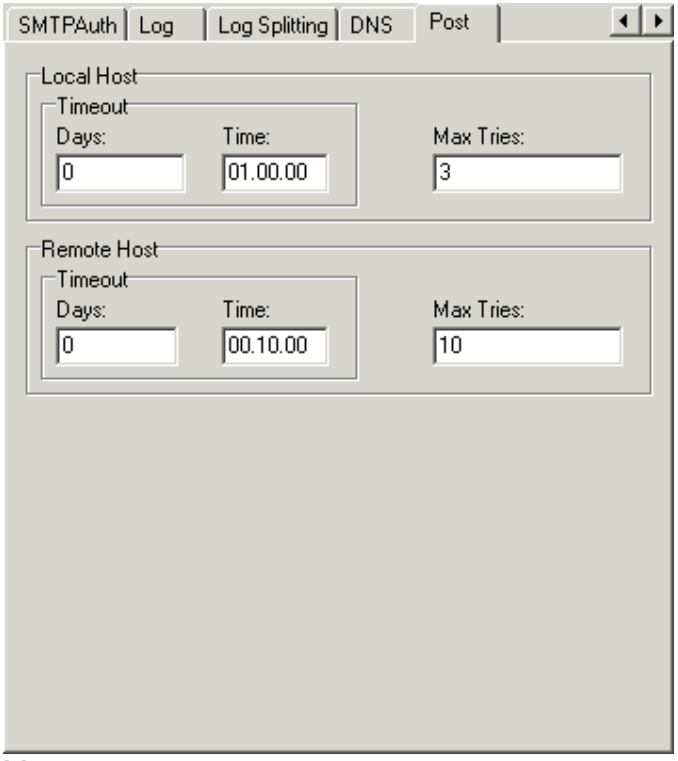
- Disabled — log splitting is disables
- Daily split — splitting is performed on a daily basis
- Weekly split — splitting is performed on a weekly basis
- Split by size — splitting is performed as soon as the specified size is achieved. The size value in KB is to be entered into the “Size limit (KB)” field

DNS Properties (the “DNS” tab)



- DNS IP addresses — the list of DNS (Domain Name System) server names, space-separated
- UDP DNS Parameters — DNS parameters while working through the UDP protocol
  - Timeout (seconds) — timeout for DNS server response waiting
  - Max Tries — maximum number of attempts to receive DNS server response
  - Answering port — the port DNS server response to be received on (required for the UDP protocol)

Message Delivery Properties (the “Post” tab)



- Local Host — local delivery properties
- Remote Host — remote delivery properties

There are the following delivery properties:

- Timeout — timeout on unsuccessful delivery attempt
  - Days — the umber of days
  - Time — time in the format `Hours.Minutes.Seconds`
- Max Tries — maximum number of delivery attempts

Regular Expressions

The regular expressions are the same as ones used in “The Bat!”. You can find their description in its help system.

Introduction into the Rules

The rules are used to solve the following main tasks:

1. Prevention of undesirable connections from being established
2. Filtering of unneeded incoming messages (spam)
3. Prevention of undesirable message traffic through server

At the moment, the following action types can be controlled by rules:

- Establishing connections under the SMTP protocol
- Establishing connections under the POP3
- Establishing connections under the IMAP
- Local message delivery
- Message traffic through the server

Each of the above actions can be either enabled or disable. Besides, there are priority levels from 0 (lowest) to 3 (highest). So, we have the following sequence of possible values (with ascending priority): E0, D0, E1, D1,…, E3, D3. Evidently, action prohibition has a priority. Let's refer to each of the values as a privilege (to perform an action), and the whole value sequence as the set of privileges.

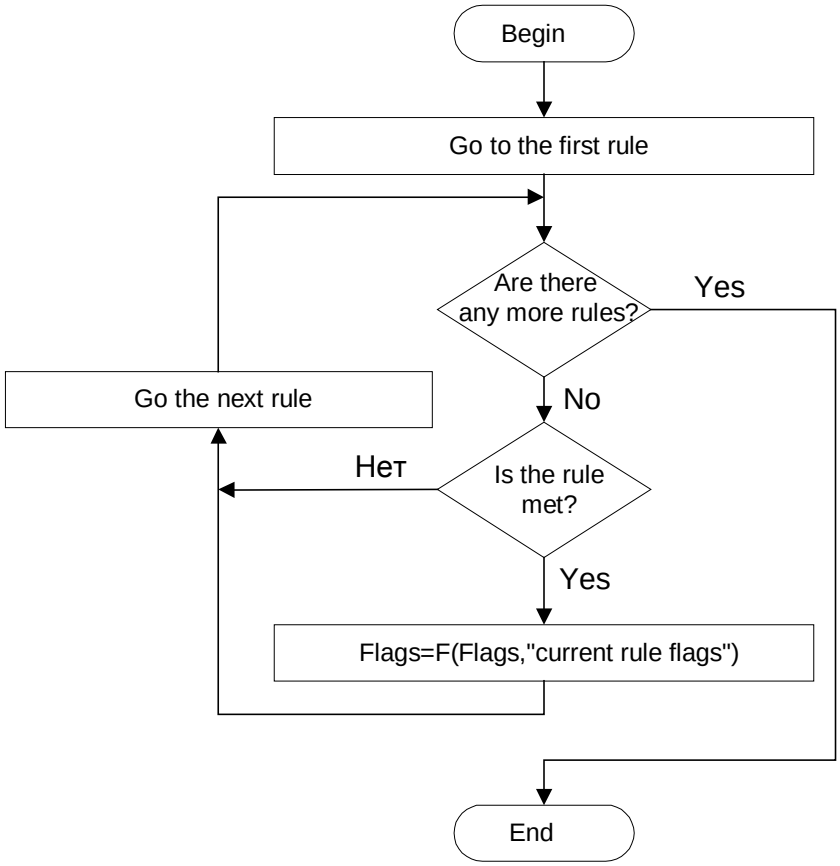
For easier operation, privileges for all actions are combined in a uniform variable: Flags. This results in a problem of combining two variable of the kind to find out the resulting privilege.

Introduce the function f(x,y) on the set of privileges, the result of the function also belongs to that set. This function chooses one of two values with higher priority. This gives us the following truth table:

	E0	**E1**	**E2**	**E3**	**D0**	**D1**	**D2**	**D3**
E0	E0	E1	E2	E3	D0	D1	D2	D3
E1	E1	E1	E2	E3	E1	D1	D2	D3
E2	E2	E2	E2	E3	E2	E2	D2	D3
E3	E3	E3	E3	E3	E3	E3	E3	D3
D0	D0	E1	E2	E3	D0	D1	D2	D3
D1	D1	D1	E2	E3	D1	D1	D2	D3
D2	D2	D2	D2	E3	D2	D2	D2	D3
D3	D3	D3	D3	D3	D3	D3	D3	D3

So, to find out the resulting value of all privileges the function f(x,y) is to be applied to each pair of privileges relevant to an action, and the values obtained are to be combined in the new flag variable. To denote such an action, we introduce the function F(X,Y), where X,Y are flag variables.

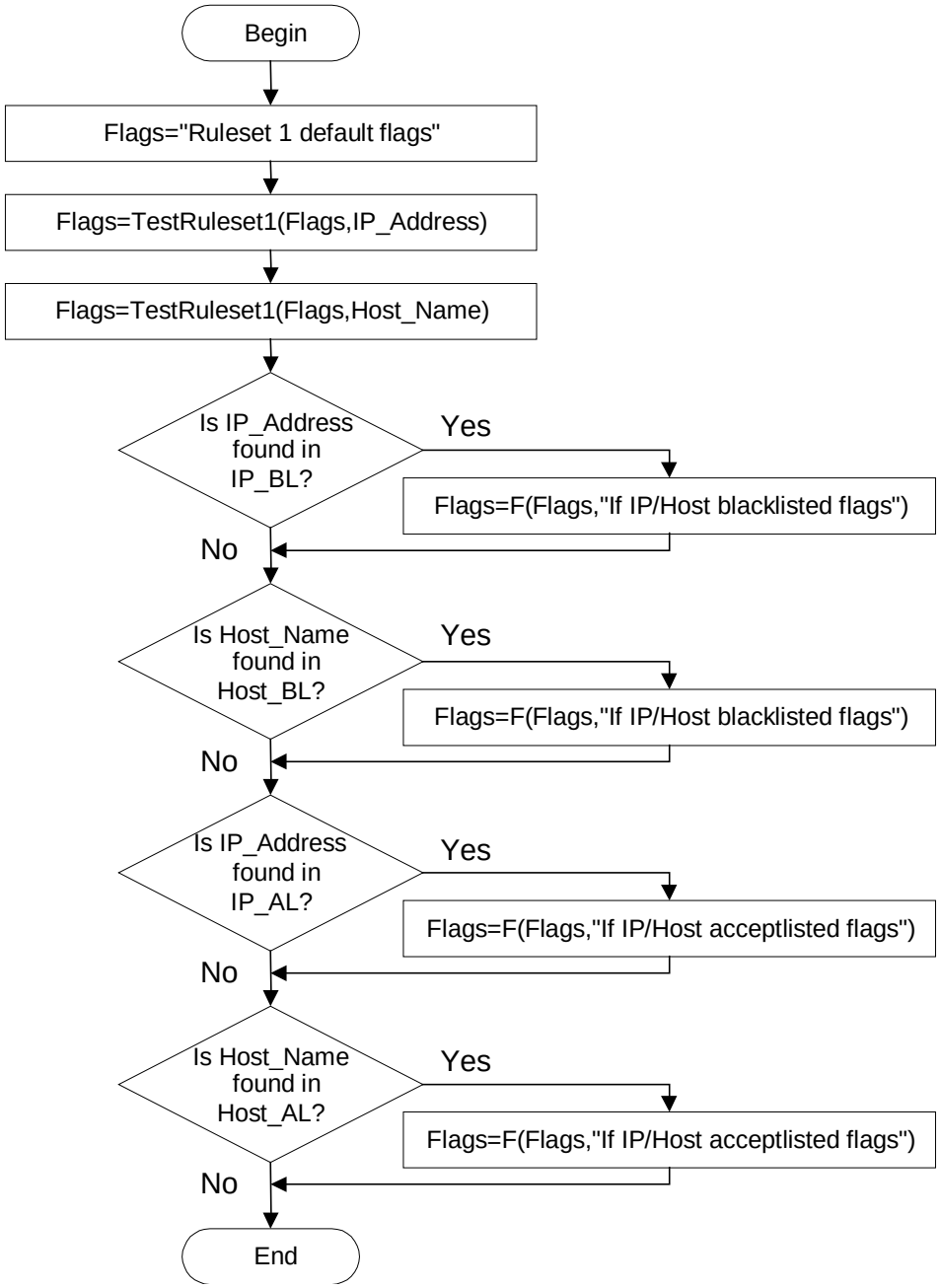
The following algorithm is used to check whether an action matches a ruleset:



The algorithm input data are initial privilege values in the Flags variable and the line being checked for matching the ruleset. Regular expressions (perl-style) are used in the rules. So, to find out whether the rule is met, the input line is checked for matching the regular expression contained in the rule. The output data are new privilege values in the Flags variable.

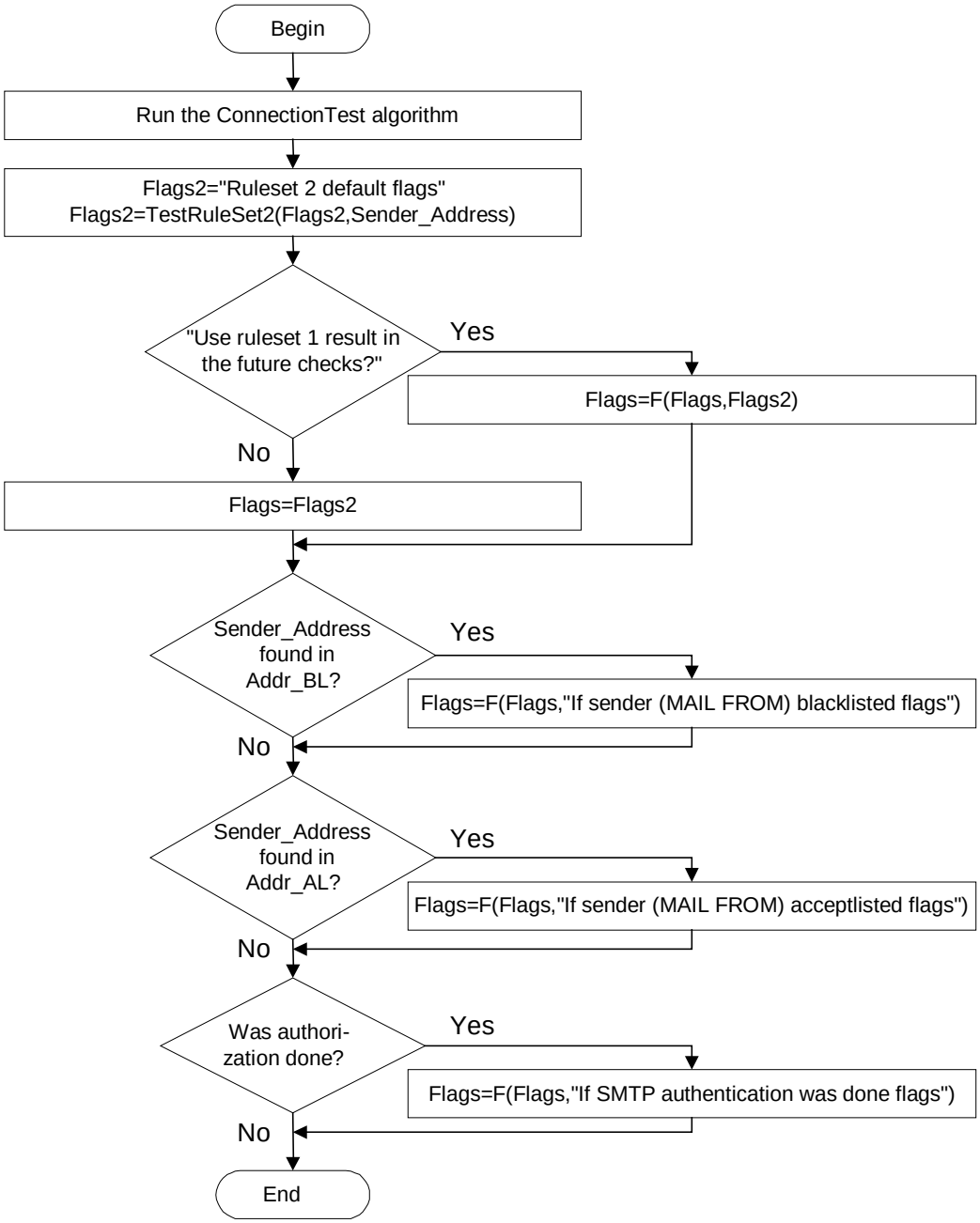
Further on, the following notations are used: TestRuleset1(Flags,String) to check if the string String matches the “ruleset 1” and TestRuleset2(Flags,String) to check if the string String matches the “ruleset 2”.

To find out privilege for establishing connection, the following algorithm is used:



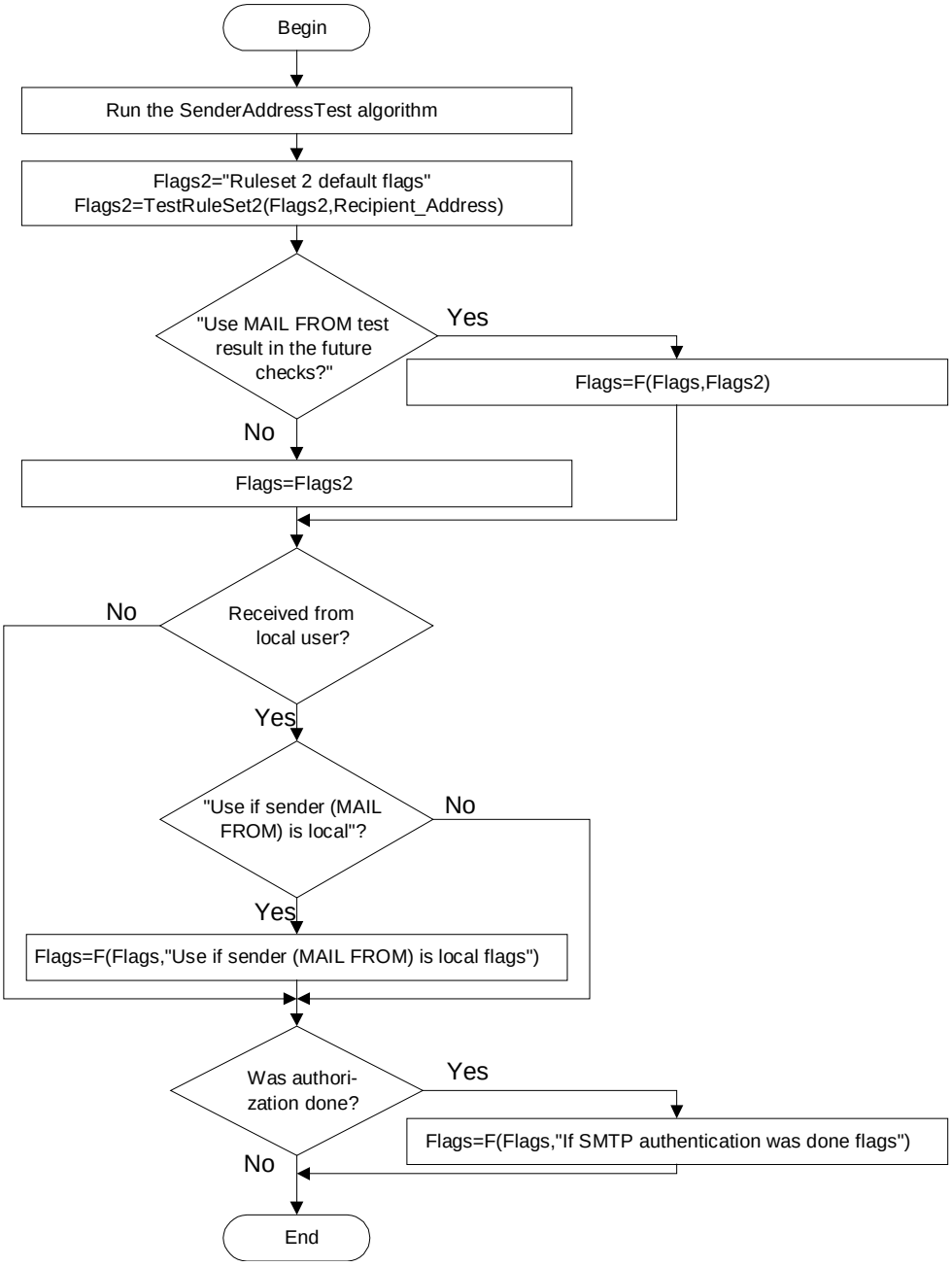
We get all privilege values in the Flags variable on the output. Further on we will refer to this algorithm as: ConnectionTest. Based on the algorithm results, undesirable connections can be screened. If the connection is permitted, the server greeting is sent back, otherwise the connection is denied.

Further discussion concerns the SMTP protocol. Once the command “MAIL FROM” is received, the Sender_Address is checked using the following algorithm:



The algorithm results show whether there is any sense in receiving recipient addresses. Thus, if the local message delivery and traffic is prohibited with the highest priority, the negative response is sent bask. Further on we refer to this algorithm as: SenderAddressTest.

Once the command “RCPT TO” is received, the Recipient_Address is checked using the following algorithm:



Based on the algorithm results we can find out whether message local delivery and traffic is permitted, and send back positive or negative response depending on whether the sender is local or remote.

Rule Usage Example

“Closed” Server

Suppose we want connections under the POP3 protocol to be established from the local network exclusively. To make the consideration easier, suppose local addresses look like “111.111.111.X”, where X may take any acceptable meaning.

To get the desired effect, set the “Disable 0” privilege for POP3 in the “Ruleset 1 default flags”. So, connection through POP3 is prohibited by default. Now, the rule in the “Ruleset 1”: set the pattern as “111.111.111.*”, check the box “Test as IP address” and choose the “Enable 1” privilege for POP3.

Configured in this way, the server will accept POP3 connections only from the above set of addresses. Suppose you need to accept POP3 connections from the address “222.222.222.222”, which doesn't belong to the local network. You can set one more rule, or you can use the “IP AL” (IP acceptlist). To do that, set in the “If IP/Host acceptlisted flags” for POP3 permission with the priority no lower than 1 (E1,E2,E3) and add the pattern “222.222.222.222” in the “IP AL”.

Once all the above actions are done, POP3 connections will be accepted only from local addresses and from the address “222.222.222.222”.