



MailMax 5 Mail Server

Installation and Reference

**Copyright © 2002-2003, SmartMax Software, Inc.
2431 E. 61st Street Suite 307
Tulsa, Oklahoma 74136-1231
USA**

1	Getting Started.....	1
1.1	Overviews.....	1
1.1.1	DataMax - Data Management for MailMax.....	1
1.1.2	SMTPMax - Inbound mail.....	1
1.1.3	POPMax - Mail for users using POP3 protocol.....	1
1.1.4	IMAPMax - Mail for users using IMAP4 protocol or Web mail.....	1
1.1.5	QueueMax - Outbound mail processing.....	1
1.2	Setting up your MailMax 5.5 server.....	1
1.2.1	Conversion from 4.x MailMax.....	1
1.2.2	Attaching to a SQL Database.....	2
1.3	Setup.....	2
1.4	Basic System Wizard.....	3
2	MailMax Admin.....	6
2.1	Connection Tree.....	6
2.2	Connection Information.....	7
2.3	Groups and Clusters.....	10
2.3.1	Groups.....	10
2.3.2	Clusters.....	10
2.4	Domains and Users.....	10
2.5	Connection Settings.....	13
2.6	Connection Activity.....	14
3	Local Settings.....	15
3.1	Local Service Settings - Locations.....	15
3.2	Local Service Settings - Database.....	16
3.3	Local Service Settings – Anti-Virus.....	17
4	Global System Settings.....	18
4.1	Global System Settings - General.....	18
4.2	Global System Settings - Open Relay.....	20
4.3	Global System Settings - SMTP.....	21
4.3.1	SMTP Logging.....	23
4.4	Global System Settings - Queue.....	24
4.4.1	QueueMax Logging.....	26
4.5	Global System Settings - POP/IMAP.....	27
4.5.1	POP3 Settings.....	27
4.5.2	POP Logging.....	28
4.5.3	IMAP4 Settings.....	29
4.5.4	IMAP Logging.....	29
4.6	Global System Settings - DNS.....	30
4.7	Global System Settings - Rules.....	31
4.8	Global System Settings - Connection Control.....	32
4.9	Global System Settings - Bans.....	33
4.10	Virus Settings.....	34
4.11	Virus Actions.....	36
5	Connections.....	38
5.1	Connection Settings - General.....	38
5.2	Connection Settings - Connections.....	39

5.3	Connection Settings - Bans	40
5.4	IP Settings	41
5.5	Service Settings.....	42
5.6	Editing Service Settings.....	43
6	Domain Settings	44
6.1	Domain Settings - General	44
6.2	Domain Settings - Mail Boxes.....	45
6.3	Domain Settings - Alias	47
6.4	Domain Settings - Rules	48
6.5	Other Domain Issues.....	48
6.5.1	Smart Hosting.....	48
6.5.2	ETRN Domains.....	48
6.5.3	Backup Domains	49
6.6	Deleting Domains	49
7	User Settings	50
7.1	User Settings - General	50
7.2	User Settings - Forwarding.....	52
7.3	User Settings – Auto-Responder.....	53
7.4	User Settings - Remote Admin	54
7.5	User Settings - Rules.....	55
7.6	User Settings - Alias	56
7.7	Deleting Users.....	57
8	Rules	58
8.1	Condition Options	59
8.1.1	Size of Message.....	59
8.1.2	Date.....	60
8.1.3	Day of Week.....	60
8.1.4	Time	61
8.1.5	Specific Header	61
8.1.6	Message Body / Entire E-mail / File Attachment Name	62
8.1.7	File Type.....	62
8.1.8	External test	62
8.2	Action Options	63
8.2.1	Store.....	63
8.2.2	Forward	63
8.2.3	Auto-Respond Text.....	64
8.2.4	Auto-Respond File.....	64
8.2.5	Note to Self.....	65
8.2.6	Run Program	65
9	Logging and Spying	67
9.1	Logging.....	67
9.2	Spying.....	67
9.2.1	IMAP Tracing.....	67
9.2.2	SMTP Tracing.....	68
9.2.3	QueueMax Tracing.....	68
9.2.4	POPMax Tracing	69

10	Frequently Asked Questions	70
11	Menu Layout and Descriptions.....	71
11.1	Main Menu.....	71
11.2	Popup Menu for Domain List	72
11.3	Popup Menu for the Services List.....	73
11.4	Popup Menu for the User List.....	73
12	Messages and Alerts.....	74
	Contacting SmartMax Software Customer Service	84

1 Getting Started

1.1 Overviews

A MailMax server system consists of the following NT/2000/XP services.

1.1.1 DataMax - Data Management for MailMax

DataMax is the hub of operations for the various MailMax Services. It must be running for the other services to operate. Besides supplying the data needed for the services to run, it also tracks the comings and goings of the services and users connecting to the system.

1.1.2 SMTPMax - Inbound mail

SMTPMax is the SMTP server for MailMax. SMTP servers take inbound mail for local users from other systems, and outbound mail from local users. SMTP servers can also relay mail from one server to another (although relay servers that are open to the public usually end up having their mail blocked by other servers for being a nuisance).

1.1.3 POPMax - Mail for users using POP3 protocol

POPMax is the server for the POP3 protocol and supports all standard POP3 commands including APOP for secure logins to POP3.

1.1.4 IMAPMax - Mail for users using IMAP4 protocol or Web mail.

IMAPMax is a full IMAP4 implementation. While IMAP4 is not quite as popular as POP3 for stand-alone mail clients, it rules the Web-based e-mail systems.

1.1.5 QueueMax - Outbound mail processing

QueueMax takes all mail generated by SMTPMax and connects to other SMTP servers passing on mail to them. QueueMax is simply a fully automated SMTP client. QueueMax needs little information to run other than where to find its mail files and how long to wait for other servers to respond to it.

1.2 Setting up your MailMax 5.5 server

1.2.1 Conversion from 4.x MailMax

If upgrading from MailMax version 4.6 or greater, convert your database and mail before continuing with the setup of MailMax 5.5.

Additionally, you MUST backup your EXMAIL4.MDB and the Domain Directories containing all the user mail! This process is NOT REVERSIBLE.

Please Note: The following conversions will only upgrade systems running MailMax 4.6 or greater.

First, run **convertdb.exe**. Then select whether your database is SQL or Access, and provide either the database path or the SQL login information. This will create a new database that is 5.5 compatible.

Second, run **e-mailconvert.exe**. This converts all e-mail to the 5.5 format. If running an

Access database simply click “ok” to convert the mail, or if running a SQL database enter in the SQL login information and click “ok”. Please note that rules, bans, blocks, and relay list information will NOT be converted.

NOTE: This process, despite its simplicity, can take a long time to run. Be patient.

1.2.2 Attaching to a SQL Database

IMPORTANT: This step is only for those who are using their own SQL server instead of the MSDE included with MailMax. If you installed MSDE with MailMax then please skip to the Setup Section.

- 1) Copy both MailMax5_log.LDF and MailMax5_Data.MDF into the Data directory underneath the install of your SQL Server. These files are in the root MailMax directory (C:\MailMax5 by default).

After the files have been moved, you will need to open your SQL Enterprise Manager and attach the MailMax 5.5 database. From the Enterprise Manager you will simply need to connect to the instance of SQL that MailMax is going to use and go to “Databases.”

Next, “right click” within or on Databases, go into “All Tasks” and click “Attach Database.” Now enter the path to MailMax5_data.MDF (where you moved it within the Data directory) and click “Verify command.” After the database has been verified, the “attach as: name” should already show it as MAILMAX5. You may set the database owner to whatever you wish.

Now simply click “ok” to attach the MailMax 5.5 database to SQL. Once you receive a successful database attachment simply click “ok” and close the Enterprise Manager. You now have one more important thing you must do before doing anything else.

Open the MailMax Admin from the Server where MailMax is installed. Select the menu **Edit | Local Settings**. Next go to the Database tab. From here you will need to enter the IP address of the SQL Server as well as the database name. By default the name is “MailMax5.”

Now you need to decide whether MailMax 5.5 will use Windows or SQL Authentication to modify the database. If you choose Windows Authentication, then simply leave the Use SQL Authentication box “unchecked” and click “ok”. If you choose SQL Authentication, then check the box and enter in a user name and password that has permission to modify the MailMax5 database and click “ok.”

NOTE: It is very important that you add the corresponding User Name and Password to your SQL server for the MailMax 5 database, otherwise MailMax 5 will not have a user to authenticate against when logging into your SQL server. This method will be using SQL Authentication.

1.3 Setup

Now that you have installed the software accordingly, you will now setup the system for use.

- 1) Go to the **Services Panel** and make sure that the **MailMax-DataMaxDB** service is running. Next, open the **MailMax Admin** tool to begin the setup.

NOTE: If you have already completed the conversions there is nothing that you need to setup right now so you may simply start the other four services; however, read further for instruction regarding setting up connections and manipulating the database from the GUI. If you have not completed the conversions you will need to setup MailMax before you are able to send or receive any e-mail.

You will now create a connection to the DataMax service from **MailMax Admin**. Since this is the first time you will connect, it must be from the server where DataMax is installed. A

new connection is created by clicking on the lightning bolt.

A connection settings box will open asking for the “registration name”, IP address or host name, and password for the connection. The registration name helps you distinguish which MailMax you are connected to if you have more than one running. The IP address or host name and Password tell the GUI where to connect to DataMaxDB and what password to use.

Now that you have connected to DataMax, you may run the basic system wizard (see next section) which will help you get MailMax up and running quickly. The wizard will ask you to change your DataMax password, setup a domain and specify the IP for that domain. It will also ask you to choose where the e-mail for that domain will be stored and where the outbound e-mail for the server will stored. After changing the DataMax password SMTPMax must be restarted before it will run properly.

Adding domains and users is done through the domains/users section. When adding a domain you must specify a domain directory (where mail will be stored for the domain). When adding a user, enter the account name. You may leave the password blank and set MailMax to save the first password that is used to check the users account.

Adding additional connections is done through Connections Settings. Simply right click and select “add new”. You will now need to enter a connection IP, a default connection display name, and a default domain.

NOTE: By default, port 25 (SMTP), 110 (POP3), and 143 (IMAP) are added for each IP in the connection settings. You may also add any additional ports you wish to have for each service, as long as the port is not already in use.

You now have the basic system configured.

1.4 Basic System Wizard

For blank systems where nothing is set up, you will be invited to run this wizard. It will add some basic settings, services and users to an empty system. The wizard pages should be self-explanatory.

Directories

For the domain, you need to specify where all the users and email are to be stored. This can be a drive and directory name, or a UNC path.

c:\mailmax5\smartmax

Enter the IP that this basic mail system will run on. If it needs to run using multiple IPs, you will need to set that manually later.

216 . 63 . 229 . 3

For outgoing mail, you need to specify a directory that will be used for queueing outbound mail. Again, this can be drive and path, or a UNC.

c:\mailmax5\queue

< Back Next > Cancel Help

Use this wizard page to enter directories where to put files. The wizard page should be self-explanatory.

Users

Below are some common users that are found on many systems. Select the desired and enter a password.

Note: you only need to enter the password once (or leave blank for no password) because you can safely change it in the user settings.

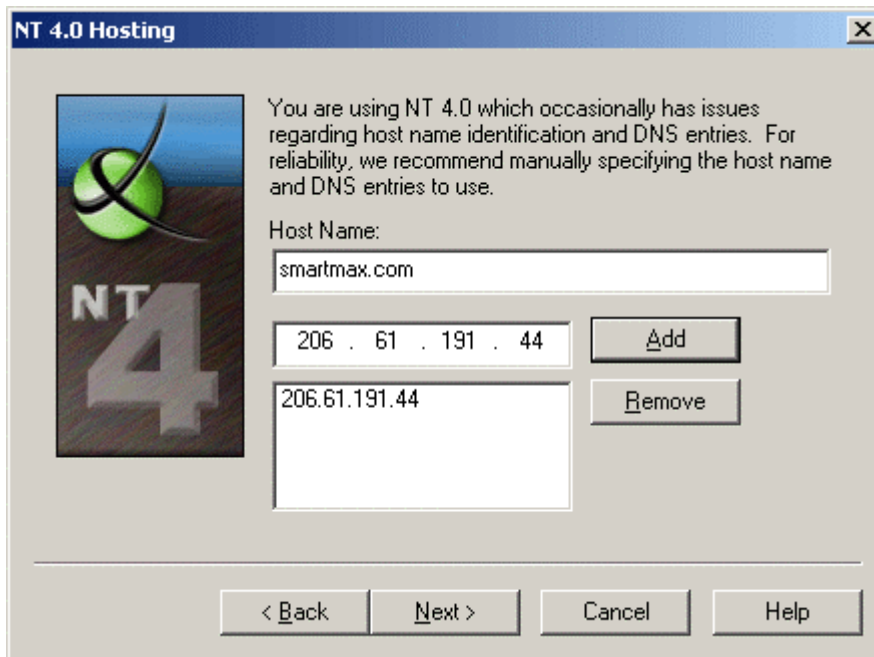
postmaster [password field]

admin [password field]

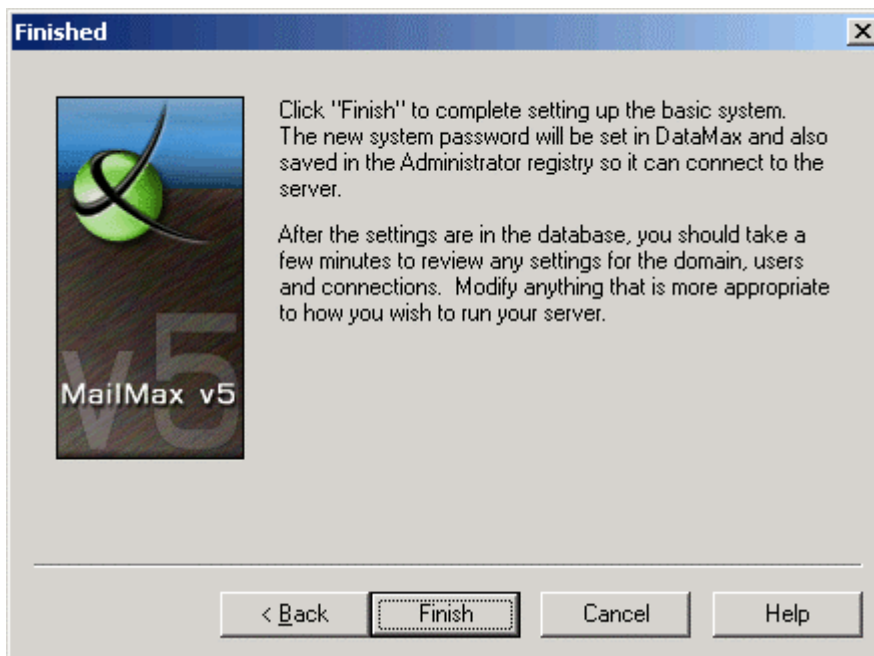
root [password field]

< Back Next > Cancel Help

This wizard page will add the users checked above. Unless you enter a password, they will be blank.



This page of the wizard only occurs if you are doing setup for a Windows NT 4.0 system. Due to certain issues with DLL's under NT 4.0, it is recommended that you enter the Host Name manually as well as the DNS entries to be used by MailMax.



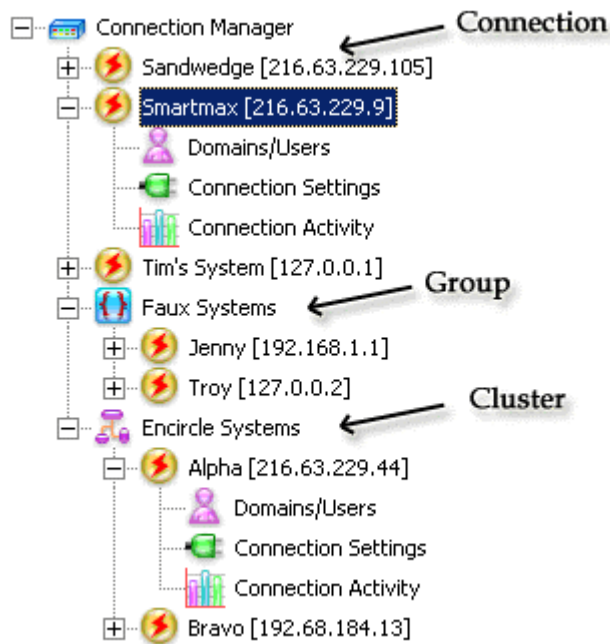
You might wish to review system settings, domain settings, and user settings for the system you have just configured.

2 MailMax Admin

MailMax Admin is the program you will run to configure and control your MailMax system. This section is a description of the main window.

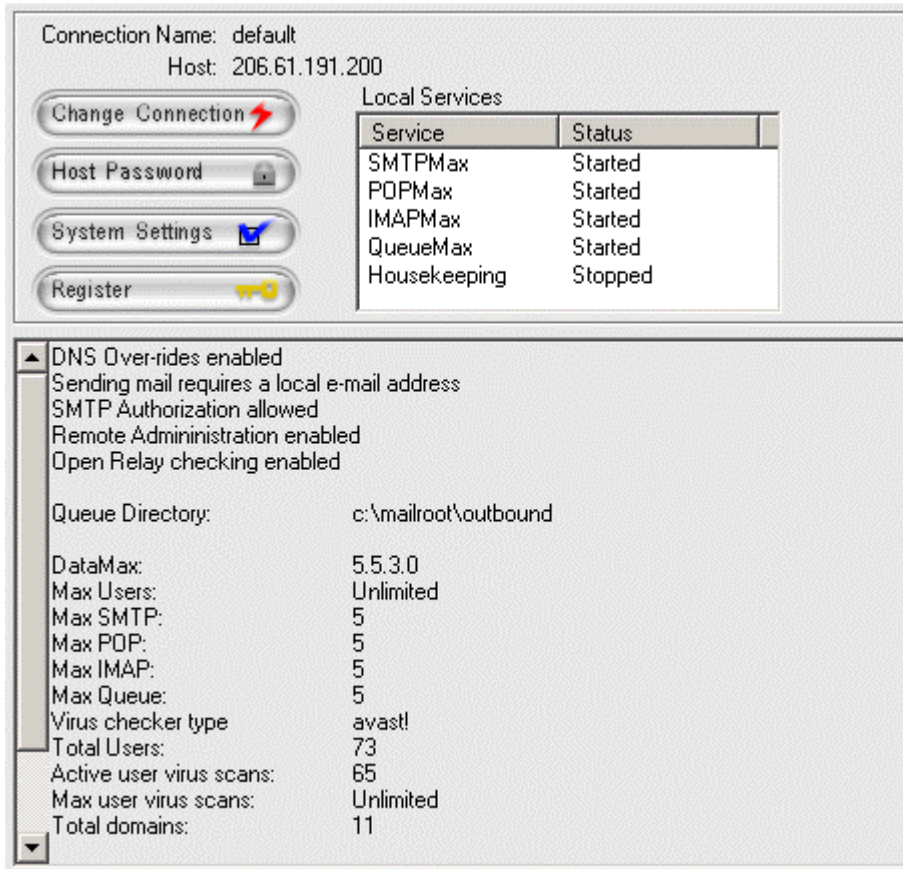
2.1 Connection Tree

The MailMax Admin main window contains a convenient layout for editing and controlling your MailMax system. The Connection Tree contains the Connection Manager and all the DataMax connections that you control. Below is an exaggerated collection of systems. Most e-mail systems (even those with thousands of e-mail domains and tens of thousands of users) will only have one connection entry in the list. If you are maintaining multiple separate systems, you can organize your connections into groups. For advanced users, mail systems may be clustered. Putting a connection in a cluster lets e-mail be routed to other members of the cluster if a user is not on the initial cluster member.





2.2 Connection Information


When a connection is selected in the connection tree, the following is displayed:




Connection Name: default
Host: 206.61.191.200

Change Connection 

Host Password 

System Settings 

Register 

Local Services	
Service	Status
SMTPMax	Started
POPMax	Started
IMAPMax	Started
QueueMax	Started
Housekeeping	Stopped

DNS Over-rides enabled
 Sending mail requires a local e-mail address
 SMTP Authorization allowed
 Remote Administration enabled
 Open Relay checking enabled

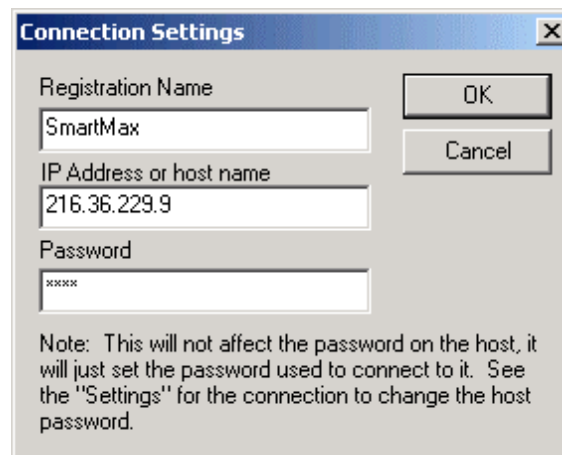
Queue Directory: c:\mailroot\outbound

DataMax: 5.5.3.0
 Max Users: Unlimited
 Max SMTP: 5
 Max POP: 5
 Max IMAP: 5
 Max Queue: 5
 Virus checker type: avast!
 Total Users: 73
 Active user virus scans: 65
 Max user virus scans: Unlimited
 Total domains: 11

Summary connection information is displayed for your convenience in this window. You can click on the buttons on the display to set the appropriate values for your system.

Change Connection

Use this to set the connection information -- IP and password -- used to connect to DataMax. Note: this does *not* change the password that DataMax uses. Instead, use "Set Host Password". You must be able to connect before you can change the host password.



Connection Settings

Registration Name: SmartMax

IP Address or host name: 216.36.229.9

Password: *****

OK

Cancel

Note: This will not affect the password on the host, it will just set the password used to connect to it. See the "Settings" for the connection to change the host password.

Registration Name

Enter the name that the connection will be known by. The choice of name is arbitrary, but entering your company name is recommended. For connections in clusters or groups, a distinct (even whimsical) name is recommended.

IP Address or host name

Enter the IP or name where Data ax is running for the system.

Password

Enter the password needed to connect to Data ax on the system. NB: This does *not* change the password for Data ax. You have to be connected to Data ax before you tell it to use a different password.

System Settings

See the section on Global System Settings.

Set Host Password

If you can connect to the server, you can give it a new password. Be aware that you will need to restart services because they will need to reconnect to Data ax with the new password.

MailMax Admin will automatically remember the password you set so you do not need to set this for the connection settings. Services running on the computer will also know the new password. However, services running on other computers will need to be told of the new password by using the local settings dialog.

Running services *must* be restarted to run properly after the system's password is changed.



A dialog box titled "New Host Password" with a close button (X) in the top right corner. The text inside reads "Enter the new system password for DataMax" above a text input field containing "xxxx". Below that, it says "Re-Enter to prevent mistakes" above another text input field also containing "xxxx". At the bottom, there are two buttons: "OK" and "Cancel".

New Password

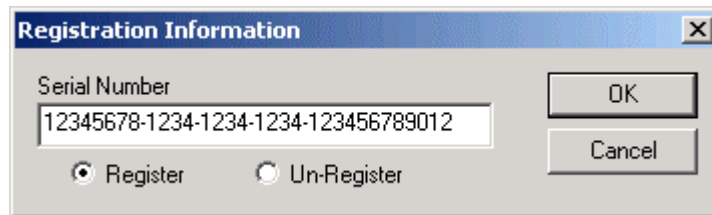
Enter the desired password. Spaces are not allowed

Re-Enter

Enter it a second time to make sure you didn't make any spelling mistakes.

Register...

Use this to register a MailMax system. Registration requires being connected to the internet and a firewall that does not block standard mail transactions.



A dialog box titled "Registration Information" with a close button (X) in the top right corner. It features a "Serial Number" label above a text input field containing "12345678-1234-1234-1234-123456789012". Below the input field are two radio buttons: "Register" (which is selected) and "Un-Register". To the right of the radio buttons are two buttons: "OK" and "Cancel".

Serial Number

The number supplied by SmartMax to register your MailMax system.

Register

Select to register.

Un-Register

Select to un-register from this computer in order to run on a different hardware configuration.

2.3 Groups and Clusters

2.3.1 Groups

Groups are supplied in the Admin program to make it easier to administer multiple running copies of Data ax. Grouping of systems has no impact on their operation. However, a grouping provides a simple mechanism for organizing an overwhelming number of MailMax systems. To create a group, select the Connection Manager tree entry and select the menu "**Edit|New|Group...**"



Group Name

The group name may be any arbitrary and useful name.

2.3.2 Clusters

Clusters are presently identical to Groups, however, in future releases of MailMax, there will be added functionality for administering clustered systems. Clustered systems are 2 or more MailMax systems with knowledge of each other and the capacity of receiving mail on one system and routing it to the other. To create a cluster, select the Connection Manager tree entry and select the menu "**Edit|New|Cluster...**"



Cluster Name

Enter any arbitrary name for the cluster.

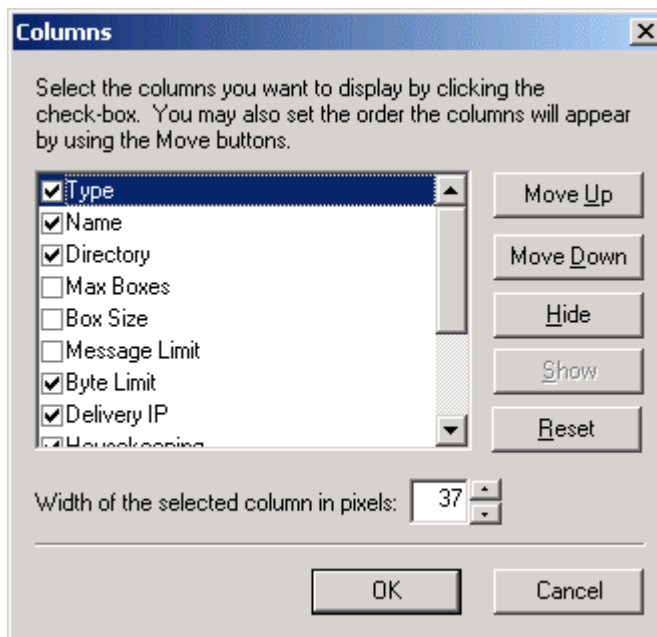
2.4 Domains and Users

The Domain and user lists can be selected by clicking on the "Domains/Users" entry in the connection tree. On the panel to the right, you will see a list of domains. If you click on any domain, its list of users will be displayed.

Type	Name	Directory	Max ...	Box Size
<input checked="" type="checkbox"/>	mailmax5-smtp.smar...	c:\mail\smartmax	N/A	N/A
<input checked="" type="checkbox"/>	testing.smartmax.com	c:\mail\testing	N/A	N/A
<input checked="" type="checkbox"/>	test.org	c:\mail\test.org	N/A	N/A
<input checked="" type="checkbox"/>	N/A	N/A

UserName	Type	First	Last	Disk Limit	Forward
test		test	test	N/A	<input checked="" type="checkbox"/>
capnclip		tim	robinson	N/A	
foobar		foo	bar	N/A	
fitclip				N/A	
fitclip2				N/A	

Users and Domains may be edited by double-clicking the entry in the list. Columns in either list can be sorted by clicking on the top of the column in the title. (The users are sorted by "Last" in the sample above.) Re-clicking will reverse the order. Right clicking on any of the columns will let you select which columns you wish to have displayed and in what order.



You can adjust the columns in the display using the Columns dialog.

The List

This is the list of column headers available. Click in the box to display the column.

Move Up, Move Down

Move the selection up or down in the list. This changes the order that the columns are displayed.

Hide, Show

Clears and sets the checkbox in the selected entry, respectively.

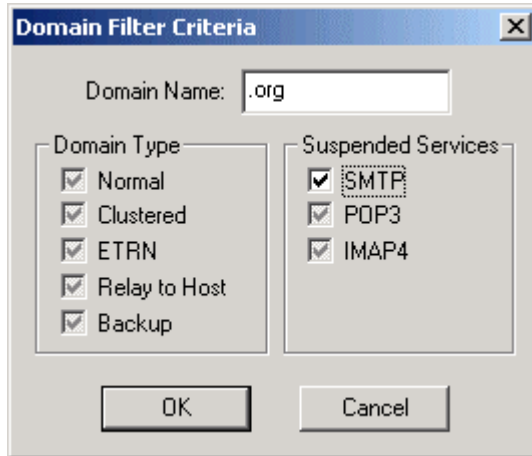
Reset

Return to original settings.

Width of the selected column in pixels

This controls the width of the selected column.

Right-click the domain list and select the "Filter..." option to filter the domain list.



The list of domains can be easier to manage if you restrict the number of domains displayed. Any strings entered in the field will be compared against the entries in the domain list and only those domains containing the match string(s) will be displayed. The tri-state check boxes let you filter by certain types of domains. If the box is grayed, the type is ignored. If checked, then only domains with that field set will be displayed. If the box is cleared, then only those which do NOT have that flag set will be displayed. For example, set the "SMTP" box and only those domains with SMTP services suspended will be shown.

Domain Name

Only those domains which contain this string will be shown..


Domain Type

Select the types of domains to show (or not show)

Suspended Services

Show only those domains with these services suspended.

Right-click the user list and select the "Filter..." option to filter the user list.



The dialog box titled "User Filter Criteria" contains the following fields and options:

- User Name:
- First Name:
- Last Name:
- Account Types:
 - Normal
 - Disabled
 - Spam Trap
- Remote Administrator
- Buttons: OK, Cancel

The list of users can be easier to manage if you restrict the number of users displayed. Any strings entered in the field will be compared against the entries in the user list and only those users containing the match string(s) will be displayed. The tri-state check boxes let you filter by certain types of users. If the box is grayed, the type is ignored. If checked, then only users with that field set will be displayed. If the box is cleared, then only those who do NOT have that flag set will be displayed. For example, clear the "Remote Administrator" box and only non-admin users will be shown.

User Name

Only those whose login name contains the string will be shown.

First Name

Only those whose first name contains the string will be shown.

Last Name

Only those whose last name contains the string will be shown.

Account Types

Select these to show users with the selected user types

Remote Administrator

Use this to filter by the Remote Administrator flag.

2.5 Connection Settings

The connection settings show a list of what clients can connect to on your MailMax system and are displayed by clicking the "Connection Settings" in the connection tree. If you click on a specific IP, the list of services running on that IP will be displayed.

IP	Default Domain	Display Domain
127.0.0.1	smartmax.com	smartmax.com
216.63.229.9	smartmax.com	smartmax.com
216.63.229.13	smartmax.com	smartmax.com
216.63.229.16	mailmaxweb.com	mailmaxweb.com
216.63.229.17	smartmax.com	smartmax.com

Service	Port
POP3	110
SMTP	N/A
IMAP4	N/A

Connections and Services may be edited by double-clicking the entry in the list. Columns in either list can be sorted by clicking on the top of the column in the title. Re-clicking will reverse the order. Right clicking on any of the columns will let you select which columns you wish to have displayed and in what order.

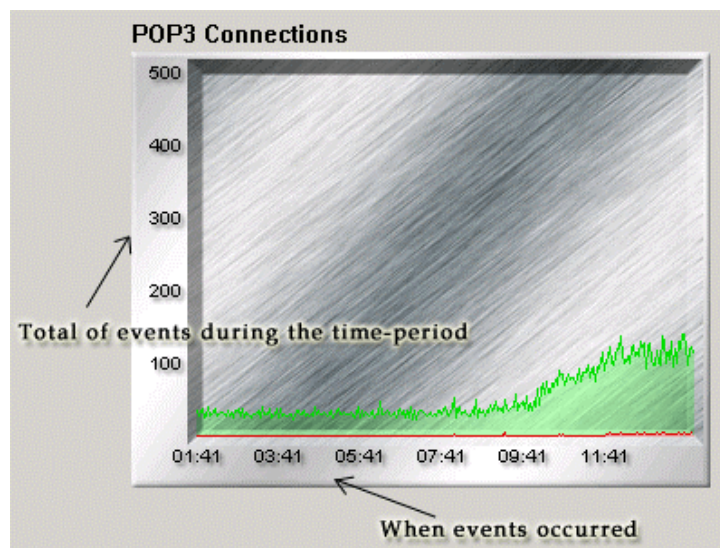
2.6 Connection Activity

The connection activity shows how busy a system has been over a period of time and is displayed by clicking "Connection Activity" in the connection tree. From here running services can also be watched from the selections in the "Spy" menu.

Service	Host
POPMax	bigbertha.smartmax.com
QueueMax	bigbertha.smartmax.com
SMTPMax	bigbertha.smartmax.com
IMAPMax	bigbertha.smartmax.com

You can right-click on any of the running services to select tracing for the service.

In addition to showing running services, summary graphs are displayed which show all connection and file traffic for all services. This information is dynamic and will reset upon terminating DataMax as a service. Here is a sample graph and explanation:

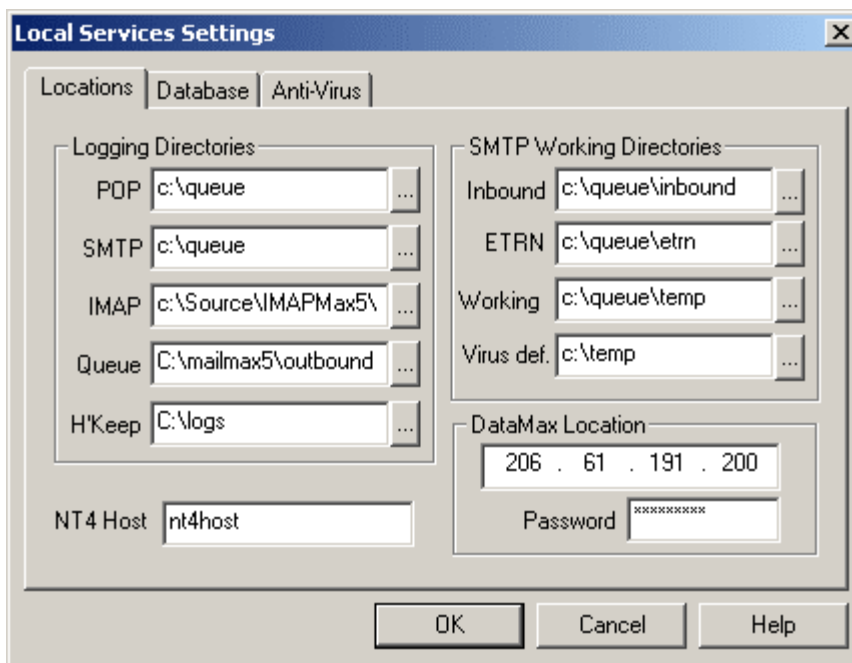


The green chart shows the total number of connections on both the POP3 and IMAP4 charts. What appears to be a red line at the bottom of the chart is actual another chart that (hopefully) remains a line. The red chart for POP3 and IMAP4 are failed login attempts. i.e. where a bad password has been entered. On the chart above, there are some small ripples in the red chart where someone tried to connect with a bad password. From what information is there, it's safe to presume that sometime starting at roughly 11:41 someone started a POP3 client with an incorrect password and then walked away from the client computer leaving it to try repeated logins. Note: This is not a security breach. Most clients automatically retry after a time-period to reconnect. If the red chart grows to be a significant percentage of the green chart, it may indicate an attempt on the security of your mail system.

SMTP connection activity is displayed in magenta and the three charts show connections and total mail traffic in both count and size.

3 Local Settings

3.1 Local Service Settings - Locations



Local service settings are used to configure local settings for MailMax servers. If MailMax was installed on a single computer, it should be configured correctly. However, if a service is moved to a separate computer from DataMax, then it needs to be told where to find DataMax and where to put its working directories.

You must run MailMax Administrator on the computer where the service operates in order for these settings to take effect.

Note that each directory entry in the dialog is followed by a button which may be clicked to browse for a folder to select.

Logging Directories

These directories are where the assorted services create their logs according to their settings for IMAP, POP, SMTP and Queue. Logging files are created with unique names for each service, so it is permissible to have all the services use the same directory.

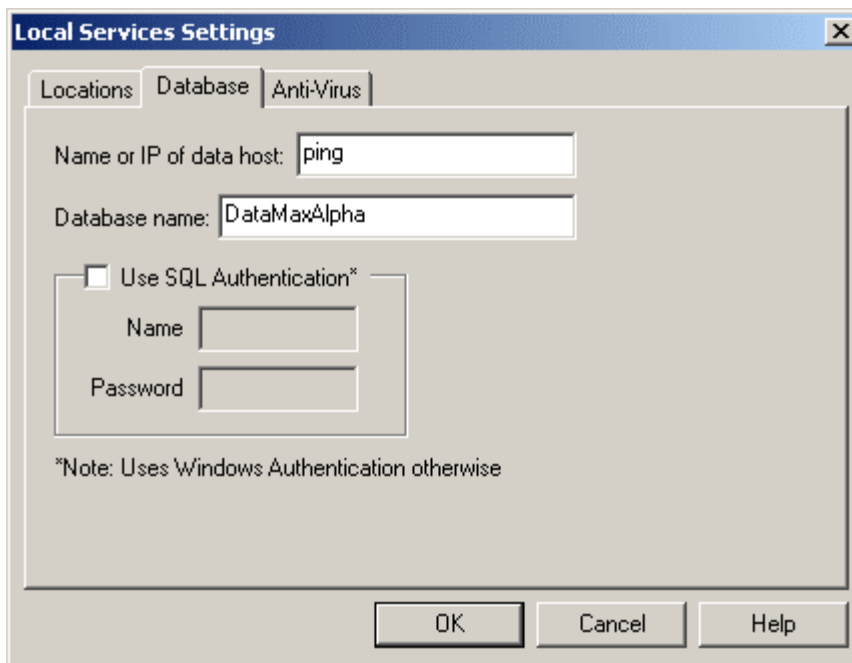
SMTP Working Directories

The Inbound and Working directories are in constant use by SMTPMax and are emptied as quickly as possible. However, the ETRN directory can potentially accumulate a lot of files. In a multiple-disk hardware configuration, reserve your larger drive for the ETRN directory. The "Virus def." directory is where the internal virus scanning software keeps virus definitions.

DataMax Location and Password

The servers on the computer on which this is run need to know where to find DataMax and the password to log onto DataMax. If the server and DataMax reside on the same computer, **127.0.0.1** can be used for the IP.

3.2 Local Service Settings - Database



The screenshot shows a dialog box titled "Local Services Settings" with three tabs: "Locations", "Database", and "Anti-Virus". The "Database" tab is selected. It contains the following fields and controls:

- "Name or IP of data host:" text box with the value "ping".
- "Database name:" text box with the value "DataMaxAlpha".
- An unchecked checkbox labeled "Use SQL Authentication*".
- A sub-dialog box containing:
 - "Name" text box.
 - "Password" text box.
- A note at the bottom: "*Note: Uses Windows Authentication otherwise".
- Buttons for "OK", "Cancel", and "Help" at the bottom right.

Just as the services need to know where to find DataMax, it needs to know where to find SQL server and its data.

Name or IP of data host

Enter the network name or the IP of the host where SQL Server (or SQL Server 2000 Desktop Engine) is running.

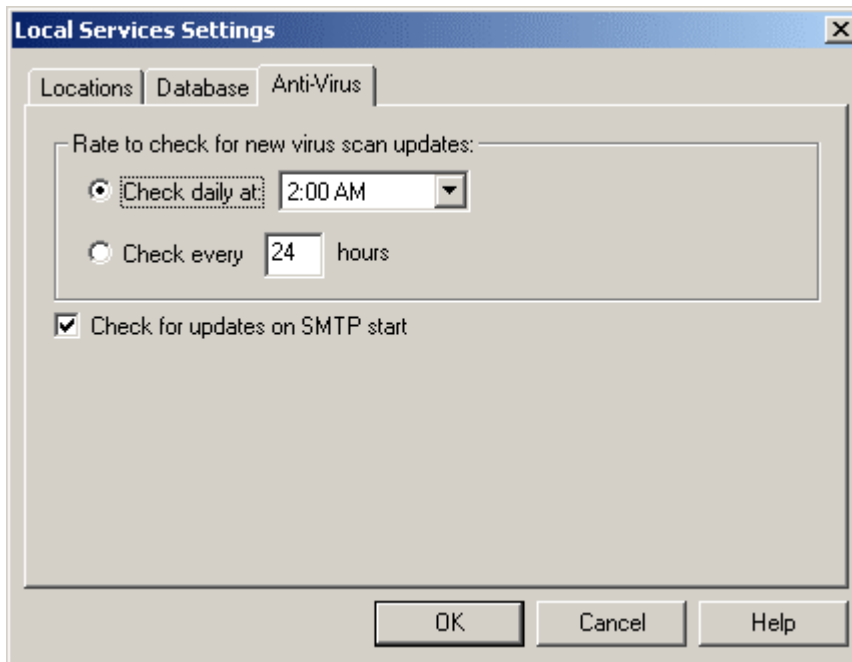
Database Name

Enter the name of the database for DataMax to use. If the database is not one DataMax expects, it will simply shut down and not cause any harm to the database entered.

Use SQL Authentication

The default behavior for DataMax is to use Windows NT authentication to access SQL Server. If your SQL Server is configured for independent authentication to use the database, then enable SQL Authentication and enter the name and password DataMax should use to connect to SQL Server.

3.3 Local Service Settings – Anti-Virus



SMTP Max checks for updates to the anti-virus software you have installed. You can set how often the check happens. Note: While mail continues being received, the "back-end" processing that delivers mail comes to a halt while SMTPMax checks for updates. It is recommended that you don't check more often than you feel you really need updates.

Check Daily at:

The time of day is used as the time to check for updates.

Check every ____ hours

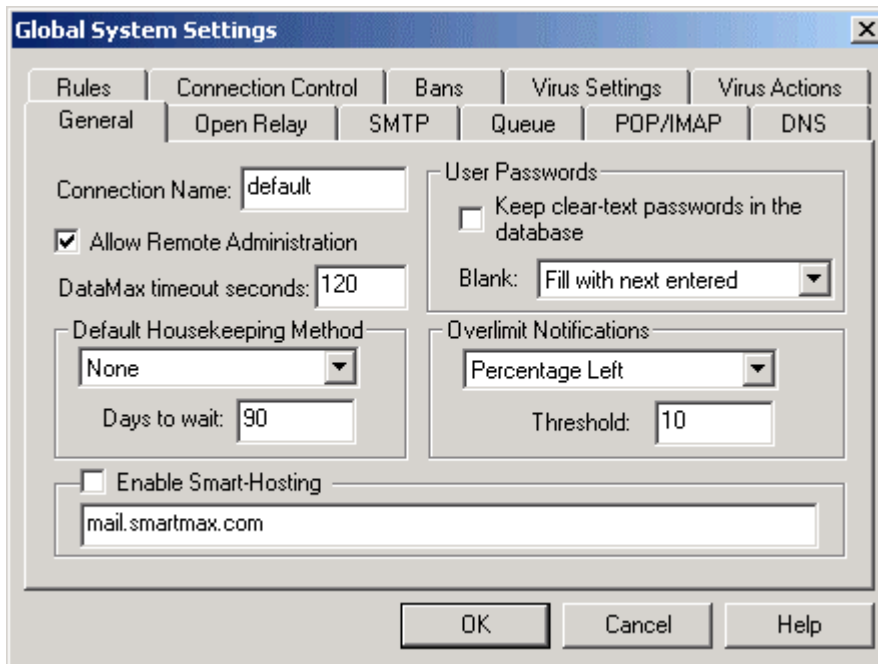
Enter how often to check for the updates.

Check for updates on SMTP start

If checked, then SMTPMax will scan for updates when the service is started and before processing any mail.

4 Global System Settings

4.1 Global System Settings - General



These are the general settings for the MailMax system.

Connection Name

This is used to identify a system in a clustered arrangement. If your system is not clustered, the name has no effect.

Allow Remote Administration

Check this to allow users to do remote administration of domains. Keep in mind; this does *not* automatically make anyone an administrator. Users must actually be set to administer specific domains.

DataMax timeout seconds

This is the amount of time before DataMax decides that a connection is inactive. Unless actively developing extensions for MailMax, 120 seconds is the recommended default.

Default Housekeeping Method

Set the house-keeping method to one of:

Disabled - no housekeeping for this domain

Messages by Age - delete messages from the system that are over a certain number of days

Users by Age - delete users who have not connected to POP or IMAP over a certain number of days

Days to Wait

Enter the number of days to use for one of the above housekeeping schemes.

User Passwords

Use the following settings for passwords:

Keep clear-text passwords

DataMax normally will encrypt passwords before placing in the database to prevent casual snooping should someone obtain access to your computer's hardware. If this option is selected, then passwords will be kept in the database as plain text. Even if the passwords are encrypted in the database, plain-text passwords may still be entered into the database and POPMax and IMAPMax will still validate users properly.

Blank

This setting controls the disposition of users with blank passwords. One of the following may be chosen:

Fill with next entered - since most users have their e-mail passwords automated, this will let the user's next connection to Poppa or IMAPMax immediately be accepted and the password used is entered into the database as the user's new password.

Use no password - POPMax and IMAPMax will disregard the password sent by the mail client and immediately allow connection.

Disable user - Users with blank passwords cannot connect at all.

Over limit Notifications

When users reach their limit on their boxes, MailMax can send them notifications. Use one of the following default schemes:

None - no notice is sent.

Percentage left - when the box drops below a given percentage (see Threshold below) the notice is sent.

Hard Limit (MB) - when the box gets below a give number of megabytes remaining (see Threshold below), the notice is sent.

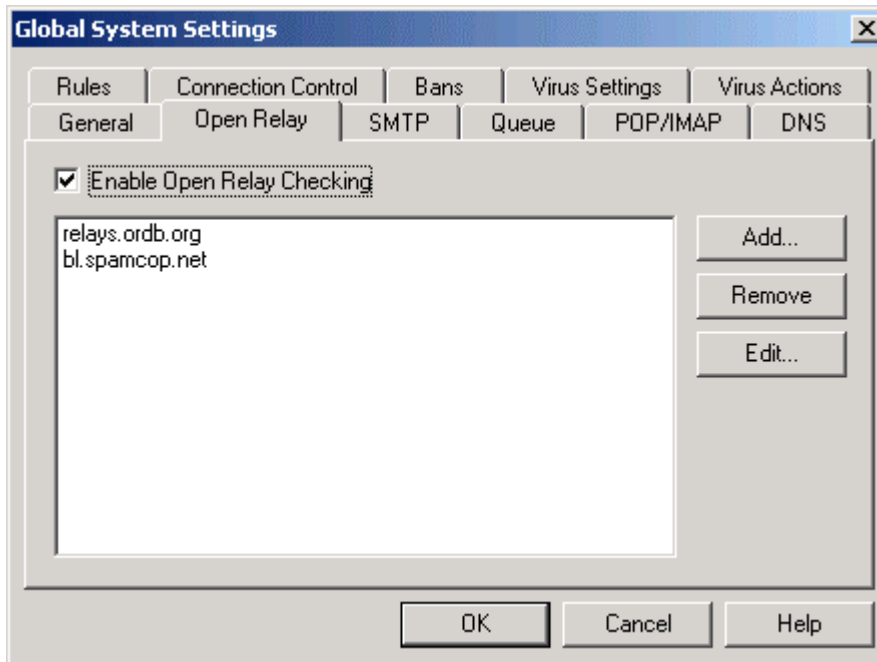
Threshold

Enter a value that is either a percentage or a number of megabytes depending on the over limit notice method set above.

Enable Smart-Hosting

This option enables Smart-hosting for the system. All outbound mail is directed immediately to the smart-host regardless of destination. The smart-host then has the duty to distribute the mail to the appropriate destination. Specify either a domain name or its IP.

4.2 Global System Settings - Open Relay



Open relay checking is yet another method of stopping spam. When clients connect to SMTPMax, before any activity occurs, SMTPMax will contact the servers in this list to see if the client is connecting from a listed open-relay server. An Open Relay Server is a Mail Server that anyone can send mail through and they are the cause of a vast majority of the spam on the internet. Servers that track Open Relay Servers normally are commercial services. SmartMax Software, Inc. neither provides nor endorses any open relay checking services.

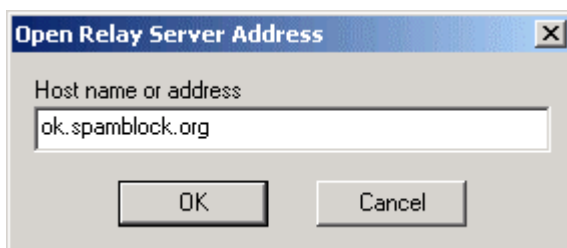
Note: Open Relay List checks do not create a significant performance impact on SMTPMax, but they do, however, introduce delays for clients as SMTPMax waits for results from the Open Relay List.

Enable Open Relay Checking

If selected, the servers below will be checked for clients which are open relays.

Add...

Adds a new open relay service. Enter the system name of the Open Relay Server or its IP.



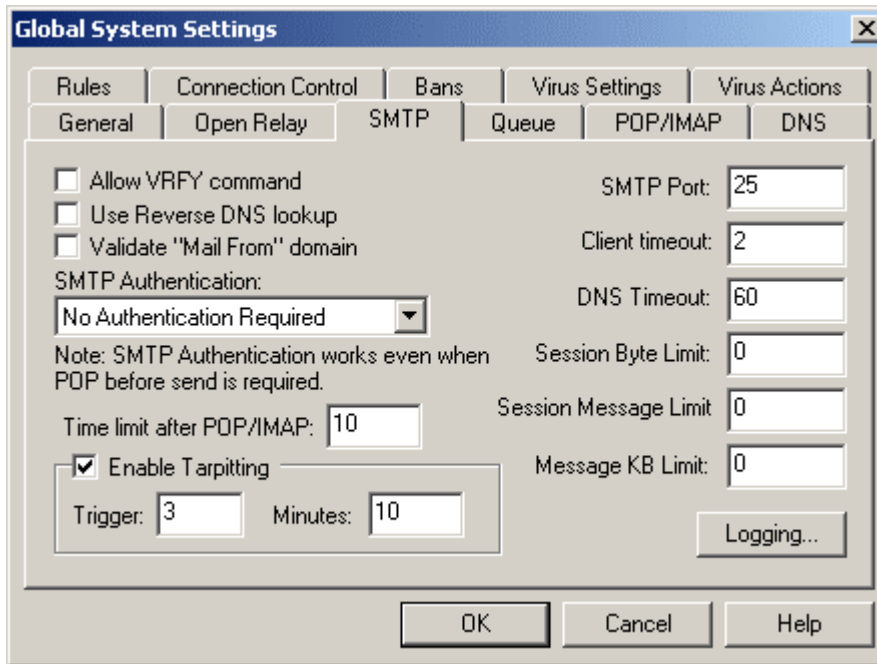
Remove

Removes the selected open relay service.

Edit...

Edits the selected open relay service.

4.3 Global System Settings - SMTP



These are the global settings for SMTPMax.

Allow VRFY command

This is normally considered a security leak in SMTP. It allows a client to ask the SMTP server if a user exists.

Use Reverse DNS lookup

When a connection comes in to SMTPMax, its IP must resolve to a named domain somewhere.

Validate "Mail From" domain

SMTPMax will verify that the domain after the @ in the "Mail From" command actually exists.

SMTP Authentication

This is the method that clients must use to authenticate themselves before using SMTPMax. Note that if SMTP authentication is set, and a user has just used POP or IMAP within the time limit, then the user is considered authorized and no SMTP authentication need be performed.

No Authentication Required

Require SMTP authentication - requires SMTP authentication protocol to be used between the client and SMTPMax.

Require POP/IMAP before send -- Before sending mail, a client connecting from a given IP must have either used POP or IMAP within the immediate past. (See Time limit after POP/IMAP below)

Time Limit after POP/IMAP

For the "Require POP/IMAP before send", this sets how long to consider the IP valid. The time limit is in minutes.

SMTP Authentication

Some SMTP clients are capable of doing authentication. This should be one of the following:
None - Authentication should not be used

Allowed - Authentication may be used if the client tries to authenticate. If not, authentication is not needed.

Required - SMTP clients are required to authenticate themselves to SMTPMax

SMTP Port

The default port to use for SMTP for all domains. 25 is the standard port for SMTP.

Client Timeout

How many minutes to wait for commands from a client before disconnecting.

DNS Timeout

How many seconds to wait for DNS responses for Reverse DNS lookup or "Mail From" validation.

Session Byte Limit

The default limit on how many bytes a client may send in a single connection to SMTPMax. Use 0 for unlimited.

Session Message Limit

The default limit on how many messages a client may send in a single connection to SMTPMax. Use 0 for unlimited.

Message KB Limit

The default limit on the size of a single message that may be sent to SMTPMax. Use 0 for unlimited.

Enable Tarpitting

"Tarpitting" is the process of detecting that a client is sending mail to multiple bogus or random recipients. For example, a spammer might have a list of thousands of names that will be tried in hopes that a few manage to be valid on the target server. When such an assault is detected by SMTPMax, the conversation is terminated and the client is blocked from re-trying for a period of time.

Trigger

This is the number of bogus recipients that must be received in a session that causes SMTPMax to tarpit the client.

Minutes

The number of minutes that the client is tarpitted before being allowed to re-try sending mail.

Logging...

Click this to set SMTP Logging events.

4.3.1 SMTP Logging



SMTPMax logging tells SMTPMax to save assorted events to a log file. To control where SMTPMax puts its logs, see the Local Service Settings dialog.

Logging Rate

The rate that the log file runs can be one of the following:

Never - never logs events

Unlimited - saves events to one log file

Hourly - creates a new log file each hour

Daily - creates a new log file once each day at midnight

Weekly - creates a new log file at midnight between Saturday and Sunday

Monthly - creates a new log file at the start of each month

Events to Log

When selected, the following events will be saved to the log file. Some events fit in multiple categories. For example, "Connections" also include "logins."

Connections

All inbound connections.

User Entries

All text sent from the client in the form of commands. The actual body any e-mail is not logged.

SMTP Conversation

Full conversations back and forth between the client and the server.

Error Messages

Errors generated during a session.

Logins

All attempts at authentication, success or failure.

Valid SMTP commands

Only standard SMTP, valid SMTP commands.

Internal Processing

Used to create logs from debug versions of SMTPMax

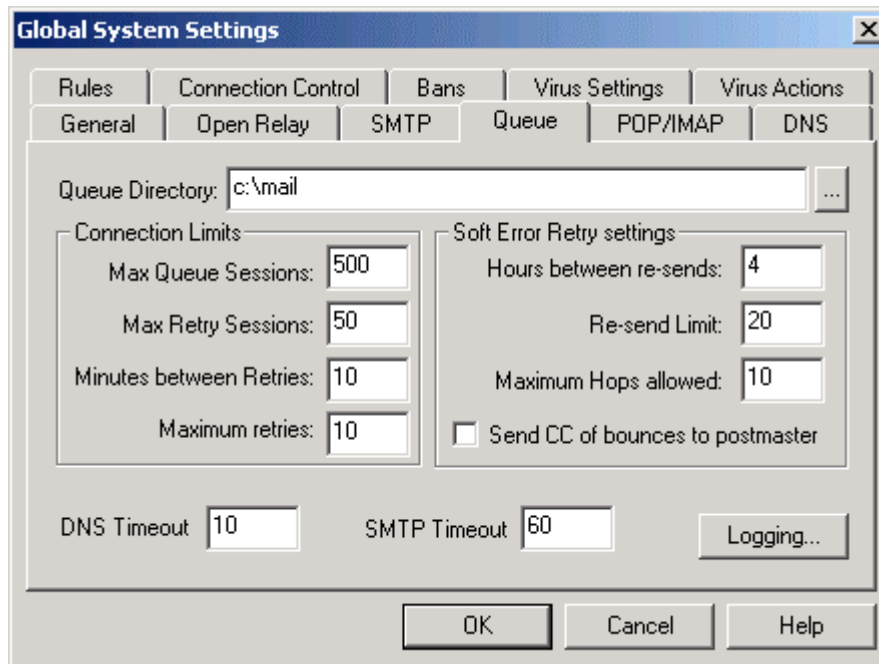
Banned Connections

Logs all attempts to connect from banned or blocked clients.

DATA text

This logs the body data of any inbound mail. This typically can flood a log file and is used only for extreme logging while actually monitoring debug conditions.

4.4 Global System Settings - Queue



These are the global settings for QueueMax, the outbound mail service.

Queue Directory

Enter the directory where mail is queued to send out to other mail systems. If using network drives, remember that SMTPMax and QueueMax share this directory and if necessary because they run on separate computers, a UNC path should be used.

Connection Limits

These are the assorted timeout limits for QueueMax.

Max Queue Settings

This is the maximum number of running simultaneous outbound connections. A piece of mail enters this queue just once. Should it fail to connect (or timeout after connect), it will get placed in a retry queue.

Max Retry Sessions

Mail that did not make it to its destination on the first attempt, are placed in the retry queue. It is assumed that mail is in this queue because the host had problems. The retry queue waits some time before trying to connect to the remote host and will retry up to the limits specified below. Should the retries fail, QueueMax will place the e-mail into the Soft Retry queue.

Minutes between Retries

For the retry queue, this specifies how long to wait before trying to send the mail again.

Maximum Retries

This is how many times a piece of mail will try to go out before being relegated to the soft error queue.

Soft Error Retry Settings

Mail can fail for a variety of legitimate reasons that deserve resending. For example, the user's mail-box is full. Mail that enters the soft-error queue will cause a bounce message to be sent to the original sender of the mail indicating the reason for the failure and that QueueMax will continue to retry sending. Also note that if mail fails immediately because of unrecoverable errors, it will immediately enter the soft error queue.

Hours between re-sends

The amount of time to wait between retries. Four hours is a fairly common retry rate.

Re-send Limit

Maximum number of retries before giving up completely.

Maximum Hops Allowed

Each time mail goes through any server, that server puts its "fingerprints" at the start of the e-mail. From this it is possible to determine how many servers that the mail has been to. It is even possible for mail to be forwarded from place to place in a circle of servers. By selecting a maximum number of hops to allow, this stops mail from floating in the internet forever, and will generate an error return message to the original sender.

Send CC of bounces to postmaster.

This is mostly used for tracing problems with mail. Copies of all bounced messages are sent to the account called "postmaster" (if it exists).

DNS Timeout

This instructs the DNS (when resolving addresses of servers), not to wait more than this number of seconds for a DNS to reply to the request for the server's IP.

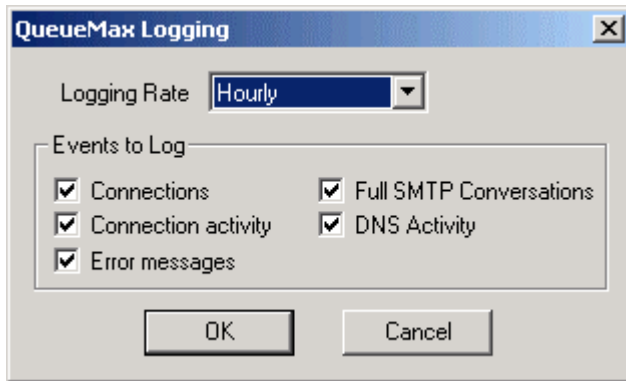
SMTP Timeout

This settings instructs QueueMax (should it connect to an SMTP server successfully), to wait no longer than this number of seconds for responses from the server before deciding that it has died.

Logging

Click this to set logging for QueueMax.

4.4.1 QueueMax Logging



QueueMax logging tells QueueMax to save assorted events to a log file. To control where QueueMax puts its logs, see the Local Service Settings dialog.

Logging Rate

The rate that the log file runs can be one of the following:

Never - never logs events

Unlimited - saves events to one log file

Hourly - creates a new log file each hour

Daily - creates a new log file once each day at Midnight

Weekly - creates a new log file at midnight between Saturday and Sunday

Monthly - creates a new log file at the start of each month

Events to Log

When selected, the following events will be saved to the log file. Some events fit in multiple categories.

Connections

All outbound connections (successful and otherwise).

Connection Activity

All connection related messages exchanged between the client and the server.

Error Messages

Errors generated during a session

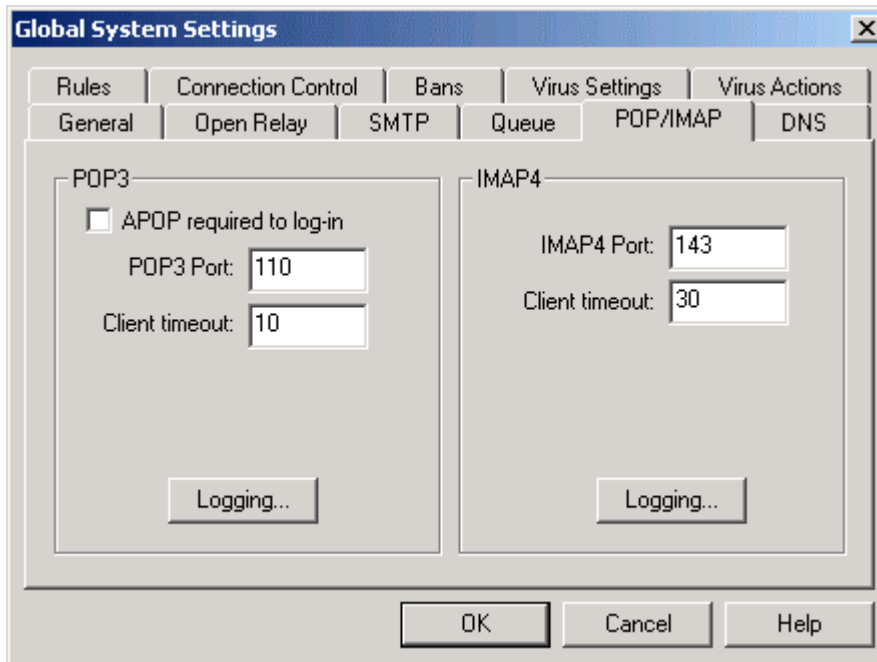
Full SMTP Conversations

Except for the body of DATA commands, this is the entire conversation between QueueMax and the remote host.

DNS Activity

Reports all commands and responses to the DNS.

4.5 Global System Settings - POP/IMAP



These are the general settings for POP and IMAP.

4.5.1 POP3 Settings

APOP required to log-in

APOP is a scheme for POP which allows encrypting of passwords when the user connects. Both the client and server scramble the password plus the login time stamp using the MD5 encryption scheme and only the irreversible data is transmitted between client and server. Not all POP3 clients support this feature, so use with care. It should only be used for a relatively high-security environment.

POP3 Port

This is the system-wide default port for POP3. This should normally be 110.

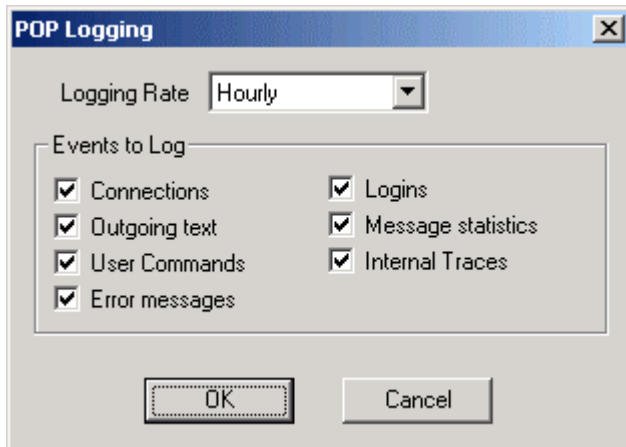
Client timeout

This is the time in seconds before clients are disconnected due to inactivity.

Logging...

Click this to set up logging for POPMax.

4.5.2 POP Logging



POP logging tells POP to save assorted events to a log file. To control where POP puts its logs, see the Local Service Settings dialog.

Logging Rate

The rate that the log file runs can be one of the following:

Never - never logs events

Unlimited - saves events to one log file

Hourly - creates a new log file each hour

Daily - creates a new log file once each day at Midnight

Weekly - creates a new log file at midnight between Saturday and Sunday

Monthly - creates a new log file at the start of each month

Events to Log

When selected, the following events will be saved to the log file. Some events fit in multiple categories. For example, "Connections" also include "logins."

Connections

All connections and (un)successful logins.

Outgoing Text

Responses from the server to the client.

Error Messages

Errors generated during a session.

Logins

All valid and invalid login attempts. (NB: merely connecting is not a login attempt.)

Message Statistics

Summary information sent to the client. This normally occurs upon logging off.

Internal Traces

Used for debugging purposes. Dumps out specific internal events which normally are not in release builds of the server.

4.5.3 IMAP4 Settings

IMAP4 Port

This is the system-wide default port for IMAP3. This should normally be 143.

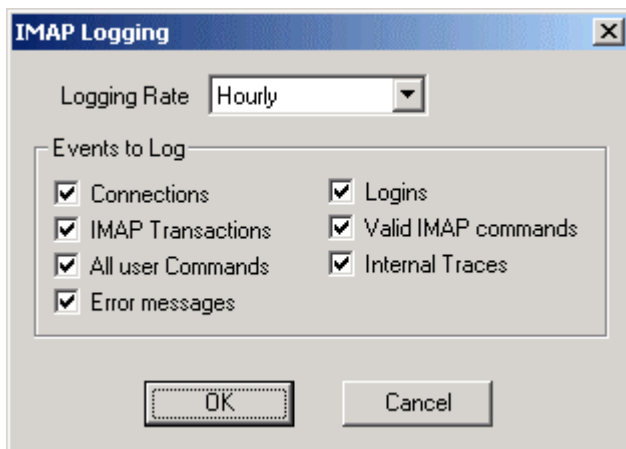
Client timeout

This is the time in seconds before clients are disconnected due to inactivity.

Logging...

Select this to set up logging for IMAPMax.

4.5.4 IMAP Logging



IMAP logging tells IMAP to save assorted events to a log file. To control where IMAP puts its logs, see the Local Service Settings dialog.

Logging Rate

The rate that the log file runs can be one of the following:

Never - never logs events

Unlimited - saves events to one log file

Hourly - creates a new log file each hour

Daily - creates a new log file once each day at midnight.

Weekly - creates a new log file at midnight between Saturday and Sunday

Monthly - creates a new log file at the start of each month

Events to Log

When selected, the following events will be saved to the log file. Some events fit in multiple categories. For example, "Connections" also include "logins."

Connections

All connections and (un)successful logins.

IMAP Transactions

All messages exchanged between the client and the server.

All User Commands

Every command sent from the user to the server (including invalid commands).

Error Messages

Errors generated during a session

Logins

All valid and invalid login attempts. (NB: merely connecting is not a login attempt)

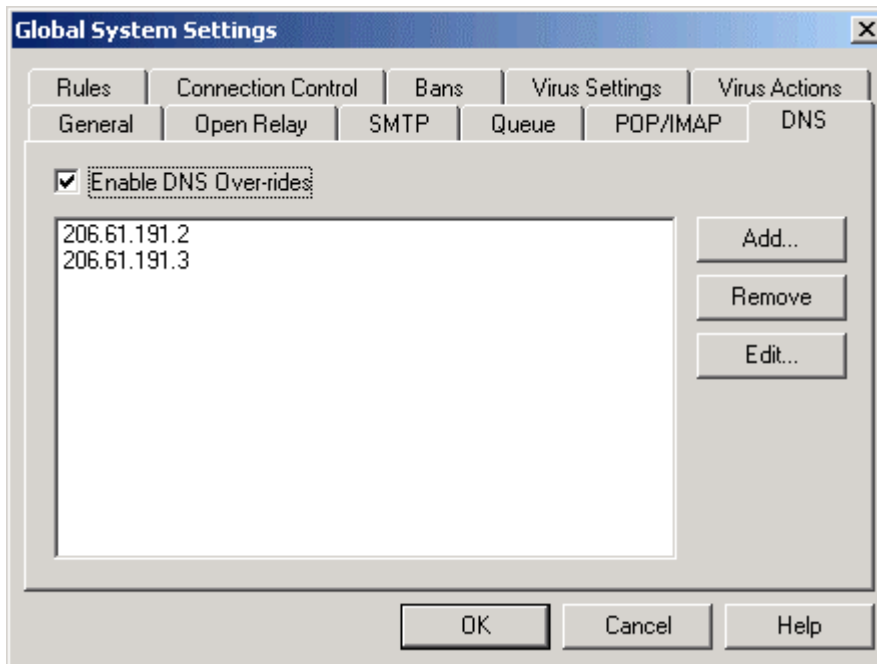
Valid IMAP commands

All legitimate commands sent to the server.

Internal Traces

Used for debugging purposes. Dumps out specific internal events which normally are not in release builds of the server.

4.6 Global System Settings - DNS



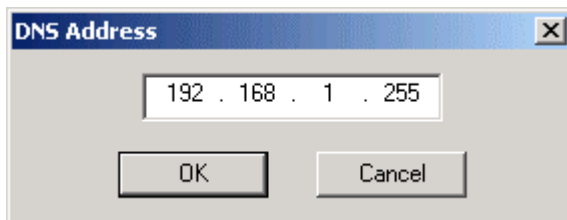
Normally, MailMax will depend on the standard system DNS to resolve addresses, however, an alternate list of DNS entries may be provided.

Enable DNS Over-rides

The list below will override the Window's default DNS settings.

Add...

Add a new DNS entry. Enter an IP address for the DNS to use.



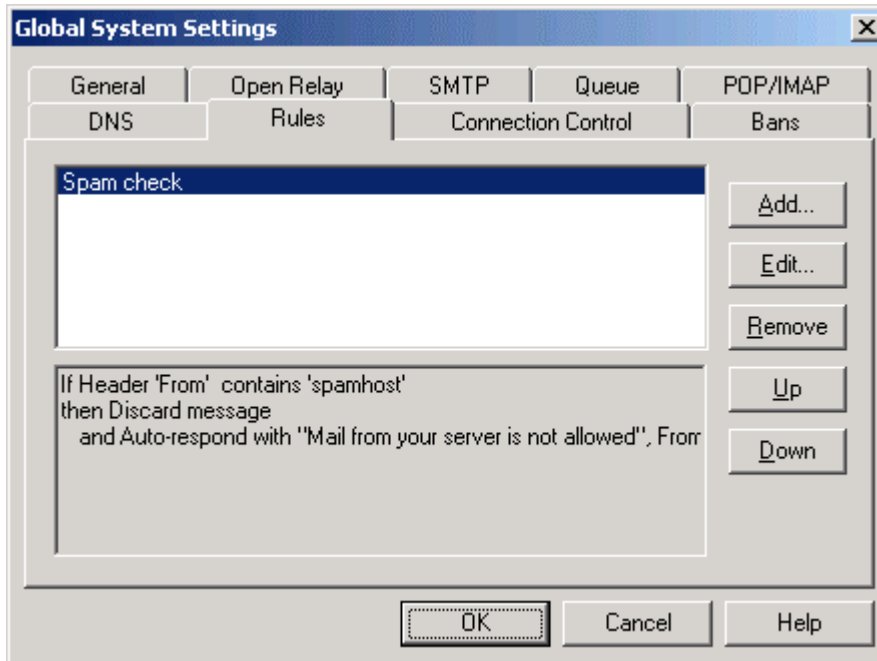
Remove

Remove the selected entry.

Edit...

Edit the selected DNS entry.

4.7 Global System Settings - Rules



The system rules are the rules applied to incoming mail for users. These rules are applied **before** both domain rules and user rules. The order of the rules is important to processing since one rule action is to terminate processing any other rules.

Add...

Click this to add a rule.

Edit...

Click this to edit the selected rule.

Remove

Click this to remove the selected rule.

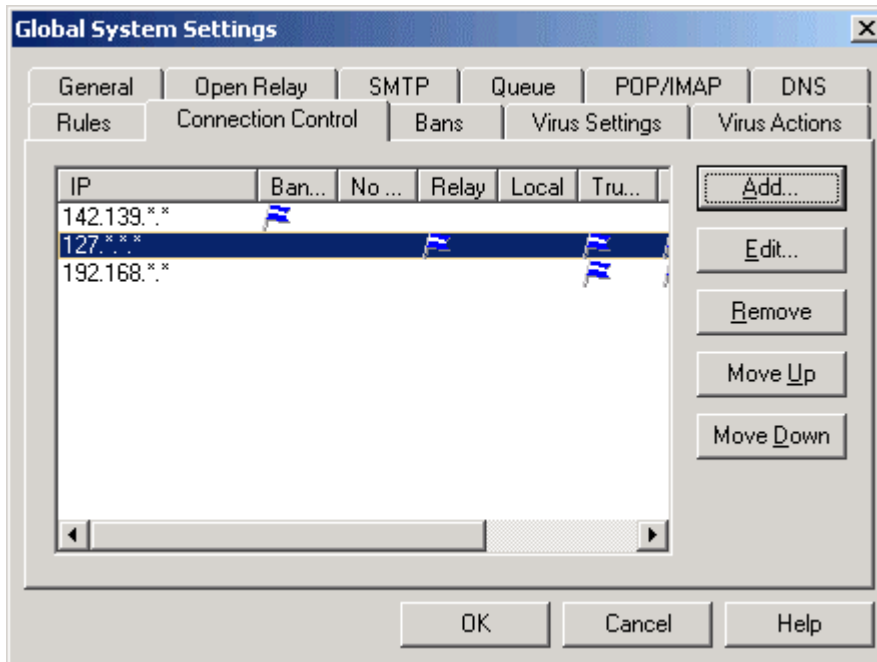
Up

Move the selected rule earlier in the list.

Down

Move the selected rule later in the list.

4.8 Global System Settings - Connection Control



The connections page shows known connections and how they are used. When a client connects to SMTPMax, SMTPMax compares the client's IP against the entries in this table in order. When a match is found, the flags set for the IP are applied and those flags in turn control what a client can do once connected to SMTPMax. Keep in mind that the sequence of the IP filters is important when the filters overlap. For example, if **147.89.**** is banned, and **147.89.8-15.*** is considered trusted, then those two ranges overlap. If the ban is encountered first, then the subsequent test match will not be found.

The column headers can be adjusted to see flags of interest. These correspond to the checkboxes in the IP Settings dialog (see 5.4).

These settings are applied to all connections to the MailMax system.

Add...

Add a new IP range to the list. The item is placed at the end of the list.

Edit...

Edit the flags for the selected IP range.

Remove

Removes the selected entry.

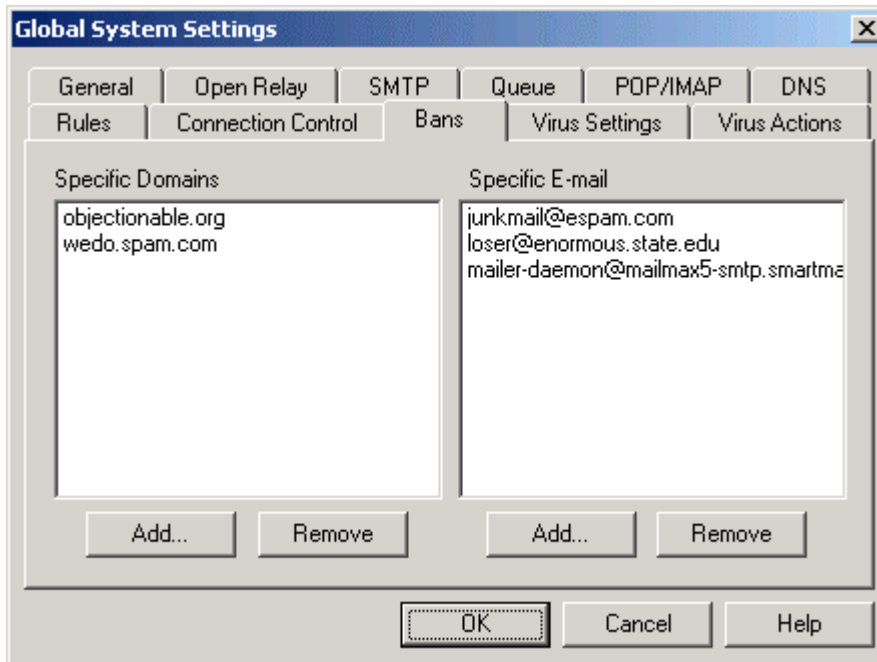
Move Up

Move the entry earlier in the test sequence.

Move Down

Move the entry later in the test sequence.

4.9 Global System Settings - Bans



Bans allow you to ban mail coming in from potential trouble-causing domains and users. These bans apply to all mail for all domains in the system.

Specific Domains

This is the list of domains whose mail should be blocked. Select one in order to use the Remove button.

Add...

Click to add a new domain to block.



Domain to block

Enter any legitimate domain name. Any mail that indicates it is from that domain will be rejected.

Remove

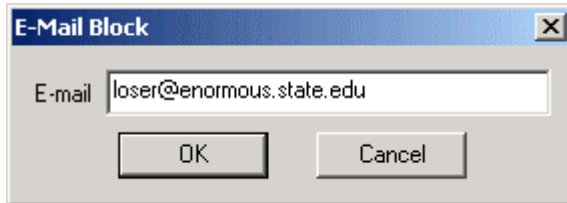
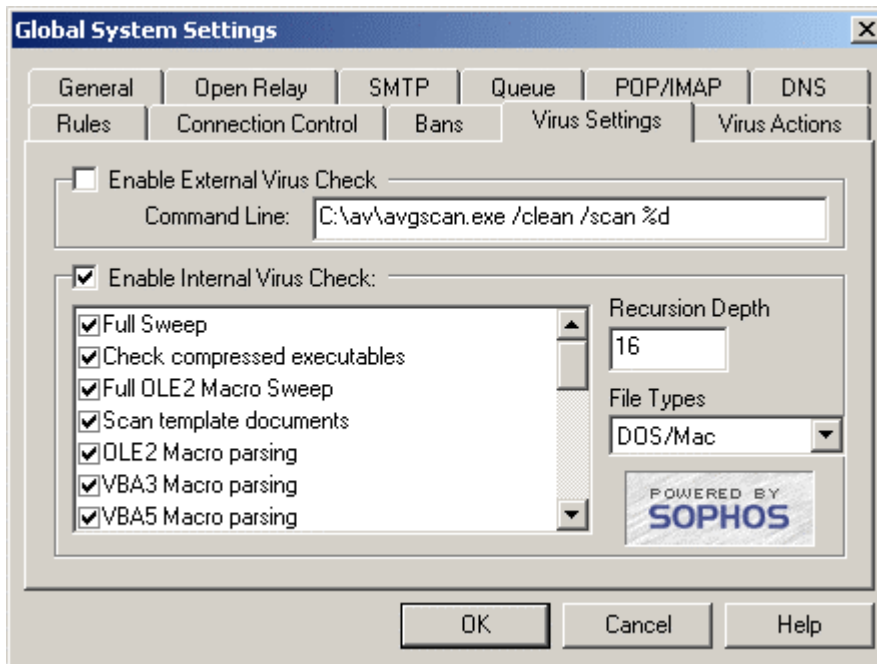
Select to remove the selected domain from the ban list.

Specific E-mail

This is the list of users whose e-mail should be blocked. Select one in order to use the Remove button.

Add...

Select to add a new e-mail address to block. Enter any legitimate e-mail address.

**4.10 Virus Settings**

Use this for configuring the internal and external virus checking for mail.

Enable External Virus Check

Check this box to enable the virus checker below. (Note: It does not have to be a virus check program. It could be any program that runs from the command line.)

Command Line

Enter the command line for the virus checker. It should consist of the path to the executable program to run, plus any additional command line arguments. If %d is placed in the command line, SMTPMax will replace it with the path to the directory where an extracted file attachment (or attachments) may be found. If the virus program removes any files from the directory, then the e-mail will be considered virus infected and will be discarded. The %d is case sensitive.

Examples:

Sophos command line:

```
"C:\Program Files\Sophos\sav32cli.exe" -di -ss -nb -nc -all -remove -archive %d
```

GRISOFT command line:

```
C:\av\avgscan.exe /clean /scan /arc %d
```

Enable Internal Virus Check

Enables the internal virus checker.

Recursion Depth

When encountering MIME e-mail with nested contents, this controls how deeply into the nesting that the virus scanner will scan.

File Types

For the Sophos virus checker, this is one of: DOS files, Macintosh files or both.

For the Avast virus checker, this is one of:

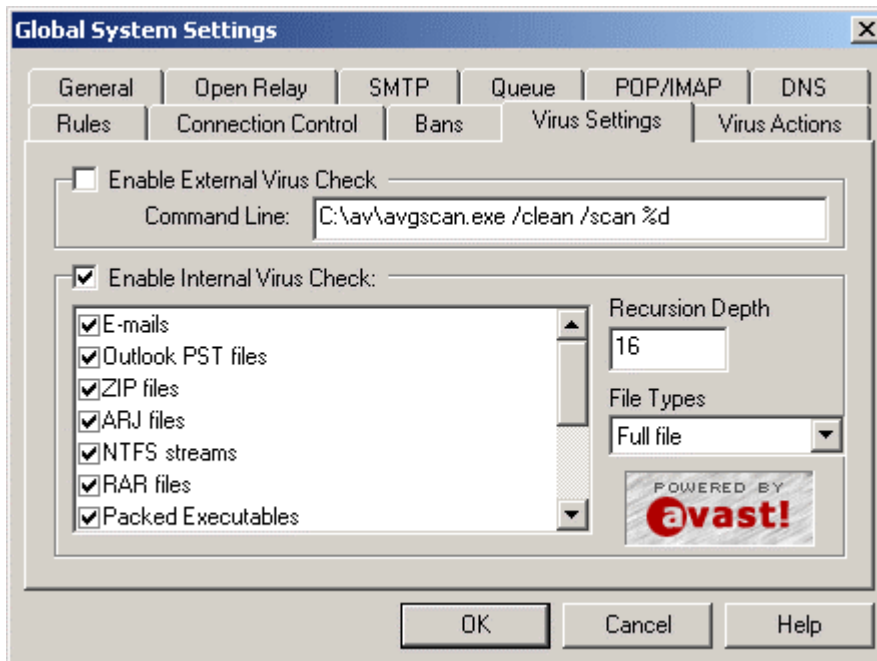
Full file. (More than 8K of the file is examined for viruses)

All files (Files other than .EXE files and libraries are tested.) Only first 8K of file tested.

Test all fully. (Full contents of all files are examined)

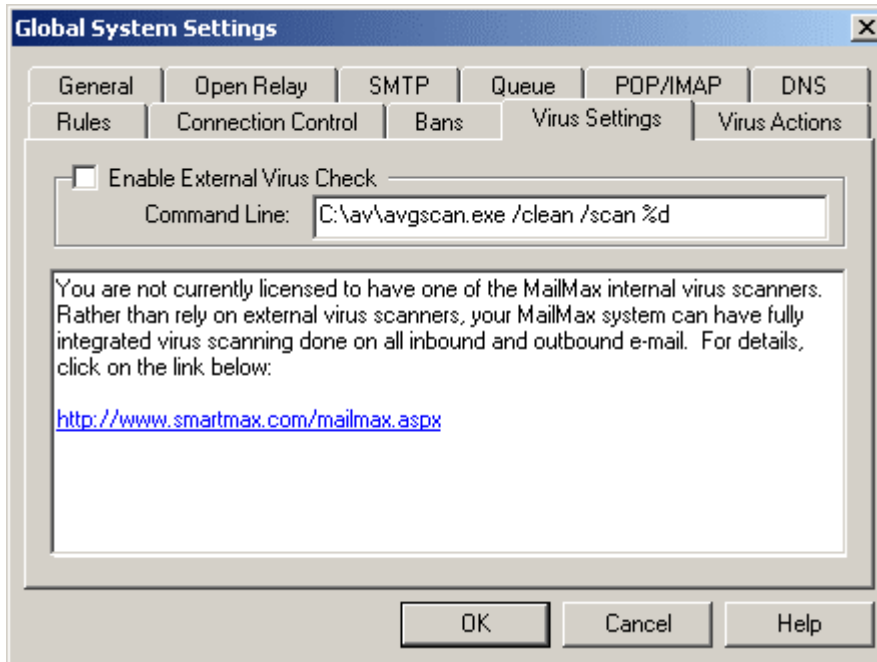
Avast! Virus checker

If you purchased the avast! virus checker you will see the following instead:



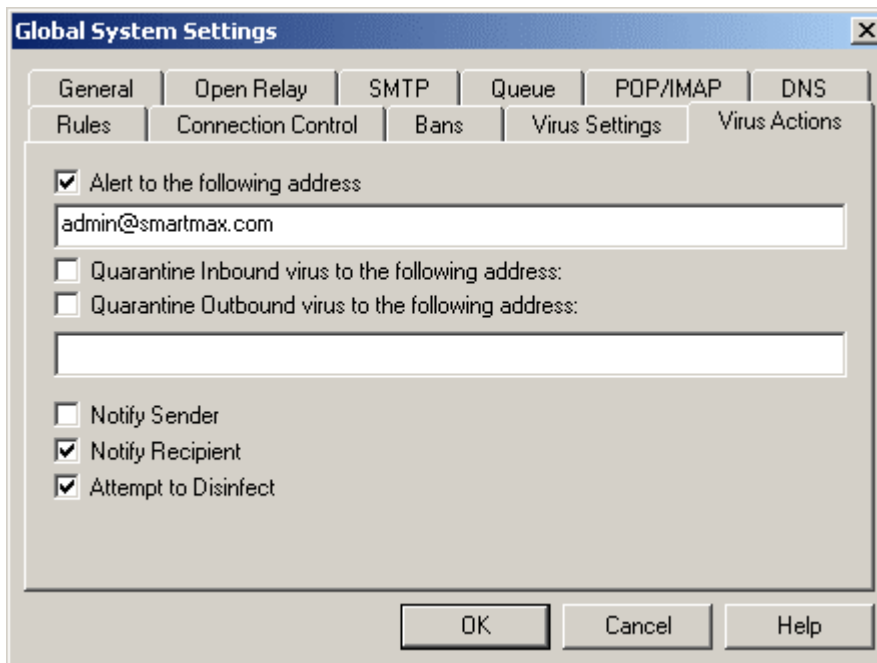
No Virus Checker

If you have not purchased an internal virus checker, you will see the following:



If you need an internal virus checker, please contact Smartmax Software, Inc. and we'll be happy to find one that fits your needs.

4.11 Virus Actions



These are the settings that control how the internal virus checker should dispose of detected viruses.

Alert to the following address

Sends an e-mail to the specified address that a virus has been detected.

Quarantine

Inbound and/or outbound mail with viruses will be routed to the address specified for later inspection or destruction.

Notify Sender

An e-mail alert will be sent to the sender of the virus.

Notify Recipient

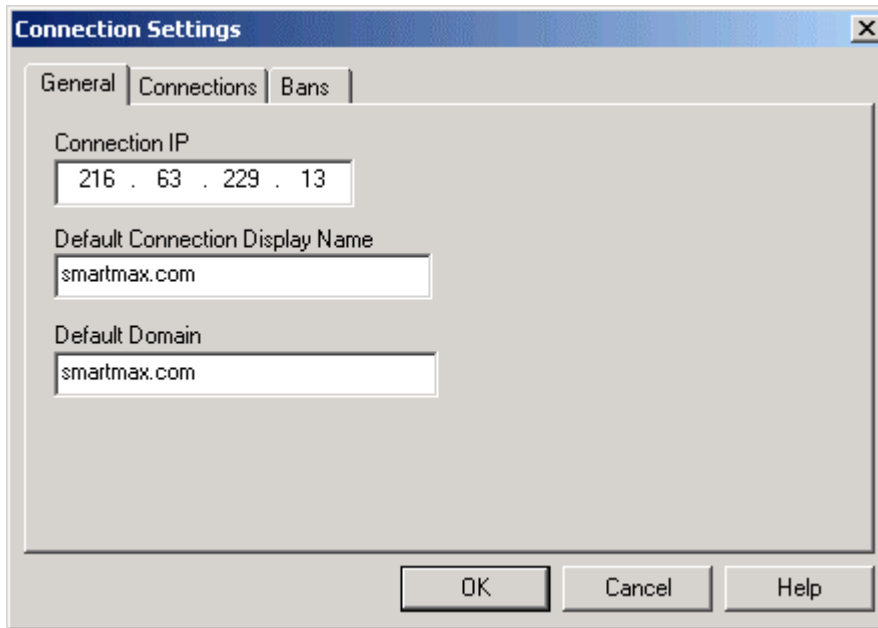
An e-mail alert will be sent to the recipient of the virus.

Attempt to Disinfect

An attempt will be made to remove the virus from the transferred executable and then it will be passed on through as "cleaned."

5 Connections

5.1 Connection Settings - General



Connection settings are used to create or set information for an IP that is used for services. Note: When editing a connection, you cannot change the IP. Once created, too many database objects depend on the IP not to change in the setup. To alter an IP, delete the old one and create a new entry.

Connection IP

An IP for the servers to use.

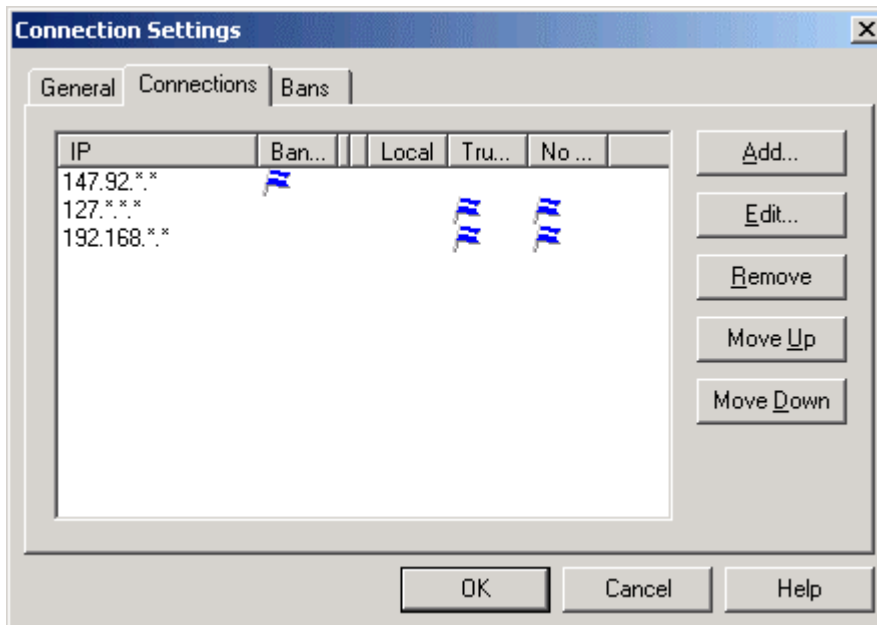
Default Connection Display Name

This is the name reported as the domain that represents the IP. More than one domain may be using this IP, so some "tourist information" is needed to give to client applications. This does not have to be a real domain, but it is wise to make it a real domain.

Default Domain

When users connect via POP or IMAP and a user-name is given to the server, then the default domain is checked for those users. For users *not* on the default domain, the user must attach a domain name to the login. POP and IMAP recognize a variety of explicit domains common to numerous e-mail clients. For example: ***user@domain.org***, ***user/domain.org***, ***user%domain.org***, ***domain.org/user***

5.2 Connection Settings - Connections



The connections page shows known connections and how they are used. When a client connects to SMTPMax, SMTPMax compares the client's IP against the entries in this table in order. When a match is found, the flags set for the IP are applied and those flags in turn control what a client can do once connected to SMTPMax. Keep in mind that the sequence of the IP filters is important when the filters overlap. For example, if **147.89.**** is banned, and **147.89.8-15.*** is considered trusted, then those two ranges overlap. If the ban is encountered first, then the subsequent test match will not be found.

The column headers can be adjusted to see flags of interest. These correspond to the checkboxes in the IP Settings dialog (see 5.4).

These settings apply only to clients who use this connection.

Add...

Add a new IP range to the list. The item is placed at the end of the list.

Edit...

Edit the flags for the selected IP range.

Remove...

Removes the selected entry.

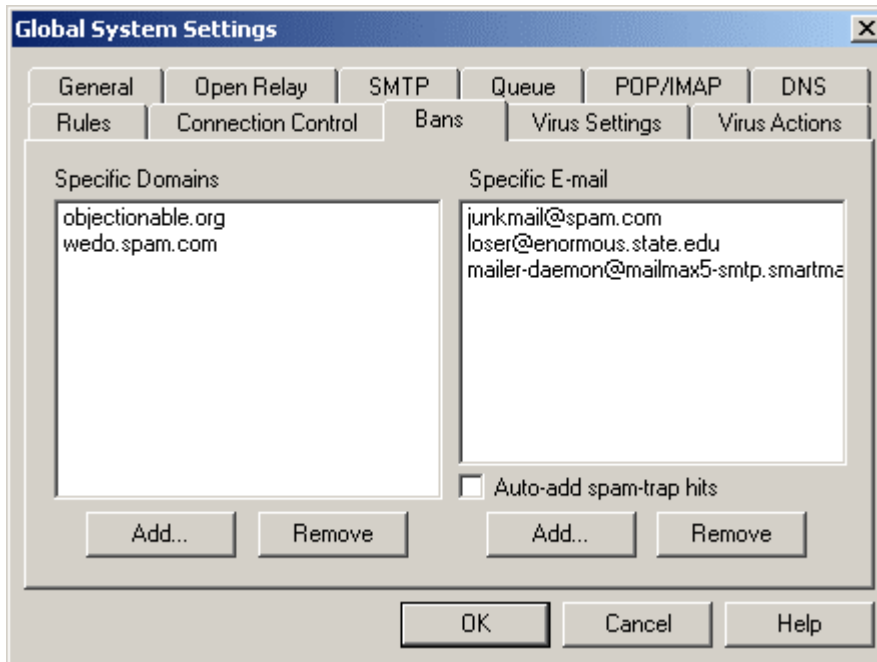
Move Up

Move the entry earlier in the test sequence.

Move Down

Move the entry later in the test sequence.

5.3 Connection Settings - Bans



Bans allow you to ban mail coming in from potential trouble-causing domains and users. The bans apply only to the selected connection.

Specific Domains

This is the list of domains whose mail should be blocked. Click one in order to use the Remove button

Add...

Click to add a new domain to block.



Domain to block

Enter any legitimate domain name. Any mail that indicates it is from that domain will be rejected.

Remove

Click to remove the selected domain from the ban list.

Specific E-mail

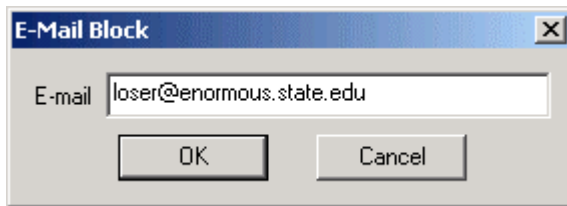
This is the list of users whose e-mail should be blocked. Click one in order to use the Remove button.

Add...

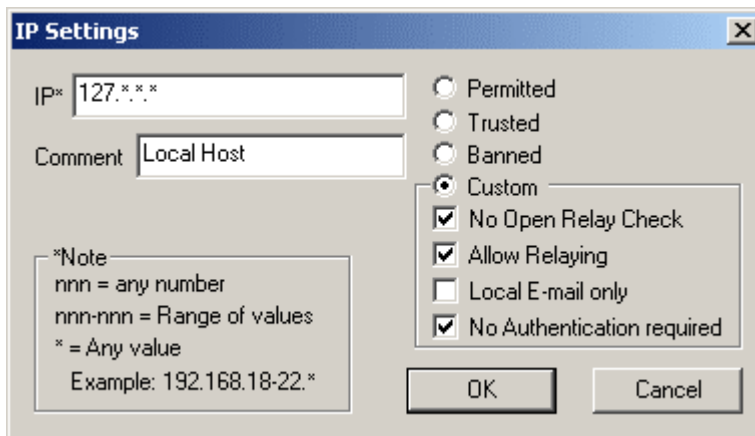
Click to add a new e-mail address to block. Enter any legitimate e-mail address.

Auto-add spam-trap hits

When mail arrives for a user whose account is of type spam-trap, the sender's e-mail will be added to the system-wide specific bans.



5.4 IP Settings



The IP settings are used to control access to a MailMax system prior to any actual authentication. The client's IP is compared against the IP settings and that client gets the selected limits/privileges.

IP

This is a filter for what IP's are affected by the flags below. This can be a specific IP, such as **192.168.1.10**. The value can be a range, such as **192.168.1.1-20**, which will affect **192.168.1.9**, but not **192.168.1.44**. You can use * as a shortcut for 0-255, for example, **192.168.1.*** which will effect **192.168.1.99**, but not **192.168.2.99**. If a client connects and its address matches the filter, then the flags listed below will be set for the connection. The IP settings are processed in order, so it is possible to ban a large range of IP's, but at the same time allow a few other IP's in the same range to connect. For example, to ban **192.168.*.*** but allow **192.168.1.20**, create the ban, but in the list of connections, precede the ban with **192.168.1.20** with the Trusted IP flag set.

Comment

Enter any descriptive comment you would like for the entry.

Permitted

Those connecting on the IP have normal access to SMTP

Trusted

Clients connecting from the IP are considered trusted and have no restrictions (such as having to authenticate or not allowed to relay mail)

Banned

The client is banned from connecting to the servers and will be disconnected immediately.

Custom

Set access based on the check-boxes below

No Open Relay Check

The client is reasonably trusted and will not be checked against any Open Relay List. This can be a performance enhancement for clients.

Allow Relaying

Relaying mail through a mail server can result in that server to be considered by the rest of the world as a Spam source. However, it may be that a host maintains a trusted secondary server that creates and relays mail through this server. This is a rather advanced and specialized arrangement. For most purposes, you should never enable relaying.

Local E-mail only

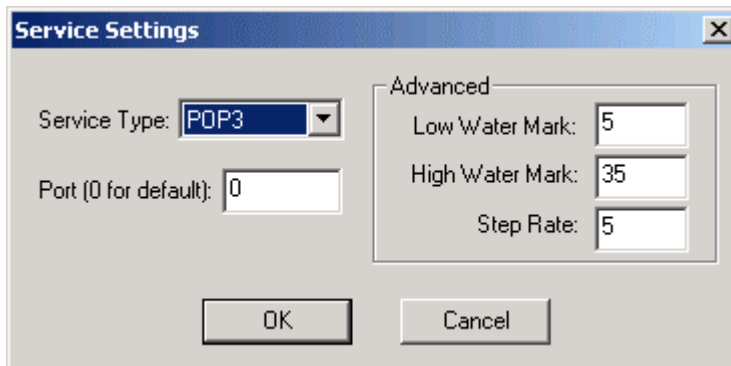
Those connecting can only send to local e-mail accounts.

No Authentication Required

For connections that require SMTP authentication in order to connect, set this flag to bypass the authentication for the IP(s) specified.

5.5 Service Settings

By right-clicking on a connection, you can add a new service to the IP. Normally, this isn't necessary because when you add a connection, all the basic services are added to the connect.



Service Type

One of POP3, IMAP4 or SMTP, depending on the service needed.

Port

This is the port the service runs on. Use 0 to use the system default.

Low Water Mark

This is the minimum number of connection sockets to keep alive waiting for clients to connect.

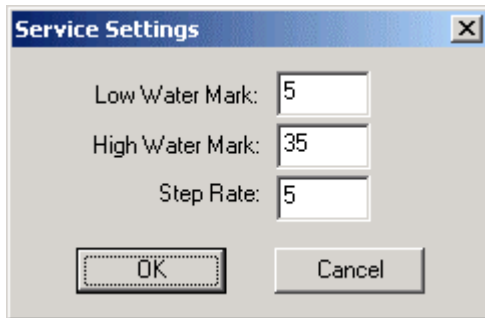
High Water Mark

If there are more open sockets than the High Water mark, they are disposed of to free up system resource.

Step Rate

This is the rate at which the service creates new connection sockets each time a client connects.

5.6 Editing Service Settings



Double-click a service entry to change the service settings. Unless told otherwise by SmartMax technical support, you should leave this set to the numbers you see above.

Low Water Mark

This is the minimum number of connection sockets to keep alive waiting for clients to connect.

High Water Mark

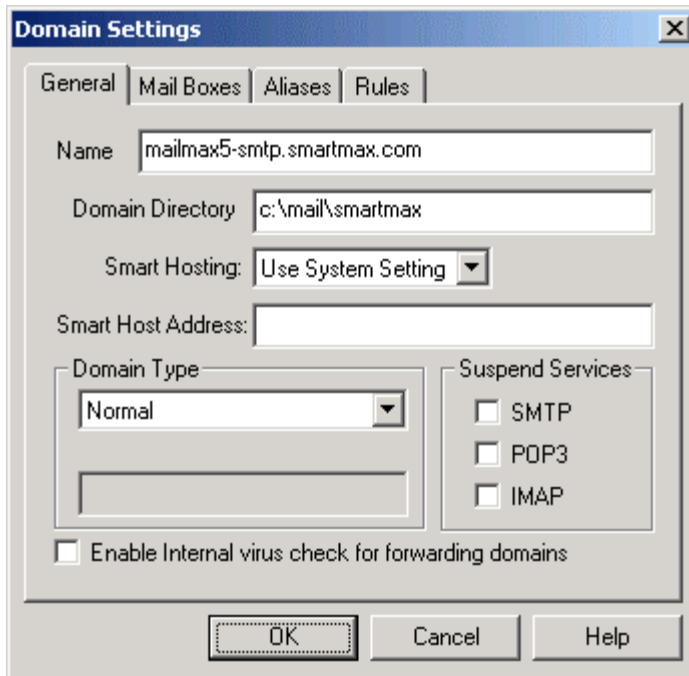
If there are more open sockets than the High Water mark, they are disposed of to free up system resource.

Step Rate

This is the rate at which the service creates new connection sockets each time a client connects.

6 Domain Settings

6.1 Domain Settings - General



A domain is what serves various users their e-mail.

Name

The registered name of the domain.

Domain Directory

Enter the drive name (or UNC path) where the mail should be stored for the users of this domain.

Smart Hosting

Use either the system smart hosting settings, or select Enable or Disable for this domain. (See also 6.5.1).

Smart Host Address

Enter the name of the registered domain for smart-hosting. If "Use System Setting" is selected above, then the system smart host address will be used.

Domain Type

Select one of the following:

Normal - Most domains will use this setting and it defines the domain as a conventional mail host.

Clustered - This domain is part of the domains used for a cluster of systems.

ETRN - This is an ETRN domain. The domain holds all mail locally until told to send to another host. (See 0).

Relay to Host - Routes all incoming mail to the server in the Delivery Address.

Backup - This domain is used to receive e-mail should the primary domain fail.

Delivery Address

When the domain type is a "Relay to Host" type, enter an IP or registered domain name for the server you wish to relay mail to.

Priority

Where the domain type is a Backup, enter the value that is to be used for the backup priority. See backup domains for details.

Enable Internal Virus Check

For domains types like ETRN, Relay or Backup, you can enable virus checking (depending on your license) for the mail being routed to the other mail server. This setting has no effect on Normal domains where mail is checked for viruses on an individual recipient basis.

6.2 Domain Settings - Mail Boxes

The screenshot shows the 'Domain Settings' dialog box with the 'Mail Boxes' tab selected. The settings are as follows:

- Boxes:**
 - Default Box Size (k): 0
 - Max User Boxes: 0
- Housekeeping:**
 - System Default (dropdown)
 - Days: 0
- Connection Sending Limits:**
 - MB: 0
 - Messages: 0
- Message Limit:** 0 kBytes
- Catch-All Account:** catchrest@smartmax.com
- Monitor Account:** monitor@smartmax.com
- Blank Passwords:** Use System Setting (dropdown)
- Overlimit Notice:** Use System Setting (dropdown)
- Threshold:** 0

Buttons at the bottom: OK, Cancel, Help.

These are all the mailbox default settings for the domain's users.

Default Box Size

This is the default upper limit for how much mail a user may have on the server. Enter an amount in kilobytes or 0 for unlimited.

Max User Boxes

A domain may have a limited number of users allowed. This setting is primarily for servers that are hosting domains and wish to limit how many users the domain administrators might add. Use 0 to have no limits on users for the domain.

Connection Sending Limits

The following two values limit how much mail a user in the domain may send in a single session.

Megabytes

Limits how many megabytes of mail the user may send in a single connection. Use 0 for

unlimited.

Messages

Limits how many mail messages the user may send in a single connection. Use 0 for unlimited.

Message MB Limit

Enter the number of megabytes that is the limit on size per message for users. Use 0 to use the system default.

Catch-All Account

Enter the fully qualified e-mail account that is to receive mail in the event that mail is sent to the domain, but the user does not exist. The domain for the catch-all account must already exist and the user account must exist as well. Typically, the catch-all account is one that exists in the domain that needs the catch-all account.

Housekeeping

Set the house-keeping method to one of:

System Default - Use the system settings for housekeeping

Disabled - No housekeeping for this domain

Messages by Age - Delete messages from the system that are over a certain number of days

Users by Age - Delete users who have not connected to POP or IMAP over a certain number of days.

Days

Enter the number of days you wish to run the selected method housekeeping schemes listed above.

Blank Passwords

If a user has a blank password, select one of the following actions to take when the user attempts to log in:

Use System Setting - Use whatever is set in the system settings

Fill with next entered - Whatever the user has for a password is immediately put in the database. Subsequent connections must continue using that password.

Use no password - Allow the user to log in no matter what password is sent

Disable user - No password is acceptable and the user may not connect

Overlimit Notice

An over-limit notice is sent to users when their boxes near full. Select one of the following methods:

Use System Setting - Use whatever is set in the system settings

None - No notice is sent

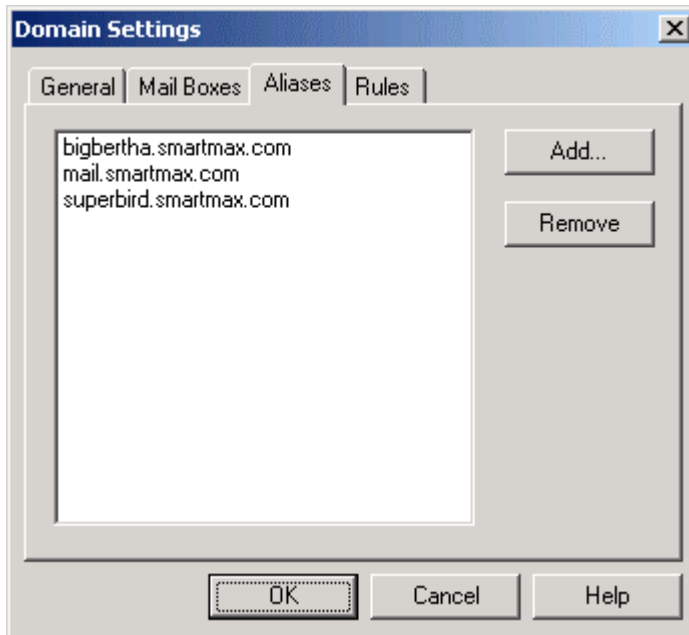
Percentage left - When the box drops below a given percentage (see Threshold below) the notice is sent.

Hard Limit (MB) - When the box gets below a give number of megabytes remaining (see Threshold below), the notice is sent.

Threshold

Enter a value that is either a percentage or a number of megabytes depending on the over-limit notice method set above.

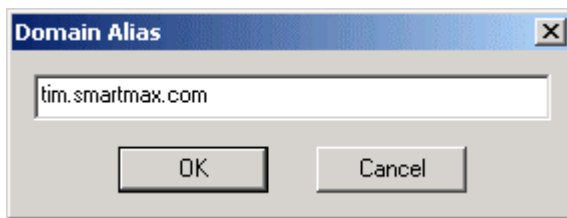
6.3 Domain Settings - Alias



A domain alias is used to allow mail to go to another domain on a MailMax system. For example, you can write to **support@smartmax.com** or **support@mail.smartmax.com** because **mail.smartmax.com** is an alias for the domain **smartmax.com**.

Add...

Allows you to add a new alias for the domain.



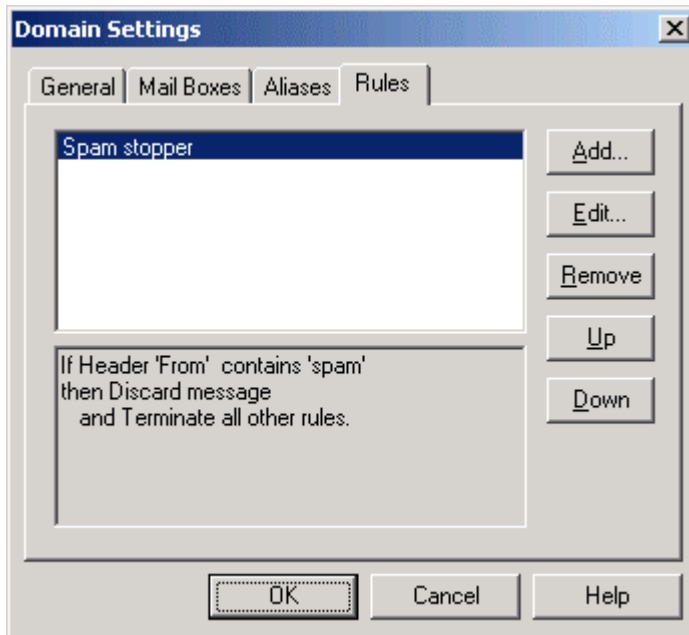
Domain Alias

Enter any legitimate, registered domain. (NB: If the domain is not registered, the alias will do nothing since no one else will know about it)

Remove

Removes the selected alias.

6.4 Domain Settings - Rules



The domain rules are the rules applied to incoming mail for users. These rules are applied **after** system rules and **before** user rules. The order of the rules is important to processing since one rule action is to terminate processing any other rules.

Add...

Click this to add a rule.

Edit...

Click this to edit the selected rule.

Remove

Click this to remove the selected rule.

Up

Move the selected rule earlier in the list.

Down

Move the selected rule later in the list.

6.5 Other Domain Issues

6.5.1 Smart Hosting

Use this feature to have MailMax deliver all outbound e-mail to a specified SMTP Server for final delivery. For example, you might have an internal Mail Server running without direct access to the internet, or you might simply want to send all outbound mail to your ISP's Mail Server to reduce the load on your internal network.

6.5.2 ETRN Domains

"ETRN" isn't so much a name as it is a command to an SMTP server. Mail to an ETRN

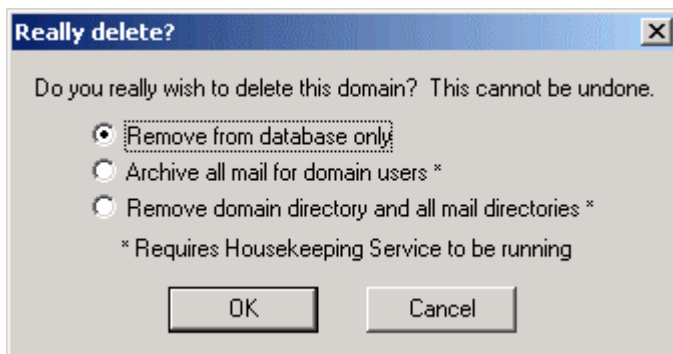
domain is simply accumulated and not sent anywhere. When SMTPMax is contacted and the ETRN command sent to it by the client, the mail is "de-spoiled" to the correct mail host.

6.5.3 Backup Domains

A backup domain is one designated to catch all e-mail for a primary e-mail server that might be inactive. A backup domain doesn't bother discriminating one user from another for purposes of directing e-mail. As soon as possible, mail directed to the backup domain tries to find the primary mail domain server and send it any accumulated mail.

It is beyond the scope of this document to detail setting up the MX records in your DNS to create mail system priorities, however, you will need sufficient knowledge of DNS configuration to attempt to create and use a backup domain. Your primary mail server needs a preference of a lower value than any backup mail server. When MailMax begins receiving mail destined for the backup domain, it is because other systems have tried to connect to your primary and have failed and have now sent to the backup. QueueMax will take mail from the backup and will routinely try to find any other server with its same domain name and lower preference number. Upon success, the mail will be routed to the primary as if it had never been down. A bit late, but better late than never.

6.6 Deleting Domains



When deleting domains, select the method of clean up for the domain. For the second and third options, the Housekeeping service must be running in order for the cleanup to take place. Cleanup is not necessarily immediate since housekeeping will get to this at its leisure.

Remove from database only.

All records related to the domain (including users, aliases and other references to the domain) are removed from the database.

Archive all mail for domain users

In addition to removing the domain from the database (as above), the mail storage folder for the domain will be renamed to the date the domain was removed. Consequently, the user mail for the domain will remain untouched on the hard-drive. Deleting the files after that time requires manual deleting.

Remove domain directory and all mail directories

In addition to removing the domain from the database (as above) all mail folders and files will be deleted completely.

7 User Settings

7.1 User Settings - General

The General settings for the user allow you to set most of the common values for users.

Name

This is the user's e-mail name. Valid user names for MailMax may contain alphanumeric characters plus the following special symbols:

^ _ { | } ` ! # \$ % & ' * + . - = ?

Caution: the use of special symbols other than the underscore ("_") is allowed, but discouraged as not all net-based programs that exist in the world recognize legitimate name symbols. (Our staff found one nationally recognized web-site that required an e-mail to use their service, but the programmer for the web-site didn't know that the dash was a legitimate e-mail character.)

Note: The slash ("/") is also a legitimate character for a mailbox, but we don't allow it because it is put to use separating an e-mail name from its domain for the sake of those with e-mail clients that use that as a protocol.

Important: When user passwords are kept in the database in encrypted form, they are only encrypted when the password is explicitly changed. The password encryption involves the user name at the time of encryption. Under the rare circumstances that the user name is changed, you should also specifically set the password or the "new" user won't be able to log in.

First Name

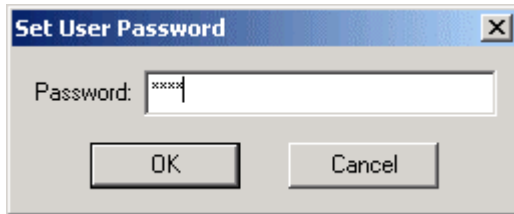
The user's real first name. (Not mandatory)

Last Name

The user's real last name. (Not mandatory)

Change Password

Click to change the user's password. Note: this password is NOT saved if "Cancel" is clicked for the user settings dialog. The password may not contain spaces.

**Account Type**

The user's account type can be one of the following:

Normal - Normal user e-mail account

Disabled - Normal account that has been disabled

Spam-Trap - This e-mail account is not designed to receive mail at all. It is, in fact, "bait" to lure spammers. Since no real human being exists to belong to this account and its presence is made known on the internet (via websites, newsgroups, etc.), then the only client program that would send mail to this account would be a client that is automatically cleaning e-mail addresses from the aforementioned sources. Anyone writing to a spam-trap can be safely assumed to be a spammer.

Disable SMTP Authentication

If SMTP authentication is normally required for users, selecting this will let the user send mail without authentication.

Disk Limit

This is the user's available disk space to hold e-mail. If the user is over-limit, mail to the user will be bounced back to the sender.

Housekeeping

These are the settings for housekeeping for the user.

Daily Sending Limits**Messages**

Limit in number of how many messages a user may send per day. Use 0 for unlimited.

Megabytes

Limit in megabytes to how much e-mail a user can send per day. Use 0 for unlimited.

Disable Sending Limits

Disables the sending limits set above for the user.

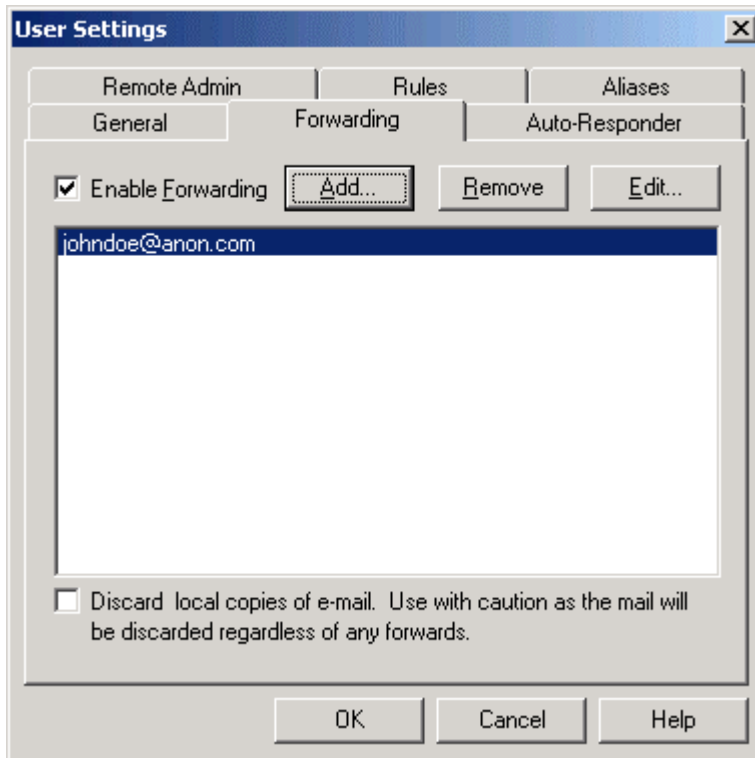
Message Limit

The largest e-mail a user may send (in kilobytes). Use 0 for unlimited size.

Enable Internal Virus Check

Enables running the internal virus check on mail to and from this user.

7.2 User Settings - Forwarding



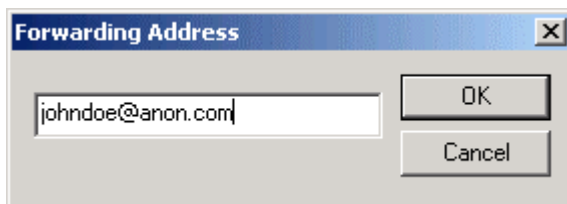
Users may forward their e-mail to any destination, both local to the host and on any other remote system.

Enable Forwarding

Enables or disables the forwarding list. For people who need forwarding because of a need to travel, the users can keep a permanent list of forwards, and then just enable or disable upon need.

Add...

Click to add a new forwarding address. Enter any legitimately formatted e-mail address. The address can be on the host system, or can be somewhere else in the world.



Remove

Click to remove the selected forwarding address.

Edit...

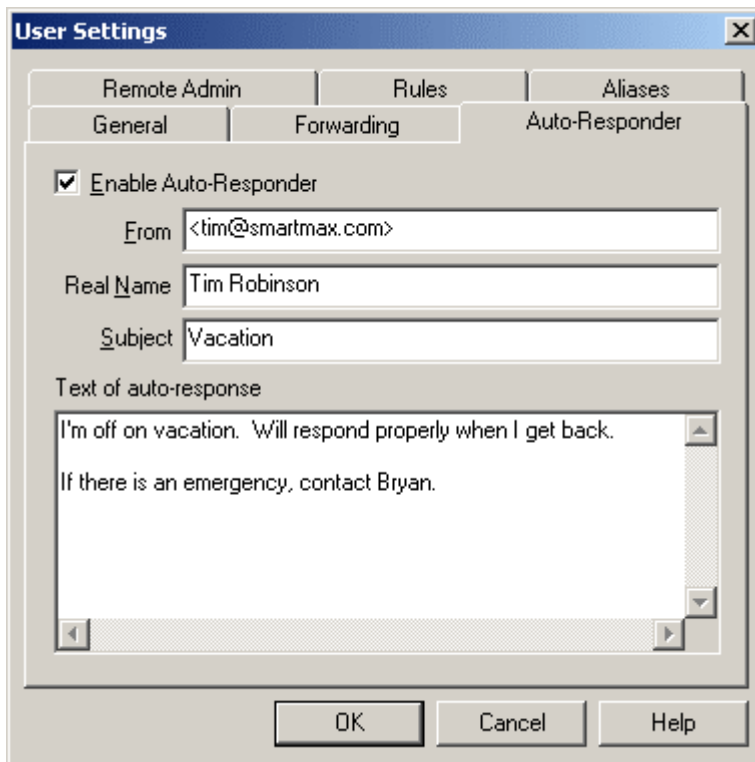
Click to edit the selected forwarding address.

Discard copies...

If this is enabled, then the e-mail will be forwarded to the addresses in the list, but no local copy will be retained. This is potentially hazardous because if the forward(s) for some reason

don't exist or won't accept the e-mail, then the mail will be lost.

7.3 User Settings – Auto-Responder



The screenshot shows the 'User Settings' dialog box with the 'Auto-Responder' tab selected. The 'Enable Auto-Responder' checkbox is checked. The 'From' field contains '<tim@smartmax.com>', the 'Real Name' field contains 'Tim Robinson', and the 'Subject' field contains 'Vacation'. The 'Text of auto-response' text area contains the following text: 'I'm off on vacation. Will respond properly when I get back. If there is an emergency, contact Bryan.' The dialog box has 'OK', 'Cancel', and 'Help' buttons at the bottom.

Auto-response mail is sent to anyone sending the user e-mail.

From

The e-mail to be used for any responses to the auto-response.

Real Name

The name to put on the e-mail.

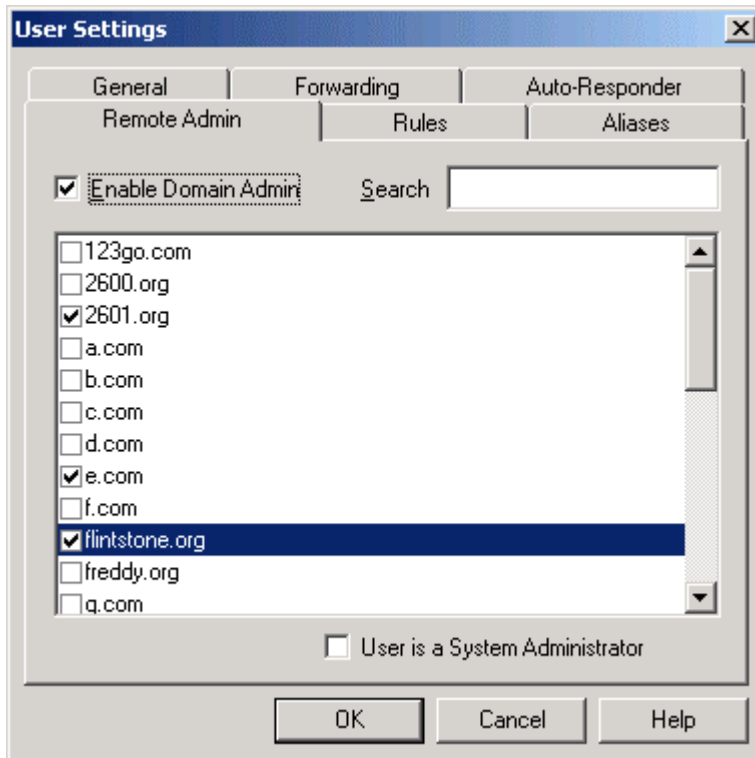
Subject

The subject of the e-mail.

Text of auto-response

Arbitrary text to send as the message.

7.4 User Settings - Remote Admin



Users can be marked to be e-mail administrators for the assorted domains maintained by your server. Such users can add, edit and delete users and adjust the settings for the selected domains using SmartMax's Web-based remote administration tool.

Enable Remote Admin

If checked, then the user is an active remote administrator for the domains selected below.

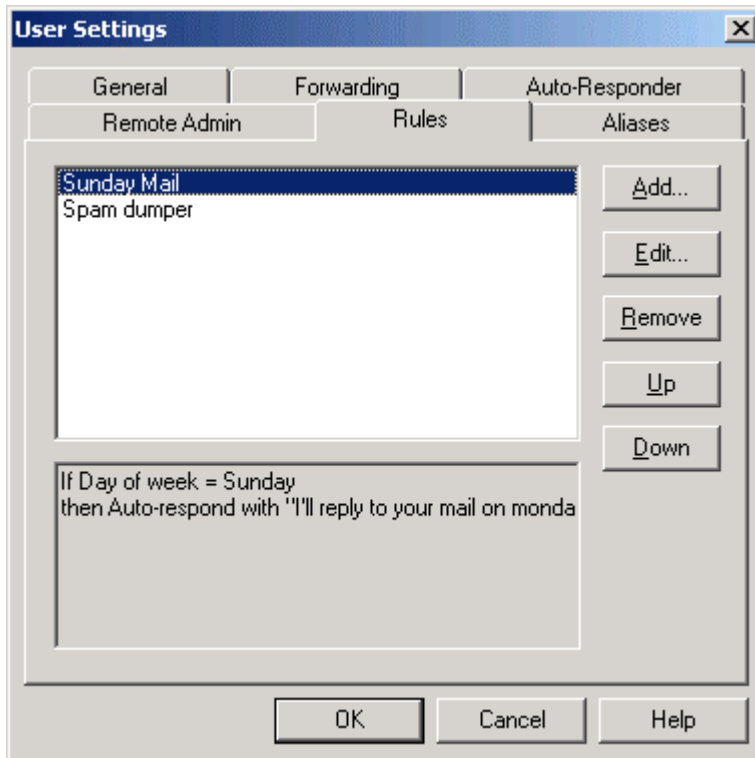
Search

Some mail systems are large enough that the list of domains is too big to scan visually. Enter a part of a domain and the display will be advanced to the next name that matches.

The List:

Click in the check-boxes to select which domains that the user may administrate.

7.5 User Settings - Rules



The user rules are the rules applied to incoming mail. These rules are applied after both system rules and domain rules. The order of the rules is important to processing since one rule action is to terminate processing any other rules.

Add...

Click this to add a rule.

Edit...

Click this to edit the selected rule.

Remove

Click this to remove the selected rule.

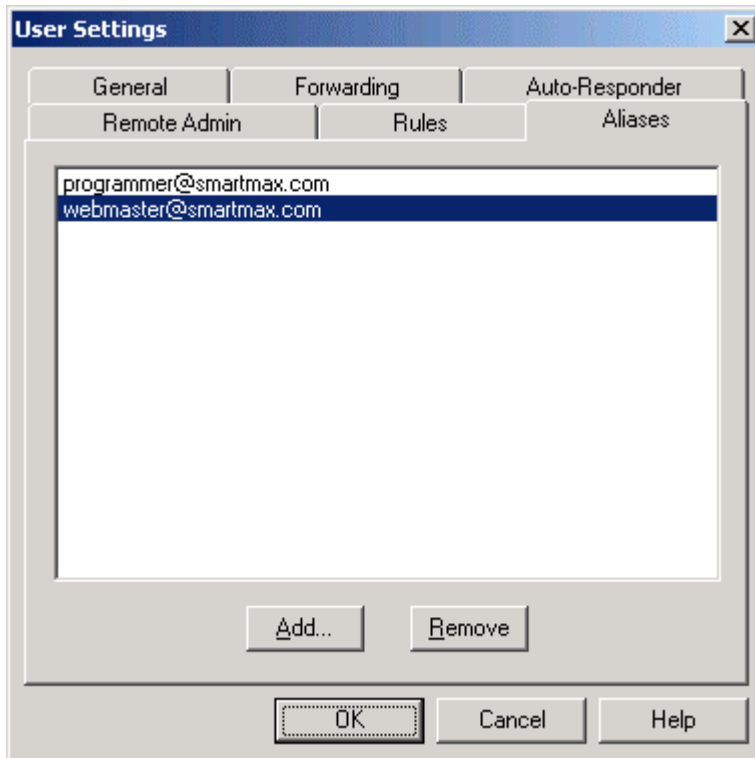
Up

Move the selected rule earlier in the list.

Down

Move the selected rule later in the list.

7.6 User Settings - Alias



Users may have aliases for themselves on the system. For example, the "postmaster" and "webmaster" and "johndoe" might all be one and the same person. This lets you set an alias for this user and mail will arrive for this user even if addressed to the alias.

Add...

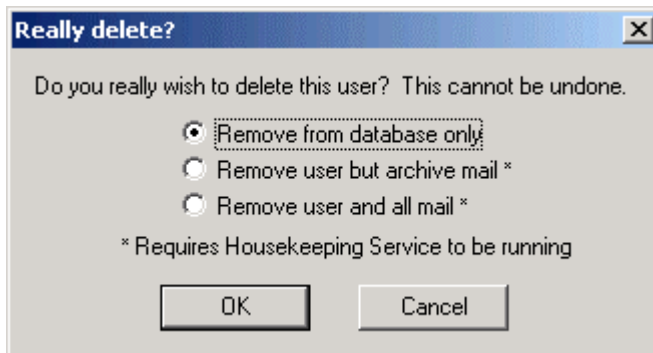
Click to add a new alias. Both the domain and the user must be on the same e-mail system as the user.



Remove

Click to remove the alias from the list.

7.7 Deleting Users



When deleting users, select the method of clean up for the user. For the second and third options, the Housekeeping service must be running in order for the cleanup to take place. Cleanup is not necessarily immediate since housekeeping will get to this at its leisure.

Remove from database only.

All records related to the user are removed from the database.

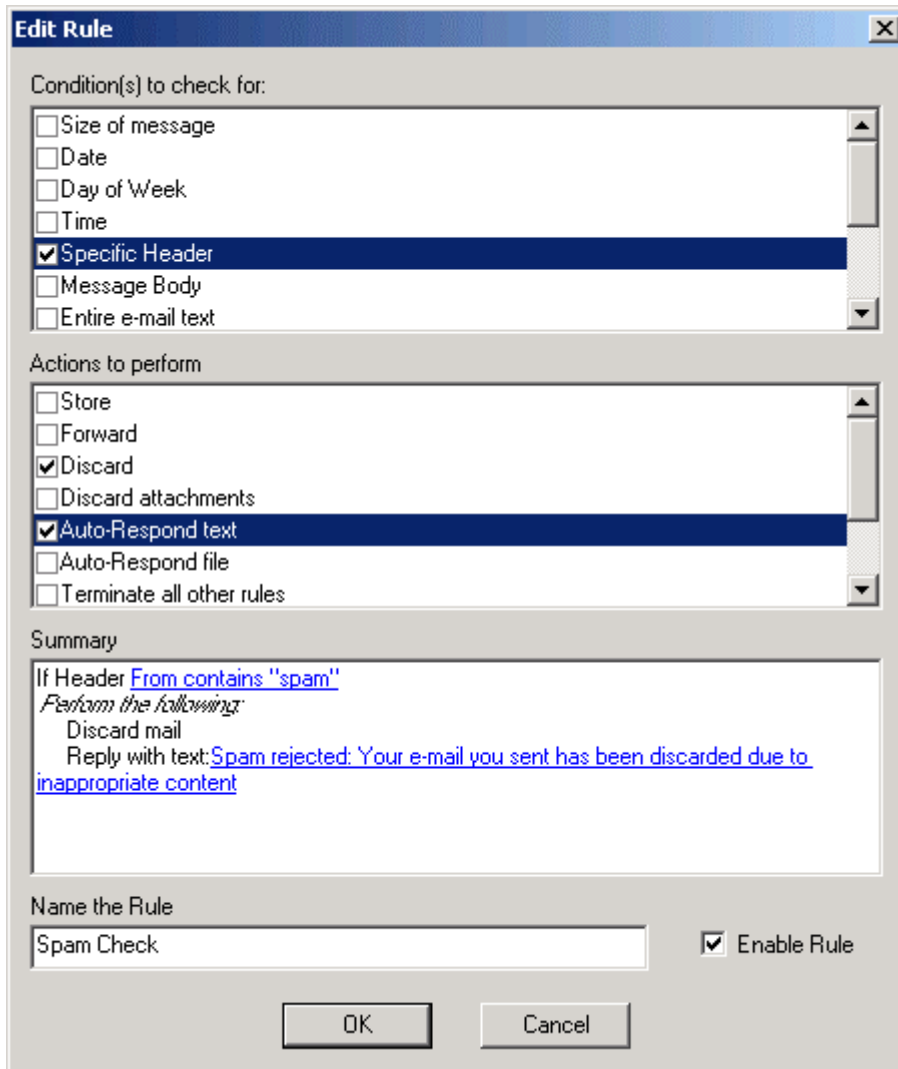
Remove User but archive mail

In addition to removing the user from the database (as above), the mail storage folder for the user will be renamed to the date the user was removed. Consequently, the user's mail will remain untouched on the hard-drive. Deleting the files after that time requires manual deleting.

Remove user and all mail

In addition to removing the user from the database (as above) all mail folders and files will be deleted completely.

8 Rules



Use this dialog to edit the settings for a rule. When a setting is selected, edit the details for the rule by clicking the hyper-link in the Summary.

Condition(s) to test for

Conditions are what indicate that an action should be performed on a piece of inbound e-mail. All of the triggers must be true for the action to apply. The test is based on:

Size of message - the message size including headers

Date - date the message arrived

Day of Week - day of the week the message arrived (for purposes of comparison, Sunday = 1, Monday=2, ... Saturday = 7)

Time - time of day the message arrived

Specific Header - check for a specific header (e.g., "From")

Message Body - looks for text in the message body

Entire e-mail text - look for text in the headers or body

File Attachment Name - Looks for specific file attachment names, including wildcards

Any message - always triggers

External Test - Runs external program for the test

Actions to perform

You can have the rule do any of the following:

Store - store the mail (this is the default for all mail)

Forward - Forward a copy of the E-mail to a list of recipients

Discard - completely discard the message

Discard attachment - discard any attachment

Auto-Respond text - send an automated response to the sender of the message

Auto-Respond file - send an automated response to the sender of the message using the contents of a file

Terminate all other rules - terminate all other rules. Note: a rule consists of its triggers and actions. If a rule triggers, all its actions will be completed. This implies that if you include several actions along with this one, they will all be done first, then the terminate action will prevent any other rule testing or processing.

Note to self - E-mail a short note to the recipient of the mail. Useful for warning of mail discards.

Run Program - run an external program.

Summary

This shows the summary of behavior for the rule. You can click on the underlined settings to alter the details of the condition or behavior. This is required when the setting is first selected.

Name the Rule

Enter a name for the rule. This is merely informational, but is required.

Enable Rule

Does what it indicates. Normally, this is enabled.

8.1 Condition Options

8.1.1 Size of Message



Triggers the rule if the size of the message (in bytes) meets the selected values. Possible settings are:

Equals

Not Equals

Less than

Greater than

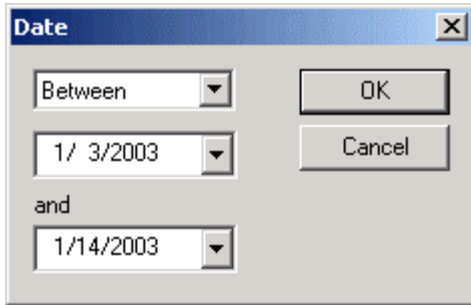
Less or Equal

Greater or Equal

Between

If Between is selected, then the second value field is enabled.

8.1.2 Date

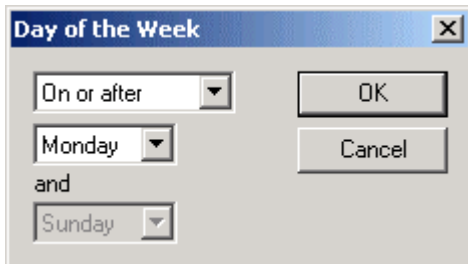


Tests to see that the arrival date matches a value. Options are:

- On
- Not on
- On or before
- Before
- On or after
- After
- Between

If Between is selected, then the second date value is enabled.

8.1.3 Day of Week

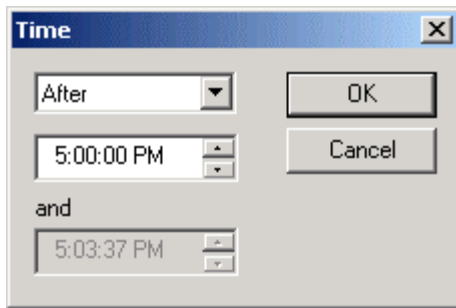


Tests to see that the day of arrival matches a value. Options are:

- On
- Not on
- On or before
- Before
- On or after
- After
- Between

If Between is selected, then the second value field is enabled.

8.1.4 Time

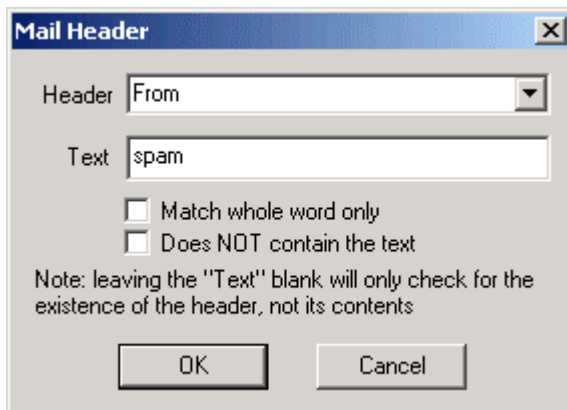


Tests to see that the arrival time matches a value. Options are:

- On
- Not on
- On or before
- Before
- On or after
- After
- Between

If Between is selected, then the second time value is enabled.

8.1.5 Specific Header



Triggers the condition if a mail header matches the selected text.

Header

The name of the header to check. This should not be blank and may not contain the ":" since this is the standard header separator character. The drop down list has some common headers you can select.

Text

The text to check in the header. If this is left blank, the condition is valid if the header simply exists.

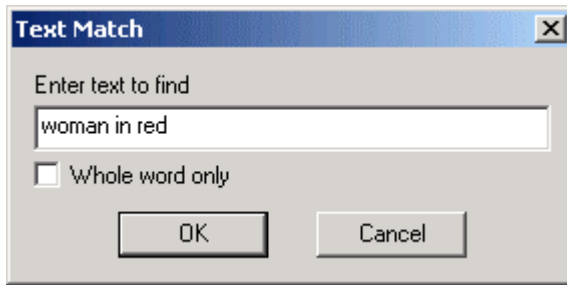
Match whole word only

The word in Text must be a whole word delimited by non-alphabetic characters.

Does NOT contain the text

Reverses the sense of the test.

8.1.6 Message Body / Entire E-mail / File Attachment Name



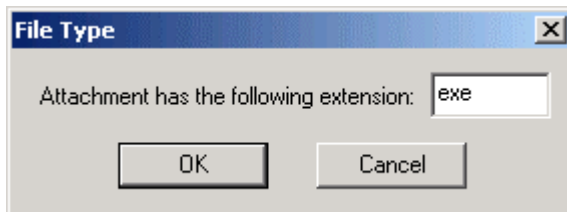
Enter text to find

Enter text to search for the in the message.

Whole word only

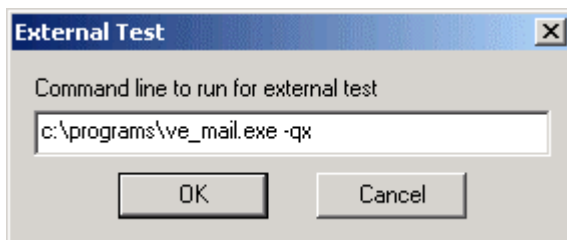
Only finds words delimited by non-alphabetic characters.

8.1.7 File Type



Triggers the condition if there is an attachment whose extension matches the selected text. The period is not needed on the extension.

8.1.8 External test



Runs an external program to use to trigger the condition. It has two functioning modes

8.1.8.1 File Level or %F mode.

This will "un-MIME" the message and hand off the files to the scanner/command-line program. This works exactly as System Level Scanning, however it does not delete the message, it only causes the rule to return a "true" value if the files are removed. You must take some sort of action in the action section of the rule to remove the files. Either "Discard Message" or "Discard Attachments" would be wise options. A "Store in Mailbox" plus a "Discard Message" option could be done which would result in the message NOT being in the INBOX but in the specified "sand box" mail box, however this could result in an IMAP user still "happy clicking" on an infected message, with possible disastrous results. POP3 users would not be able to access the message (because all POP3 can "see" is the "INBOX", so this option would "hide" infected message from them, but allow it to be retrieved if there was important information in message, above and beyond the virus. Example:

```
C:\av\avgscan.exe /clean /scan %F
```

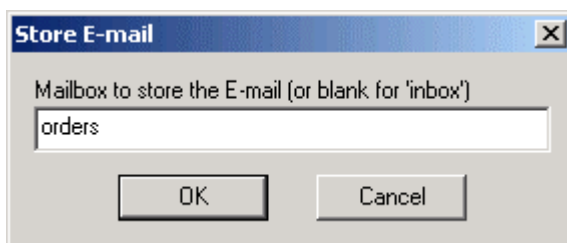
8.1.8.2 Message Level or %M mode.

In this case, a copy of whole message is handed to the scanner, with out "decoding" the attachments. This mode should only be used if the scanner software supports "MIME Decoding". This mode works like the %F mode, in that it will return "true" if the scanner software removes the copy of the message, and you must take some sort of action like in the %F mode. Example:

```
C:\av\avgscan.exe /clean /scan %M
```

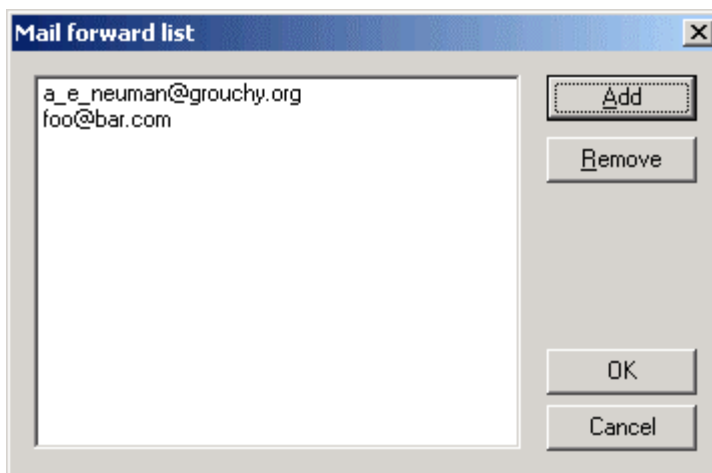
8.2 Action Options

8.2.1 Store



Enter a mailbox name to store the e-mail. Normally this is something other than the usual "inbox" but both "inbox" and a blank entry can be used to store the message in the "inbox." For POP, "inbox" is all that exists. For IMAP, this is wide open. Any existing box will do.

8.2.2 Forward



This is the list of users to receive mail as a result of a rule. Click **Add** to add entries, **Remove** to remove the selected entry.

8.2.3 Auto-Respond Text



Auto-Respond

Name on mail: tim

Reply address: tim@smartmax.com

Subject: Spam rejected

Message:
Your e-mail you sent has been discarded due to inap

OK Cancel

Creates an auto-responder action for a rule.

Name on mail

Actual "real-name" to use in the e-mail reply.

Reply address

Mail address to use for replies

Subject

Subject to be used for the auto-response e-mail.

Message

The body of the message to send (limit 255 characters)

8.2.4 Auto-Respond File



Auto-Respond File

Name on mail: tim

Reply address: tim@smartmax.com

Subject: Thank you for your interest

Path to file
c:\mail\productresponse.txt

OK Cancel

Creates an auto-responder action for a rule.

Name on mail

Actual "real-name" to use in the e-mail reply.

Reply address

Mail address to use for replies

Subject

Subject to be used for the auto-response e-mail.

Path to file

The file containing the body of the message.

8.2.5 Note to Self

Creates an additional, automatic E-mail to the recipient. This is most useful when the original message is discarded.

Name on mail

Actual "real-name" to use in the e-mail message.

Reply address

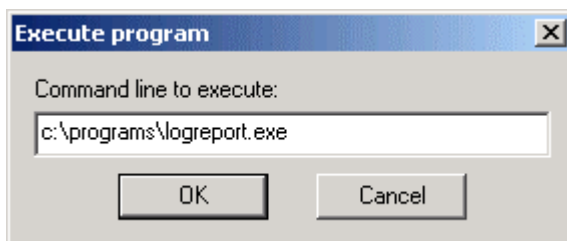
Mail address to use for replies

Subject

Subject to be used for the note.

Message

The body of the message to send (limit 255 characters)

8.2.6 Run Program

The path to a program to execute should be the rule trigger. Like the trigger program, this has the same two modes.

8.2.6.1 File Level or %F mode.

This will "un-MIME" the message and hand off the files to the command line program.

Example:

```
C:\av\avgscan.exe /clean /scan %F
```

8.2.6.2 Message Level or %M mode.

In this case, a copy of whole message is handed to the scanner, without "decoding" the attachments. This mode should only be used if the scanner software supports MIME Decoding.

Example:

```
C:\av\avgscan.exe /clean /scan %M
```

9 Logging and Spying

9.1 Logging

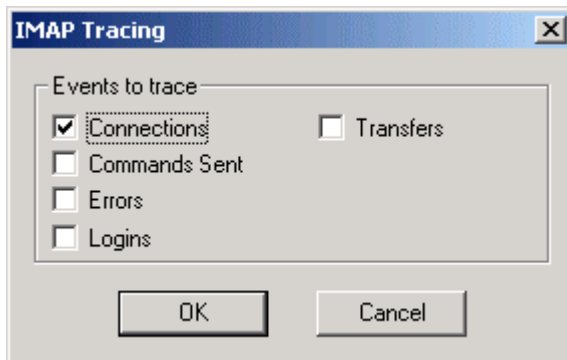
Logging for individual services is covered in the global system settings for those services. (For IMAP, see 4.5.4; for POP, see 4.5.2; for SMTP, see 4.3.1; For QueueMax, see 4.4.1.)

9.2 Spying

Spying is the ability to watch the assorted services and their activities in real-time. While this is often instructive to watch, spying is not as robust as general logging. Spying has a limited number of lines of output that you can view. Older entries are removed. When you close MailMax Admin, the spy information is lost. Finally, spying can place new burdens on DataMax as well as the services talking to it. Use spying sparingly.

Spying can be enabled by selecting the service to watch on the Connection Activity pane (see 2.6) and from the **"Spy"** menu, choosing either **"Track Logins"** or **"Trace Events..."** Tracking logins places no burdens on the servers since login information is already flowing between them and DataMax. Tracing events will ask you what events to trace. Descriptions of those activities follow.

9.2.1 IMAP Tracing



This starts tracing the activities of a running IMAPMax server. A spy window will be added to MailMax Admin that will show running activities.

Connections

Shows clients connecting and disconnecting

Commands Sent

Shows individual commands sent to IMAP

Errors

Shows any errors during a client's session.

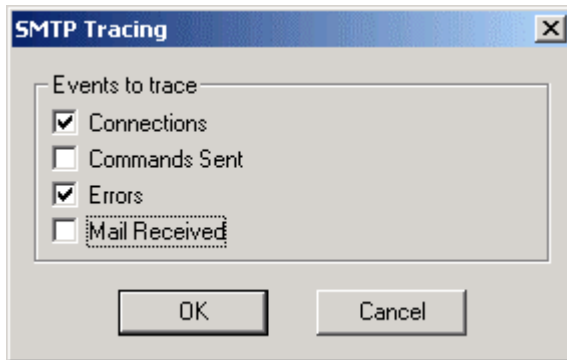
Logins

Shows successful/failed logins. This also shows connections.

Transfers

Shows file transfers both in and out.

9.2.2 SMTP Tracing



This starts tracing the activities of a running SMTPMax server. A spy window will be added to MailMax Admin that will show running activities.

Connections

Shows clients connecting and disconnecting

Commands Sent

Shows individual commands sent to IMAP

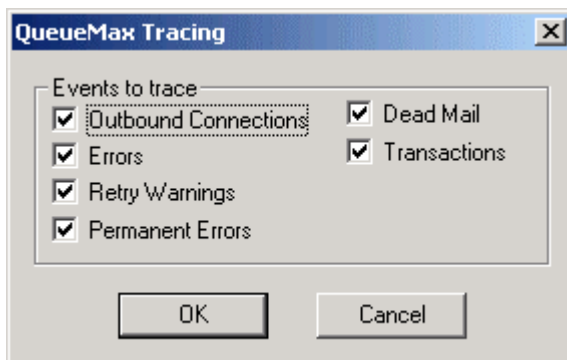
Errors

Shows any errors during a client's session.

Mail Received

Shows information about mail received.

9.2.3 QueueMax Tracing



This starts tracing the activities of a running QueueMax server. A spy window will be added to MailMax Admin that will show running activities.

Outbound Connections

Shows attempts to connect to other servers.

Errors

Shows any errors in transactions and any internal errors.

Retry Warning

Shows attempts to re-try sending mail.

Permanent Errors

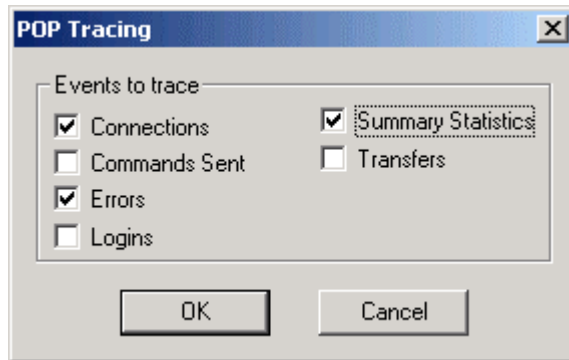
Shows errors that produce un-deliverable mail.

Dead Mail

Shows mail that is placed in the dead-mail folder.

Transactions

Shows complete conversations between QueueMax and remote servers.

9.2.4 POPMax Tracing

This starts tracing the activities of a running POPMax server. A spy window will be added to MailMax Admin that will show running activities.

Connections

Shows clients connecting and disconnecting.

Commands Sent

Shows individual commands sent to POPMax.

Errors

Shows any errors during a client's session.

Logins

Shows successful/failed logins. This also shows connections.

Summary Statistics

Shows the summary statistics normally sent to the client when it disconnects.

Transfers

Shows file transfers both in and out.

10 Frequently Asked Questions

What happened to the Ban/Block IP lists in previous versions of MailMax?

The old Bans/Blocks have been replaced by the more flexible connection settings found in the system settings and in the settings for individual connections.

I've added a domain and users to the system, so why don't the servers respond to clients?

The most likely problem is that you don't have any connections. Select the "Connection Settings" for your system and right-click in the upper list to add a new connection. Set the IP and domain settings for the connection. Click OK and MailMax Admin will also create entries for the basic services and the default ports for those services.

Why does MailMax 5 use this "Connection" scheme?

Previous versions of MailMax could only listen on one port and had other restrictions besides. The connection arrangement allows for more power and flexibility.

Can I have a user alias to a domain that is an alias?

Yes.

What do you mean you can telnet to my system? My firewall has that blocked!

"Telnet" is more than the well known port 23. "Telnet" is the protocol used by most of the major services: POP3, SMTP, WWW, etc. While telnet clients by default connect to port 23, there is no reason they cannot connect to other ports that recognize the protocol. Our customer service people routinely use this method to troubleshoot mail services. It does not represent any kind of security risk. In fact, the only way to keep a telnet client from connecting to your computers is to unplug from the net.

What happens if a mail forwards to another user in the system and that user forwards the mail back? Will we get infinite mail forwarding?

No. When mail arrives, a list of recipients is built. Normally this is just one user. If forwarding mail, then the list grows until all local forwards have been resolved. However, duplicates are not allowed in the list, so if user Adam forwards mail to Eve and Eve forwards back to Adam, then they will both appear in the list of recipients once and circular forwarding won't occur.

What about circular forwarding involving a remote e-mail address?

MailMax can't stop that, but when mail is forwarded, each server that handles the mail indicates that the mail has passed through. Ultimately this list grows longer than most servers will accept. QueueMax will ultimately refuse to let the circular forwarding continue. See the Maximum Hops setting for QueueMax.

Can a group or cluster contain another group or cluster?

No. For clusters, this would be unreasonable. For groups, such a feature has not been implemented.

11 Menu Layout and Descriptions

11.1 Main Menu

File

Basic System Wizard...

Runs the basic system configuration wizard. This is useful for setting up a new system if you declined using the wizard earlier.

Register...

Register MailMax.

Exit

Exits from MailMax Admin

Edit

Delete

Deletes the selected item.

Local Settings...

Configures services running local to this computer.

Connection...

Changes the connection settings for the DataMax you are connected to.

Host Password...

Changes the password used by the selected DataMax.

System Settings...

Edit global system settings for the selected system.

New

Connection...

Adds a new connection to the Connection manager (or to a group or cluster).

Group...

Adds a new group to the Connection Manager. You may then add connections into the group.

Cluster...

Adds a new cluster to the Connection Manager. You may then add connections to the cluster.

Domain...

Adds a new domain to the system

IP...

Adds a new IP and associated connections to the system.

User...

Adds a new User to the selected domain.

Activity

These menu items apply only to the display of connection activity.

Last Hour

Updates the display with the summary connection activities for the last hour.

Last 12 Hours

Updates the display with the summary connection activities for the last 12 hours.

Last 24 Hours

Updates the display with the summary connection activities for the last 24 hours.

Last Week

Updates the display with the summary connection activities for the last week.

Refresh

Refreshes the display by getting the current activity summary depending on the time range set.

Spy

Assorted options for tracing events on the various servers

Track Logins

For those servers which support logins (IMAP4 and POP3), this will show total connections and login activity. Note: tracking logins has little performance impact on any of the servers and should be used in preference to tracing all events for the servers if all that is desired is tracing system usage, not all events.

Trace Events...

Allows you to trace most activity on the server in real time. Tracing general events can consume system resources and potentially slow down servers. If all you want to track is clients connecting, use Trace Logins instead.

Pause/Unpause

Pauses or resumes the display of events to the current tracing window.

Close

Closes the current spy window and stops any tracing.

Save...

Saves the contents of the current spy window to a file.

Clear

Clears the contents of the current spy window.

View

Turns on or off the following MailMax Admin windows:

Toolbar

This is the button bar normally found at the top of the window.

Status Bar

The status bar is found at the very bottom of the window.

Spy

The Spy Window is a multi-pane, dockable window that shows any spy activity on the servers.

Help**Help Topics**

This help file.

About MailMax Admin...

Displays the About Box for MailMax Admin

11.2 Popup Menu for Domain List

Delete

Deletes the selected domain

Add New...

Adds a new domain

Edit...

Edits the selected domain

Add User...

Adds a new user to the domain.

Virus Check**Enable for Users**

For all users in the highlighted domain, turn on internal virus checking.

Disable for Users

For all users in the highlighted domain, turn off internal virus checking.

Filter...

Turn on a filter for the list of domains.

11.3 Popup Menu for the Services List

Trace Logins

For those servers which support logins (IMAP4 and POP3), this will show total connections and login activity. Note: tracing logins has little performance impact on any of the servers and should be used in preference to tracing all events for the servers if all that is desired is tracing system usage, not all events.

Trace Events...

Allows you to trace most activity on the server in real time. Tracing general events can consume system resources and potentially slow down servers. If all you want to track is clients connecting, use Trace Logins instead.

11.4 Popup Menu for the User List

Delete

Deletes the currently selected user

Add New...

Adds a new user

Edit...

Edits the currently selected user

Change Password...

Change the user's password

Unlock Box

In the event that the user has a "ghost" lock on the primary mailbox, this will remove the lock on it

Filter...

Restrict the user list to those that fit the user filter criteria.

12 Messages and Alerts

The priority setting of the backup domain may not be zero.

Set the priority to some non-zero value. Number is arbitrary, but most system administrators use values like "10" and "20", or "100", "200" and "300" for their various servers.

Caution! Giving a user this setting gives the user the same access to your system that MailMax Admin gives you.

This should only be done if want the user to have unlimited privileges on your system.

Do you wish to give this user System Administrator Privileges?"

Select Yes or No, but make sure it is what you really want.

Invalid serial number form. Please check the registration number given you by Smartmax Software, Inc.

Check the text and try again. If you received your serial number by e-mail, you should cut-and-paste the string rather than type it.

Congratulations! You have successfully registered MailMax. Thank you very much.

Confirmation.

You have successfully un-registered MailMax.

Confirmation.

Password successfully changed for the server. Restart all running MailMax services.

The registry has been updated for the MailMax services, but they don't use the new password until re-start, so you need to restart them. If you have services on distributed systems, you will have to run MailMax Admin on the individual computers and sent the new host password for them.

Failed to delete the service.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Name field cannot be left blank

Enter a name.

IP address cannot be empty.

Enter a complete IP.

Password cannot be left blank.

Enter a password.

Password and confirmation do not match.

Make sure you typed the same password twice.

An entry by this name already exists. Cannot complete the operation.

Pick a different name and try again (or delete the other entry).

Are you sure you really want to delete this entry and all connected entries? This operation cannot be undone and may result in a significant loss of data.

This is a reminder of data loss. Confirm the deletion or cancel it.

Unable to connect to the selected server.

DataMax has either been shut down or network connectivity has been lost to it.

Lost connection to server.

DataMax has either been shut down or network connectivity has been lost to it.

Failed to delete selected item.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Internal error setting registration. Contact SmartMax.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down. In the event that this is not the problem, contact SmartMax customer service.

Error. Unable to save changes to domain settings.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Are you sure you want to delete this domain? This will also delete all the users in the domain and cannot be undone.

This is a reminder of data loss. Confirm the deletion or cancel it.

Failed to delete the selected domain. Cause unknown.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down or its password has been changed.

Invalid domain name specified.

Enter a properly formatted domain name.

Directory name cannot be blank.

Enter a complete path for the directory. Drive letters and UNC paths are acceptable.

Failed to add domain to the database.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

This entry already exists.

The forward you tried to add already exists. The item was not added.

Really delete the user? This cannot be undone.

This is a reminder of data loss. Confirm the deletion or cancel it.

Invalid e-mail address.

Enter a properly formatted e-mail address.

The data field for the action cannot be blank.

Fill in the needed data for the action.

The text entered may not contain a vertical bar ("|").

Remove the vertical bar.

The data field for the condition cannot be empty.

Enter a test value for the condition.

Name cannot be blank.

Enter a name.

Unable to get user list. Error code ____.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Unable to retrieve system settings.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down or its password has been changed.

The domain name cannot be blank.

Enter a domain

Invalid Domain Name. Must be a valid address or IP.

Enter a proper domain name (e.g.: *smartmax.com*) or an IP (e.g. *192.168.1.3*)

Are you really sure you want to log this information? It is the full contents of every e-mail message placed into the log. The log will constantly get flooded with the full contents of every e-mail that goes through your server.

Use this with extreme caution. It is useful only for doing debug testing on the server.

Unknown data error communicating with DataMax.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Really delete the connection? This cannot be undone.

Confirm or deny the operation.

Failed to delete the connection from the database.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Failed to save connection data.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Unable to add the connection

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Unable to get services list. Error code ____.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Really delete this service? This cannot be undone.

Confirm or deny the operation.

Failed to save service settings.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Failed to add service.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Unable to save user settings.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Unable to add the user.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Unable to delete the user.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Failed to set the user password.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Invalid password.

The wrong password has been entered. Try again. Also, check the state of your caps-lock key.

Error getting domain list:

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

An alias for this domain already exists.

Use a different name for the domain.

The following aliases duplicate existing real domains: _____

In trying to add the aliases of the domain, duplicate aliases or existing domains conflicted. The aliases were not added.

The following aliases could not be set. Either the domain doesn't exist or the user name already exists: _____

An attempt to add user aliases failed. Either the domain specified for the user doesn't exist on the MailMax system, or there already was an alias by that name.

The header name cannot be blank

Enter a header

Colons are not allowed in headers.

Colons are used to separate headers from their data in e-mail, consequently, colons aren't allowed in headers names (though nearly every other 7-bit character is allowed)

The test you wanted only can be done against a named header.

Don't use the test you selected. Only use it for header testing.

Cannot compare against an empty expression.

Enter a value to compare against.

Comparison for size must be numeric only

Only enter numeric data for the test.

Invalid date format. Date must be in the form of _____

Date entry follows the short date form in your windows regional settings. This is shown in the error message for your convenience.

Invalid time format. Time must be in the form of _____

Time entry follows the time form in your windows regional settings. This is shown in the error message for your convenience.

Forward destination cannot be blank.

Enter a forwarding address.

The forwarded address is not a legitimate e-mail address.

Enter a properly formatted e-mail address. The e-mail address can be both remote or local, but it still must conform to a standard e-mail name form.

Automated reply may not be blank.

Enter a reply string.

Error _____ in getting domain rule list.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down or its password has been changed.

Error adding rule.

Some kind of internal error occurred. Likely cause is that DataMax has been shut down.

Invalid value specified. Must be 0-255.

Enter a value in the proper range.

Ranges must be specified from low to high.

Order the range from low to high. **10-5** is not correct. **5-10** is correct.

Improperly formatted IP range.

IPs must be specified as **XXX.XXX.XXX.XXX** where **XXX** can be a number from 0 to 255, or it can be a range with a dash between (eg. **20-45**) or it can be an asterisk.

The requested default domain is unknown.

An attempt to find the domain to use as the default. Check the name and try again.

Error ____ getting IP settings.

Some kind of error occurred getting the settings. Most likely cause is DataMax has stopped running.

Unable to find the user requested as the Catch-All account

The user entire wasn't found on the MailMax system. There is now no Catch-All account if there was one before.

This appears to be an un-configured system. Do you wish to run the Basic Server Setup Wizard?

Confirm or cancel the request. If you agree, you will be given the Basic Setup Wizard.

Password cannot be blank.

Enter a password.

IP cannot be blank.

Enter a complete IP.

New basic system completed.

Confirmation.

New system password set.

Confirmation.

Unable to add user. Either the user already exists or the selected name exists as an alias for another user.

You will need to use another name for the user or remove the other user or a matching alias.

Are you sure you want to unlock this user's mailbox(es)? This should only be done in the event of a "ghost" connection.

This is a check warning. The greatest hazard is that someone lied to you and you are unlocking an INBOX for a connected user resulting in confusion for the user's client software.

Failed to unlock the user box.

Unable to communicate with DataMax to unlock the user's box. You may need to restart system services.

Can't start tracing. No events were selected to trace.

Select something.

You have already registered this program.

You don't need to register it again

You cannot re-register the demo version of the program.

You either need to remove the program from your computer or contact SmartMax Software about purchasing a copy of MailMax.

Can't find the account requested as the monitor account.

The account you entered as the monitor account does not exist. Either create the account, or pick another name.

Command line may not be blank.

Enter a valid path to a program to run.

Warning! You have too many domains set to have internal virus checking. If you need more forwarding domains virus checked, contact SmartMax Software, Inc. for an upgrade.

You have a limited license for how many forwarding domains may use the internal virus checker. An expanded license is needed to virus-check additional domains.

Warning! You have too many users set to have internal virus checking. If you need more users virus checked, contact SmartMax Software, Inc. for an upgrade.

Contact SmartMax Software to get an increase in users who can use the internal virus check.

File extension cannot be blank.

Enter some kind of file extension to check. You can leave off the dot on the extension.

Field cannot be blank

Fill in the required value in the empty field in the dialog.

Field is too long

Enter fewer characters. There are limits on text for this value.

Forward list may not be empty

Add at least one forward to the list.

You have incomplete action(s) in your rule. Click on them and set them to contain values.

You need to finish setting the details about one or more of the actions in your rule.

You have incomplete condition(s) in your rule. Click on them and set them to contain values.

You need to finish setting the details about one or more of the actions in your rule.

String to search for cannot be blank.

Enter some text to search for. The content is arbitrary, but it must be something.

You have not set any actions for the rule.

Select at least one action.

You have not set any conditions to test.

Select at least one condition.

Headers cannot contain colons. (E-mail uses them as header delimiters)

Take the colon out of the header name.

Registry server does not appear to be the correct one.

This is an internal error. Contact SmartMax Software for registration assistance.

Can't unregister. DataMax is not registered on this computer.

Register first before you try to un-register.

The Queue directory may not be blank.

Enter a valid path.

Caution! Giving a user this setting gives the user the same access to your system that MailMax Admin gives you.

This should only be done if want the user to have unlimited privileges on your system.

Do you wish to give this user System Administrator Privileges?

Use this option with caution. Confirm or deny.

Unable to connect to the registry server.

There could be transient failures on the net, problems with your own network or DNS, or the SmartMax registry server is down. Try registering again after waiting a bit. If the problem persists, contact SmartMax Software.

The serial number you entered is unknown

Check the registration number you were given. If you typed it in correctly, contact SmartMax Software customer service.

This will enable internal virus checking for all users of this domain. If there are more users than your license allows, none of them will be enabled and you will need to set users individually. Continue?

Confirm or deny. Regardless of how this sets the users in the domain, you can still manually disable individual users. This is just a convenience to avoid having to set everyone manually.

This will disable internal virus checking for all users of this domain. Continue?

Confirm or deny. Regardless of how this sets the users in the domain, you can still manually enable individual users. This is just a convenience to avoid having to set everyone manually.

Virus check settings updated for each user in the domain.

Indicates task complete. Click OK.

Unable to enable virus checking for all the users. You may be over-limit on number of users who can have the internal virus scan.

When you get this error, no users have been altered. You are likely near the limit of the number of users that may have an internal virus scan. Either upgrade your license or set the last few users individually.

Disconnected from server due to bad password. Check connection settings and enter the correct password.

Make sure you have the right password.

You cannot re-register the demo version of the program.

Your demo period has expired. Contact SmartMax Software, Inc. to purchase a copy of MailMax.

This will disable internal virus checking for all users of this domain. Continue?

Confirm or cancel

Warning! You have too many domains set to have internal virus checking. If you need more forwarding domains virus checked, contact SmartMax Software, Inc. for an upgrade.

Confirmation

Field is too long. Must be less than ___ characters.

Shorten the amount of text you typed in the selected field.

Forward list may not be empty

You must put some forwarding e-mails in the list.

You have incomplete action(s) in your rule. Click on them and set them to contain values.

Find the incomplete actions and finish setting values for them.

You have incomplete condition(s) in your rule. Click on them and set them to contain values.

Find the incomplete conditions and finish setting values for them.

String to search for cannot be blank.

Enter a search string.

You have not set any actions for the rule.

Select some actions.

You have not set any conditions to test.

Select some conditions.

Contacting SmartMax Software Customer Service



Snail Mail:

SmartMax Software, Inc.
2431 E. 61st Street Suite 307
Tulsa, Oklahoma 74136-1231
USA

WWW:

<http://www.smartmax.com>

E-mail:

info@smartmax.com

Customer Service:

Voice: 918-496-8103

Fax: 918-491-0033

From the menu "Help|About..."



[This page deliberately left blank.]

- Account Type, 52
- Action Options, 64
- Actions, 60
- alias, 48, 57
- Auto-Respond, 60
 - File, 65
 - Text, 65
- avast!, 36
- backup, 45, 50
- bans, 2, 34, 41, 42, 71
- Basic System Wizard, 3
- blank passwords, 20, 47
- blocks, 2, 71
- Catch-All Account, 47
- clear-text passwords, 20
- cluster, 7, 9, 11, 19, 45, 72
- Columns, 12
- comment, 42
- Condition Options, 60
- Conditions, 59
- Connection
 - activity, 15
 - control of, 33, 40
 - information, 8
 - name, 19
 - new, 72
 - settings, 14, 39
 - tree, 7
- Conversion, 1
- Database, 17
- DataMax, 1, 9, 17
- Date, 59, 61
- Day of Week, 59, 61
- Default Box Size, 46
- Default Connection, 39
- deleting
 - domains, 50
 - users, 58
- directories, 5, 76, 82
 - DataMax, 16
 - domain, 3, 45, 50
 - logging, 16
 - QueueMax, 25
 - SMTP, 17
 - virus check, 35
- Discard, 60
- Discard attachment, 60
- Disk Limit, 52
- DNS, 31
- domain, 3, 11, 73
 - alias, 48, 71
 - backup, 50
 - ban, 41
 - bans, 34
 - default, 39
 - directory, 45
 - ETRN, 50
 - filter, 13
 - new, 72
 - remote administration, 55
 - remote administration of, 19
 - settings, 45
 - Smart Hosting, 49
- Enable Forwarding, 53, 54
- Entire E-mail, 63
- ETRN, 45, 50
- events, 24, 68
- external program, 60
- External test, 63
- File Attachment, 59
- File Attachment Name, 63
- File type, 63
- file types, 36
- filter, 13, 14
- Find text, 63
- forward, 53, 54, 60, 64
- graphs, 15
- Group, 11
 - new, 72
- Header, 59, 62
- High Water Mark, 43
- Housekeeping, 19, 47, 52
- IMAP, 28, 30
 - logging, 30
 - tracing, 68
- IMAP4, 16
- IMAPMax, 1
- inbox, 64, 81
- IP, 39, 42
- Local Service Settings, 16
- logging, 68
 - directories, 16

- IMAP, 30
- POP, 29
- QueueMax, 27
- SMTP, 24
- logins, 68
- Low Water Mark, 43
- Mail From, 22
- Max Retry Sessions, 25
- Max User Boxes, 46
- maximum hops, 26, 71
- Message Body, 59, 63
- Name, 51
- Note to Self, 60, 66
- NT 4.0, 6
- open relay, 21
- overlimit, 20, 47
- password, 8, 9, 16, 20, 47, 52
 - clear-text, 20
- POP, 28
 - logging, 29
- POP3, 16
- POPMax, 1
 - tracing, 70
- port, 43
- postmaster, 26
- Priority, 46
- Queue directory, 25
- QueueMax, 1, 25
 - logging, 27
 - tracing, 69
- Register, 10
- Registration, 9
- remote administration, 19, 55
- Reverse DNS, 22, 23
- rules, 2, 59
 - domain, 49
 - global, 32
 - user, 56
- Run Program, 60, 66
- Self, 66
- Serial Number, 10
- Service Settings, 43
- Session Byte Limit, 23
- Session Message Limit, 23
- Size of message, 59, 60
- Smart Hosting, 20, 45, 49
- SMTP, 22
 - Authentication, 22, 52
 - logging, 24
 - Port, 23
 - tracing, 69
- SMTPMax, 1
- Soft Error Retry Settings, 26
- Sophos, 35
- Spam-Trap, 52
- Specific Header, 62
- spying, 68
- SQL, 2, 17
 - authentication, 17
- Step Rate, 43
- Store, 60, 64
- Tarpitting, 23
- Terminate, 60
- Time, 59, 62
- timeout, 19, 23, 26
- tracing
 - IMAP, 68
 - POPMax, 70
 - QueueMax, 69
 - SMTP, 69
- unregister, 10
- user, 11, 74
 - ban, 34, 41, 42
 - filter, 14
 - forwarding, 53
 - new, 72
 - password, 20, 47
 - remote administration, 55
 - rules, 56
 - settings, 51
 - valid name, 51
- virus, 17, 46, 52, 63, 74, 81, 83
 - actions, 37
 - settings, 18, 35
- VRFY, 22