

MERCUR Messaging 2005

User Guide

Introduction	14
MERCUR Features	15
Overview Product Features	15
Secured password authentication for SMTP, POP3 and IMAP4	15
Anti-virus-checking for incoming messages	15
Check open relay database by using DNS suffix	15
Attachment filtering for MIME encoded attachments	15
Exception handling for mail addresses and hostnames (Black List).....	15
Language selection "On the fly"	16
Sending and receiving SMTP messages	16
Check for waiting mail with POP3 or IMAP4.....	16
Management of unlimited domains	16
Management of unlimited users in local and remote mailboxes	16
Mailing list.....	16
Management of auto responders	16
Mail routing.....	17
Remote mail account management	17
Event logging	17
Dial Up network support	17
Remote configuration.....	17
Executables via mail	17
Management of static routes	17
Windows NT/2000 user manager.....	18
Database connectivity (ODBC).....	18
Scheduling	18
Priorities	18
Security	18
POP3 Authentication	18
SMTP Authentication.....	18
Email-to-Fax and SMS/Pager Gateway	19
Statistic lists.....	19
Integrated WebMail-Client.....	19
Online-Help	20
The Help menu MERCUR Messaging 2005	20
Direct help	20
MERCUR Messaging 2005 User types	21
User types	21
Default user	21
Default user with administration permissions for ...all Domains.....	21
Default user with Administration permissions for ...only this Domain.....	21
Authentication with MERCUR	22
1. Login to POP3- and IMAP4- accounts	22
2. Authentication in SMTP	22
Import/Export of Data	24
Import from directory/Export to directory.....	24
Type of data.....	24
Into domain/From domain.....	24
System Requirements	25
Server requirements	25
Operating system	25
Network.....	25
Manual Installation of the MERCUR-Service.....	26
Manual Installation of the MERCUR Services.....	26
The SMTP Service	26
The POP3 service	26

The IMAP4 service	26
The Fax/Pager Gateway.....	26
The control service.....	27
The User Interface	28
The main window	28
The Menu bar	29
The Symbol bar	30
Apply	30
What's this?	30
Change representation of the symbol bar.....	30
The Function bar	31
The Status bar.....	32
Language selection "on the fly" (EN).....	32
Help line	32
Dialog System	33
Install a MERCUR service	33
Uninstall a MERCUR service.....	33
Dialog box Connect	34
Dialog Domains	35
Domain settings	36
Domain	36
Description.....	36
Administrator	36
Mailbox name.....	36
Standard Alias	36
More Aliases.....	36
List server.....	36
Standard alias	36
Unknown users	36
Reject mail.....	36
Send info to administrator.....	36
Forward to	36
Send info to originator	37
Windows NT/2000 user (<i>Enterprise Edition only</i>).....	37
Include Windows NT user manager for this domain	37
Account	37
Domain	37
Dialog Users	38
User settings	39
User	39
Alias	39
Domain	39
Name.....	39
Login name	39
Password	39
Forward to.....	39
Local mailbox	39
Type.....	39
Mailbox size unlimited	39
Limit mailbox size to	39
Remote address	39
Copies	40
Received messages.....	40
Sent messages	40

User options	41
Options	41
Respond automatically with.....	41
Add originator addresses to mailing list.....	41
Delete mail older than	41
Forward mail older than.....	41
Info to administrator, if older then.....	41
User can send mails to local domains only.....	41
Administrator permissions	41
....all Domains	41
....this Domain only.....	41
Remote mail accounts	41
Available mail accounts	41
Selected mail accounts.....	42
Mailing Lists	43
Mailing List Settings.....	44
Mailing-List	44
Alias	44
Domain.....	44
Description.....	44
List owner.....	44
Alias	44
Domain.....	44
Options	44
Send message copy to list owner	44
Deny EXPN command	44
Max. message size.....	44
Send with low priority	44
Max. number of recipients.....	44
Set list owner to 'From:' field	45
Send info to list owner when a member joins the list	45
Send info to list owner when a member leaves the list.....	45
'To:' field contains	45
'Reply-To:' field contains	45
List options and permissions	46
Options	46
Files	46
List members	46
File index	46
Header for all messages.....	46
Footer for all messages.....	46
Info to new members	46
Log list activities to file.....	46
Permissions	46
Send message to the list.....	46
Add new members to the list.....	46
Remove members from the list.....	46
Show members using REVIEW/RECIPIENTS	47
Show file index using INDEX	47
Download file using GET	47
Show the list on LIST command	47
Add Mailing List Members	48
Members	48
Import.....	48
File Index	49

Overview list server commands	50
List server commands	50
JOIN or SUBSCRIBE	50
LEAVE or UNSUBSCRIBE	50
LISTS.....	50
WHICH	50
INDEX.....	50
RECIPIENTS or REVIEW	51
GET	51
HELP.....	51
Dialog Auto Responders	52
Auto Responder settings	53
Description	53
Name.....	53
Domain	53
Global	53
Special Domain.....	53
Respond with.....	53
Text file	53
Text.....	53
Options	53
Log	53
Log responses to file.....	53
Time range	53
Delete Auto Responder after expiration.....	53
Exception	54
Enable duplicate response cache	54
Dialog Executables	55
Executable Settings	56
Address	56
Alias	56
Domain	56
Description.....	56
Command	56
Application	56
Parameter	56
Forward message to local mailbox	56
Keywords.....	57
Execute without keywords.....	57
Use the following keyword definitions	57
Executable HOLIDAY	58
Dialog Remote Mail Accounts	59
Remote Mail Account Settings	60
Remote Account.....	60
Description.....	60
Server.....	60
Domain	60
Global	60
Special Domain.....	60
Login.....	60
Use login name from user account.....	60
Use alias from user account	60
Special login.....	60
Login name	60
Password	60

Schedule	61
Add or Edit.....	61
Execute.....	61
Weekdays.....	61
Frequency.....	61
Once, at startup	61
Once, at	61
Periodical every... ..	61
Message size.....	61
Options	61
Parse mail header for recipients (<i>Shared Mail Account</i>)	61
Delete mail from server.....	61
Receive only unread messages	61
Synchronize with Out Basket	62
Dialog Static Routes.....	63
Static Route Settings	64
Static-Route.....	64
Name.....	64
Activity	64
Forward to mail-address.....	64
Forward to mail-domain	64
Forward to remote mail host	64
Forward to original domain as host	64
Delete !.....	64
Address.....	64
Filter	64
Use default filter	64
Use installable filter	65
Default Filter Settings	66
Operator	66
Operator	66
Expression	66
Header-Field.....	66
From Host	66
Message size	66
Server Options Setting	67
Connection	67
Wait until the remote host opens the connection	67
Wait until the remote host sends an ETRN request	67
Use dial-up connection.....	67
Scheduling.....	67
Weekdays.....	67
Execution	67
Immediately, when the mail arrives	67
If the out basket contains more than ... messages.....	67
Once at	67
Periodical every... ..	67
Fax-Gateway.....	68
Features	68
Sending fax messages using predefined profiles	68
Receiving fax messages to forward by E-Mail	68
Use of templates	68
Support for analog Modems and ISDN boards	68
Event-Logging	68

SMS/Pager-Gateway	68
Sending SMS messages using predefined profiles	68
Use of predefined providers.....	68
Support for analog Modems and ISDN boards	68
Event-Logging	69
Description	70
Name.....	70
Type.....	70
Provider	70
Template	70
Filter	70
Accept if...	70
Take destination number from.....	70
Forward to special number	71
Execution	71
Forward immediately	71
Forward between.....	71
Provider.....	72
Name.....	72
Access number	72
Destination number	72
Protocol	72
Mode	72
Append Pager id to access number	72
Remove prefix from Pager id	72
Numeric page mode.....	72
Max. number of messages per session	72
Maximum Text length	72
Authentication.....	72
No authentication required	73
Use Pager id for authentication.....	73
Use the following authentication	73
Device	73
Use T.70 prefix.....	73
Data bits, Parity and Stop bits	73
Init string.....	73
SMS/Pager settings	74
Activate modem provider	74
Activate ISDN provider.....	74
Cut message text, if text exceeds maximum length.....	74
Reject, if message text exceeds maximum length	74
Info to originator	74
Update interval.....	74
Number of retries for delivery.....	74
Fax-Gateway-settings	74
Send attachments, if possible	74
Reject, if attachments not convertible	74
Info to originato	74
Activate fax delivery (E-Mail to Fax).....	74
Activate fax receipt for following email address	74
Update interval.....	75
Number of retries for delivery.....	75
Modem for SMS/Pager.....	76
Port	76
Dial using.....	76
Init string.....	76

Wait for dial tone before dialing.....	76
Use line access prefix.....	76
Modem for Fax-Gateway.....	76
Port	76
Dial using.....	76
Init string.....	76
Wait for dial tone before dialing.....	76
To access outside line, dial.....	76
Settings.....	77
Speed	77
Station-ID	77
Resolution	77
Header font style.....	77
Text font style.....	77
Fax template.....	77
Edit fax template.....	77
Description	77
Name.....	77
Local Fax Id	77
Header	78
Left, Middle and Right.....	78
Template	78
File name	78
Dialog Security.....	79
Check name of sending host	79
Check open relay database by using DNS suffix.....	79
Reject mail, if originator domain has no MX record	79
Do not relay, if the originator address is not local	79
Do not relay, if the originator domain is not local.....	79
Reject incoming mail, if number of external recipients exceeds.....	79
Info to administrator, if number of external recipients exceeds.....	79
Usage of Additional Options.....	80
Watchdog	80
Time range interval.....	80
Options	80
Encrypt message files	80
Save message encrypted.....	80
Deny Telnet connections.....	80
Deny VRFY.....	80
Firewall Settings	81
SMTP, POP3, IMAP4, configuration	81
Edit Firewall	81
Permission	81
Originator address/domain.....	81
All addresses/domains	81
Only domain	81
Only address	81
Range of validity	81
Subnet-Mask	81
SMTP authentication required.....	81
POP3 authentication required	81
Services.....	82
How can I close my open relay	83
Example	83
Exceptions of Addresses	84

Exceptions Dialog	84
Delete Attachments	85
Attachments	85
Delete Attachments from the Messages	85
List contains allowed masks only	85
Delete Only If Larger Than	85
Store Removed Attachments in a Folder	85
Extension Mask.....	85
Exclude address mask for auto responders.....	85
Address mask.....	85
Dialog Virus Control	86
Enable Virus-Scan for MIME encoding messages	87
Scanner-Type.....	87
Application	87
Execute hidden.....	87
Arguments	87
Return codes.....	87
Activity on Virus Alert	88
Activity on Virus Alert	88
• Delete Email.....	88
• Delete infected attachments.....	88
• Store infected attachments in the following folder.....	88
• Info to Administrator.....	88
• Info to Originator.....	88
• Info to Recipient.....	88
• Info to local recipients only	88
• Remark in original message.....	88
Norman Internet Update.....	88
Manually only	88
Automatically every	88
Update now !	88
Examples of Command Line Scanners	89
Norman Virus Control.....	89
McAfee Virus Scan	89
F-Secure Anti-Virus	89
SOPHOS.....	89
Server-Settings	90
Webmail port	90
Clear trash after XX days.....	90
Logout user after XX minutes idle time.....	90
SMTP-Server	90
Use local MERCUR SMTP Service	90
Use the following SMTP Server	90
Hostname	90
Port	90
Database	90
Provider	90
Database	90
Options.....	90
Login name and Password.....	90
Dialog Settings.....	91
Server	91
Hostname	91
Domain	91
Name server.....	91

Administrator Alias.....	91
Administrator mailbox	91
Protocol.....	91
Use 'ESMTP'	91
Max. message size.....	91
Send messages with ESMTP	91
Send message size	91
Supported Authentication methods	91
Adapter	91
Exchange Settings.....	92
Forwarding	92
Use DNS-Lookup.....	92
Use IP cache size.....	92
Clear cache	92
If no MX record available	92
Use domain as hostname	92
Search sub domains.....	92
Forward to Exchange-Host	92
Server requires a SMTP authentication	92
Server requires a POP3 authentication	92
Login name	93
Password	93
Update out basket.....	93
Add a schedule entry	93
Edit a schedule entry	93
Delete a schedule entry	93
Update Outbasket Settings	94
Weekdays.....	94
Frequency.....	94
Immediately, when the mail arrives	94
If the out basket contains more than ... messages.....	94
Once at.....	94
Periodical every...	94
Priority.....	94
Connect only if outgoing mail is waiting	94
Send ETRN request for node name.....	94
To exchange host.....	94
To host.....	94
Delivery Settings Dialog.....	95
Undeliverable Mail	95
Send info to originator	95
Return message to originator	95
Send info to administrator.....	95
Attach original message	95
Info to originator, during delivery problems after.....	95
Mail is undeliverable after.....	95
Keyword for Priority.....	95
Keyword	96
Connection Settings Dialog.....	97
Connection	97
Ports	97
Maximum number of threads for external SMTP connections	97
User data.....	98
MERCUR default format	98
In ODBC database	98

Event-Logs	98
MERCUR default format	98
In ODBC database	98
Enable ODBC error logging	98
Statistic-Information	98
In ODBC-database	99
Default Dialog	100
Unknown users	100
Search alias in other local domains	100
Reject mail	100
Send info to administrator	100
Forward to	100
Send info to originator	100
Advanced options	100
Generate 'Reply-To:' entry if not exist	100
Confirmation of receipt, at demand	100
Info to administrator, if free disk space less than	100
Expiration time for POP3 authentication	100
Settings Dialog	101
E-Mail Backup	101
Max. timeouts...	101
...for client connections	101
...in command mode	101
...opening connections	101
...for name server requests	101
Folders	101
Temporary files	101
Mail folder	101
HTML-Files	102
Event-Logs	102
Time range	104
Date:	104
Total time range	104
Display	104
Domain	104
User	104
Originator	104
Recipient	104
All mail	104
Only sent mail	104
Only received mail	104
Number of messages	104
Total KBytes	104
Statistic display	105
Date	105
Time	105
Event R/S	105
Originator Address	105
Recipient Address	105
Domain	105
User account	105
Volume (Bytes)	105
Duration (Sec.)	105
Number of messages	105
Total KBytes	105

Dialog License	106
License-information	106
MERCUR Remote Configuration	107
Login	107
... all domains	107
... only this domain	107
Dialogs	107
MERCUR Tool MCRSEND	108
Usage of dialog window	108
Settings	108
Delivery	108
Forward to SMTP Server	108
Hostname	108
Port	108
Server requires SMTP login	108
Login name	108
Password	108
Forward directly using DNS	108
Name server	108
Options	108
Keep application open	108
Write event log	109
Recipient information	109
From	109
To	109
Cc	109
Subject	109
Message Text	109
Attachments	109
Help	109
Usage as command line application	109
Options:	109
MERCUR Tool MCRPASS	110
Dialog	110
Options	110
Server	110
Port	110
Change POP3 keyword	110
Username	110
Old password	110
New password	110
Confirm Password	110
Change/Cancel	110
From command line	110
MERCUR Tool HOLIDAY	112
Activate Holiday via E-Mail	112
Deactivate Holiday via E-Mail	112
Holiday at command line	112
Usage	112
Event Log Dialog	113
Options	113
Logging level	113
Delete logs older ... days	113
Support Dialog	114

Required parameter	114
E Mail Address	114
Problem description.....	114

Introduction

The possibility to send messages in your own intranet or the World Wide Web is not just important for large scale enterprises. It is also getting more and more important for the small business. Single email accounts by Internet provider or free mail provider normally cannot perform the efficiency and flexibility to simplify work. For this reasons an own mail server is necessary.

The MERCUR Messaging 2005 may be used as gateway to send on SMTP mails, for automatic control remote mailboxes or as real mail server. MERCUR Messaging 2005 100% corresponds to all standards for **SMTP** (Simple Mail Transfer Protocol after RFC821), **POP3** (Post Office Protocol Version 3 after RFC1939), **IMAP4** (Internet Message Access Protocol Version 4rev1 after RFC2060) and as well **DNS** (Domain Name System after RFC882, -883) and is compatible with most existing mail programs.

MERCUR Features

MERCUR Messaging 2005 Version is recognized as one of the most powerful Internet mail server in the world. Many satisfied MERCUR users around the world describe the software as a high quality product. The development of MERCUR Messaging 2005 is due in part to the constant feedback between atrium software international and our users. This version of MERCUR Messaging 2005 contains five different system services that are easily configured with the help of a Windows Control Panel.

MERCUR can be used as a simple Gateway to route SMTP-Messages, for an automatic POP3/IMAP4 lookup on a remote mail server(s) or MERCUR can be used as a real mail server.

MERCUR is designed in accordance with the current SMTP (Simple Mail Transfer Protocol in RFC821), POP3 (Post Office Protocol Version 3 in RFC1939), IMAP4 (Internet Message Access Protocol Version 4rev1 in RFC2060) and DNS (Domain Name System in RFC882, -883) industry standards.

Overview Product Features

Secured password authentication for SMTP, POP3 and IMAP4

MERCUR supports user password authentication for POP3 (RFC1734) and IMAP4 (RFC1731), as well as POP3-Login using APOP. Furthermore you may use subnet- or domain authentication for SMTP to RFC2554. Also POP3 before SMTP is possible. MERCUR supports simple authentication via PLAIN and LOGIN, or CRAM-MD5 Mechanism (Challenge-Response Authentication Mechanism - Message Digest Version 5) to RFC2195.

Anti-virus-checking for incoming messages

Version offers an build-in interface of Norman Virus Control and an interface to control third party anti-virus scanners. Within the scope of this interface you are able to enter command line virus scanners. Whenever a new message is received, the virus application will call via command line to locate virus infected attachments. The Norman Virus Control can only be used if an registered version is installed or an mercur virus control license is entered. If a virus is found you may define how to proceed with infected messages.

Following options are available: Delete mail, delete the infected message part or save to quarantine directory.

Check open relay database by using DNS suffix

The Open Relay Database can be used by anyone in the configuration of their own network or mail relay, toward the goal of limiting theft of resources by spammers. By accessing these open relay databases, system administrators are allowed to choose to accept or deny email exchange with servers at these addresses.

Attachment filtering for MIME encoded attachments

The MIME Filtering feature is used to remove special attachments, e.g. *.exe, *.vbs etc., from incoming email messages, defined in a list of file masks. This feature offers a usable extension to the anti-virus interface to filter not virus infected but also dangerous executable files like Trojans.

Exception handling for mail addresses and hostnames (Black List)

The new Black List feature allows you to create a list of special email addresses, server names or IP-addresses to deny messages coming from not allowed origins. Together with the regular firewall option is this feature a suitable way to filter unwanted bulk mails.

Language selection "On the fly"

While the program is running you may decide to change the language in which you like to work. If you do so rebooting the program is not necessary. Changing the language also affects as well the online help. The online help will be shown in the newly selected language.

Sending and receiving SMTP messages

Send your messages using a standard email client program to MERCUR. Whether MERCUR is used within a private Intranet or for communications on the Internet, all real destinations (mail addresses) are automatically determined and all mail messages automatically distributed. All incoming mail is placed in their corresponding mailbox by MERCUR. Mail messages can be forwarded or copied to other destinations as well.

Check for waiting mail with POP3 or IMAP4

You can query your mailbox for new mail, whenever you want. New messages are saved in your personal mailbox for as long as they are not collected. IMAP4 (Internet Message Access Protocol) enables a totally sever based post box administration. Thereby it is possible to work messages from more than one computer. The widespread Post Office Protocol (POP) was not developed for this task. It is mainly designed for Client-Computers because POP sends all mail to the client and removes afterwards the mail from the server.

Management of unlimited domains

You may manage user accounts and mailing lists for multiple domains. The destination address of incoming mail will be verified for membership listing and distributed accordingly by MERCUR. Messages addressed to mailboxes on non-local or remote domain, will be delivered to the appropriate remote mail server.

This feature is limited of 3 domains in the Standard Edition of MERCUR Messaging 2005. This feature is limited of 1 domain in the Lite Edition of MERCUR Messaging 2005.

Management of unlimited users in local and remote mailboxes

MERCUR administrates a separate post box for every user in which all incoming messages will be stored until they get collected. For this it is not important if it is a local or remote post box. As well you may grant several users one post box or several post boxes to one user.

This feature is limited of 15 users in the Lite Edition of MERCUR messaging 2005.

Mailing list

Create a mailing list, and send messages automatically to multiple recipients. The number of mailing list members in MERCUR is unlimited. Send an email to designated mail address on the mailing list, and MERCUR will distribute the mail to all the mailing list members. If they got permission remote users can use commands like join/subscribe or leave/unsubscribe to join or leave a mailing list. This feature got many options to make your own adjustments e.g.: mail header declarations **Reply-To;** **To:** and **From:** may be freely defined. Authorizations for owners, members and other users may be adjusted separately. The index administration also enables you to add text and binary files as attachments into the mailing list.

Management of auto responders

Incoming mail can be automatically answered by MERCUR, using predefined profiles (Auto-Responders).

Mail routing

Outgoing mail will be updated periodically. MERCUR automatically determines the host destination for all outgoing messages and delivers them directly to that host destination. While using a name-server MERCUR automatically determines the appropriate server and sends the mail within the scope of the defined parameters. While using an exchange server all mail will be sent to this server.

Remote mail account management

If your Internet Service Provider does not forward mail automatically to your mail server MERCUR can periodically request the remote POP3/IMAP4 server for new mail. MERCUR then delivers all mail messages into their appropriate local mailboxes. External mail accounts can be assigned to individual users or as shared group accounts. With shared accounts MERCUR will receive all waiting messages from the remote account and distribute them to their corresponding user mailboxes on the local MERCUR Messaging 2005.

Event logging

MERCUR contains an extensive set of protocol functions that controls all events on the mail server. The event-log provides information on possible errors and data transfer confirmations.

Dial Up network support

If you do not have a dedicated connection to your Internet Service Provider, but use a dial-up connection, MERCUR can be configured to open your dial-up connection automatically at pre-scheduled time intervals and to close after your activity is done.

Remote configuration

The MERCUR Configuration Utility can be accessed from a remote workstation, using the MERCUR Configuration Service. All configuration and user accounts settings accessible from the local server are also accessible from a remote workstation. The HTTP compatible expansion of the MERCUR configuration service is a useful feature for remote configuration. You may use this service with a browser like the Microsoft Internet Explorer or the Netscape Communicator. The HTML version of this utility is fully compatible with the delivered configuration utility.

Executables via mail

You can execute applications on your system by sending a mail to special addresses, for example you can use the automatic address (Executables) to manage user accounts and passwords via mail.

Management of static routes

Static routes are used to forward incoming mails for filtered mail addresses directly to other mail-server or domains. This is a powerful and time saving feature for administrators managing large networks where mail user accounts are managed on multiple mail server. The processing of static routes is one of the most efficient features of MERCUR. Static routes are highly important for controlled transmitting of messages. It is also possible to use multiple filters for all header fields and to integrate them into the elaboration. Without queues it is possible to send mails in pre-scheduled time intervals to other servers.

This feature is limited to 3 static routes in the Standard Edition of MERCUR Messaging 2005. This feature is not available in the Lite Edition of MERCUR Messaging 2005.

Windows NT/2000 user manager

User accounts defined in Windows NT as well as Windows 2000 user manager can be accessed and configured using the MERCUR user management. This will save administrations time and duplication of user accounts.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

Database connectivity (ODBC)

MERCUR allows you to store user accounts and event log information in ODBC data source format. This simplifies importing existing user data into MERCUR's mail management database. ODBC connectivity provides fast access to large amounts of data. ODBC based event logging provides an easy interface for accessing detailed statistics on user accounts and mail server activity.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

Scheduling

MERCUR contains a time scheduling system for updating incoming and outgoing mails. Outgoing mails can be delivered pre-scheduled time intervals. Schedules can be configured on a daily or/and weekly basis, e.g. every 30 Minutes but only between 8:00 and 18:00, otherwise every 2 hours and once at 12:00 o'clock at the weekend. This powerful feature available for local and remote mail account and for time controlled forwarding when using static routes

Priorities

The message handling is shared using a low, normal and high priority setting. User defined header fields can be used to detect the message priority. Different messages with different priorities are managed by separate tasks. The priority feature is useful for managing large quantities of mail from mailing lists, preventing any delivery delays of regular mail.

Security

A built-in IP based firewall system protects your local mail system from unwelcome intruders. You can grant and deny the access to special IP-addresses and subnets. Incoming mail can be parsed for unwanted originator addresses and then rejected. The new mail storage system in MERCUR allows message encryption for incoming and outgoing messages.

POP3 Authentication

When your provider requires an (**POP3 before SMTP**) authentication so you can use this option by MERCUR. You must insert the user name and the password and activate this option in the exchange page from MERCUR by using the Extended button. If you do so messages send to an exchange server will use first the POP3 authentication. This option is only available by using an exchange server.

SMTP Authentication

When your provider requires an (**SMTP before POP3**) authentication so you can use this option by MERCUR. You must insert the user name and the password and activate this option in the exchange page from MERCUR by using the Extended button. If you do so messages send to an exchange server will use first the SMTP authentication. This option is only available by using an exchange server.

Email-to-Fax and SMS/Pager Gateway

The Gateway is an interface between Email and regular fax devices. In this way, it is possible to receive in-coming messages and to then transmit to fax numbers according specific routes. In addition, faxes can also be received and forwarded via Email. Further more with predefined profiles, you can define which kind of messages shall be accepted by the gateway and forwarded to a mobile phone or pager. The gateway uses special filters to select incoming messages and forward it to predefined or automatically determined pager ids.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

Statistic lists

MERCUR allows administrators to view and generate statistic reports on all activity in and out of the mailserver. The statistics report can be viewed on screen and will contain specific details as per the selection made. The statistics report will also identify the on a per message basis the size of the message. Once the report has been generated a display of the total number of messages and total number of Kbytes will be visible at the bottom of the statistics window.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

Integrated WebMail-Client

Access your email anytime, whether you are sitting at a cafe, in a public library, at work or in the privacy of your home. With the integrated Webmail-Client you have access to your email, personal contacts, personal calendar, all via your browser.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

The MERCUR WebMail-Client allows email message access via any standard browser. With MERCUR WebMail-Client all your contacts, appointments, tasks, and user settings are stored in a database format using either Microsoft Access or Microsoft SQL Server. The integrated MERCUR WebMail-Client uses Microsoft Data Access Objects (MDAC), other major database applications are also supported. Full database support ensures that all your daily data can be secured and easily backed up.

The MERCUR WebMail-Client pages are available in English and German. Language selection is available at the user level.

For further information send your mail at:
info@atrium-software.com

atrium software international

Idsteinerstraße 51
65527 Niedernhausen

Online-Help

In the online help of the MERCUR Messaging 2005 you will find information's to all features. There are two methods to use online help:

The Help menu MERCUR Messaging 2005

With **MERCUR Help...** you call the MERCUR Online Help. The menu item **Help** you will enter the online help. Here you will find links to all options and how to work with them. You may return to the **Help** item if you press the **Contents** button. If you press **F1** you will get more information to use the menu items **Contents**, **Index** and **Search**.

Direct help

In the right upper corner many dialogs and the MERCUR Messaging 2005 main window contain a **Direct Help** button. Here you get further information.

MERCUR Messaging 2005 User types

MERCUR Messaging 2005 defines three types of users, which the MERCUR administrator may allocate. Mainly these are default user and user with different administrator permissions.

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

User types

Default user

These are user whose mailbox get administrated in a local domain and also have no administration permissions.

Default user with administration permissions forall Domains

If this option is activated this user may configure the complete MERCUR Messaging 2005 from a remote computer. He has to login with the complete email address and the password.

Default user with Administration permissions foronly this Domain

If this option is activated this user may configure only this domain from a remote computer. He has to login with the complete email address and the password.

Authentification with MERCUR

1. Login to POP3- and IMAP4- accounts

The two standard protocols for administrating email accounts POP3 (Post Office Protocol Version 3 after the RFC1939) and IMAP4 (Internet Message Access Protocol Version 4 after the RFC2060) generally require a user login. The login may happen plain or encoded.

If no other setting of the used mail client is done the authentication will happen plain. This procedure will be supported by all systems and is the standard login procedure. As a matter of the fact this procedure is very insecure because with simple network monitor-programs other persons may find out the login names and passwords and misuse them easily.

Far better method of the user login is using a secured password authentication. Then the user password will be sent encrypted. The server normally is enabled to use several encryption procedures. Your client will choose the preferred procedure and send the command AUTH (using POP4) or AUTHENTICATE (using IMAP4).

The MERCUR Messaging 2005 is enabled to use the authentication procedures PLAIN, LOGIN, CRAM-MD5 and NTLM. PLAIN and LOGIN will send the message encoded but not encrypted. Encoded messages may be hacked by third persons. More secure is the CRAM-M5 mechanism (Challenge-Response Authentication Mechanism - Message Digest Version 5), which will encrypt the user password with a server generated time stamp. These time stamps will be newly generated each login so every encrypted password is used only one time. More complicated is the NTLM mechanism, which is the standard authentication, used by Microsoft products like Outlook or Outlook Express. Here as well the encrypted data is different in every connection.

The POP3 protocol also provides you with the APOP-command (Authenticated POP). Besides the AUTH command the APOP command is another form of authentication, which works similar to the CRAM-MD5 procedure.

The used client always directs the type of the login procedure so you do not have to make any settings in the MERCUR. The preferred procedure has to be chosen your used mail client. The explained procedures are always available. The only exceptions are domains, which use the Windows NT user manager. In this case no secured login is possible.

2. Authentication in SMTP

The SMTP-protocol (Simple Mail Transfer Protocol after the RFC821) serves for delivering messages and normally uses no kind of authentication. It is also impossible to do so because else no worldwide message transfer would be possible. Anyway in special cases an authentication is required. This kind of authentication is normally not for general use of the service but for permissions to forward mail to other systems. For these special cases the ESMTP (Extended SMTP) enables the AUTH command after the RFC2554. ESMTP is not a different protocol but provides several extensions of the normal SMTP protocol.

The SMTP AUTH command works similar to AUTH by POP3 and AUTHENTICATE by IMAP4. As well the authentication mechanisms PLAIN, LOGIN, CRAM-MD5 and NTLM will be provided.

To use the SMTP authentication in MERCUR the ESMTP option must have been enabled. Here by the ESMTP mode is activated and the server reacts on AUTH requests.

So the SMTP login is possible but not always required. If a client authenticates himself successfully the relaying option **Do not forward if originator address is not local** in the anti spamming section is deactivated. Then the client is enabled to forward as well mail to foreign domains.

As well it is possible to demand an authentication for certain domains or addresses if you enter them with their belonging subnet into a firewall list. In this way you are able to restrict several addresses and domains to a defined ip address range or to demand a belonging authentication.

Another possibility of the SMTP login is a login in POP3 (POP3-before-SMTP). Therefore the mail client has to make an authentication at the POP3 service before delivering messages. The POP3 service will store this au-

thentification for a certain time in a list, which will be used from the SMTP service for authentication. This procedure is more an improvised solution because the SMTP authentication in the scope of AUTH will not be supported form all systems. The POP3 login and the message transfer have to be one after another because the login data will be stored only for a short while.

Import/Export of Data

The Import/Export command in the menu **File** is used to import user data from other MERCUR databases or export data to other databases. The import or export of data works only with MERCUR version 3.0 databases or higher.

Import from directory/Export to directory

Enter the name of the directory that contains the data to import or should contain the exported data. Import is only possible when the selected directory contains valid MERCUR user data.

Type of data

Specify here the types of data you want to import or export. You may choose multiple types.

Into domain/From domain

Enter the name of the domain that should contain the imported data or contains the data to export. You can also import data to a new domain. The domain will be created automatically.

System Requirements

Before you try to install the MERCUR Messaging 2005 you should control that your computer meets the software requirements.

Server requirements

To use MERCUR Messaging 2005 under Microsoft Windows NT or Windows 2000 the following software requirements are needed:

The operating systems **Microsoft Windows 9x** and **Microsoft Windows ME** are not supported.

Attention: Make sure that no anti-virus application is scanning the MERCUR directories, because this can create trouble.

Operating system

- Microsoft Windows NT Workstation or Server Version 4.0, with Service pack 4, for INTEL based systems or higher
- Microsoft Database Access Components (MDAC 2.5 RTM or higher)

OR

- Microsoft Windows Professional/XP-Professional or Microsoft Windows 2000/2003 Server
- Microsoft Database Access Components (MDAC 2.5 RTM or higher)

Network

An installed and correctly configured TCP/IP protocol.

Manual Installation of the MERCUR-Service

Manual Installation of the MERCUR Services

MERCUR consists five different system services, SMTP, POP3, IMAP4, and the Fax-/Pager-Gateway also the CONTROL SERVICE used for remote configuration. These services can be installed and removed manually as follows:

The SMTP Service

Command	Function
mcrsmtp -install	Installs the SMTP Service
mcrsmtp -autoinst	Installs the SMTP Service. The Service will be started during System-Startup
mcrsmtp -remove	Removes the SMTP Service from the system
mcrsmtp -start	Starts the SMTP Service
mcrsmtp -stop	Stops the SMTP Service

The POP3 service

Command	Function
mcrpop3 -install	Installs the POP3 Service
mcrpop3 -autoinst	Installs the POP3 Service. The Service will be started during System-Startup
mcrpop3 -remove	Removes the POP3 service from the system
mcrpop3 -start	Starts the POP3 Service
mcrpop3 -stop	Stops the POP3 Service

The IMAP4 service

Command	Function
mcrimap4 -install	Installs the IMAP4 Service
mcrimap4 -autoinst	Installs the IMAP4 Service. The Service will be started during System-Startup.
mcrimap4 -remove	Removes the IMAP4 service from the system
mcrimap4 -start	Starts the IMAP4 Service
mcrimap4 -stop	Stops the IMAP4 Service

The Fax/Pager Gateway

Command	Function
mcfpgate -install	Installs the Fax-/Pager Service.
mcfpgate -autoinst	Installs the Fax-/Pager Service. The Service will be started during the system startup.
mcfpgate -remove	Removes the Fax-/Pager Service.
mcfpgate -start	Starts the Fax-/Pager Service.
mcfpgate -stop	Stops the Fax-/Pager Service.

The control service

Command	Function
mcrctrl -install	Installs the Control Service
mcrctrl -autoinst	Installs the Control Service. The Service will be started during System-Startup.
mcrctrl -remove	Removes the Control Service from the system
mcrctrl -start	Starts the Control Service
mcrctrl -stop	Stops the Control Service

The User Interface

After you have started the MERCUR Messaging 2005 the main window will be displayed. You may use keyboard and mouse to work with the main window.

The main window

In the upper section of the main window you will see the header line with the program icon, name and the windows system buttons. Right under the header line you will see the *Menu bar* with all dialog commands. Then follows the *Symbol task*. The available buttons are as well dependent on the chosen dialog. On the left side you will see the *Function bar* it contains all dialogs. At the bottom part the *Status bar* will be shown. Here you have got the language selection **On the fly** and the help line.

The Menu bar

The menus of the menu bar will arrange after the chosen dialog. You will find any dialog commands here.

Menu	Content
File	Here you may load or save your settings, end the program and have the option of remote configuration.
Dialogs	Contains the main options of the function bar.
System	Here you may start and stop all MERCUR services as well as install or uninstall them.
View	Here you may change the symbol bar and the status bar.
Extras	Enables to change quickly between the dialogs <i>Security</i> , <i>Settings</i> and <i>Support</i> .
Help	Here you get information, help and support for this application.

The Symbol bar

You can change the representation of the symbol bar in the MERCUR Messaging 2005. To do so you may use the menu item *View* or point with the mouse on the symbol bar and press the right mouse button.

These buttons are always available:

Apply

Saves your changes of the program.

What's this?

This enables you to get help information about all buttons and parts of the program.

Change representation of the symbol bar

1. Point with the mouse on the symbol bar and press the right mouse button.
2. Choose a display type.

Following representations are available:

Symbols and Text

The buttons will be displayed with big symbols and text.

Only Symbols

The buttons will be displayed with big symbols.

Text only

The buttons will be displayed only with text.

Small Symbols

The buttons will be displayed with small symbols.

Hide Symbol bar

Will hide the symbol bar.

The Function bar

The function bar is on the left side of the window and contains all dialogs. To use one of them just click on the symbol. The scroll button is used to scroll because of the window size it may possible not all services can be shown in the function bar.

You also can use the menu item *Dialogs*. The actually chosen dialog will be shown in the dialog headline.

The Status bar

The status bar is found in the bottom line of the main window. Here information to the menu commands and buttons is shown. The command status bar in the menu item **View** activates and deactivates the status bar. You may as well deactivate the status bar if you click on it and choose the **Hide status bar** option.

Language selection "on the fly" (EN)

Here you may change the language of the program, this also affects the online help. Rebooting the program is not necessary.

Help line

The help line shows short information of the chosen command or where the mouse pointer is pointing.

Dialog System

The dialog *System* shows the state of all MERCUR services. This means the SMTP service, the POP3 service, the IMAP service, the Fax-/Pager-Gateway and the CONTROL service. Every service will be shown separately. With **Start** and **Stop** you may start or stop any service separately. To update the display press **Update**. You may as well install or uninstall services in the pop up menu of the chosen service.

Install a MERCUR service

To install MERCUR services please enter the menu item *System*. Now choose the services and push **Install**. After this you will be asked if you want to auto run the services. If you decide so the services will be started automatically if you turn on your computer. Else you have to start it by yourself.

Uninstall a MERCUR service

To uninstall a MERCUR service please enter the menu item *System*. Now choose the service and push **Uninstall**. Now you will be asked if you are sure about to uninstall this service. If you accept the service will be uninstalled else it will stop to do so.

Dialog box Connect

You may edit the MERCUR Messaging 2005 with every computer in a network. This may be a local as well a computer or workstation in a TCP/IP network. These computers or workstations have to use the same version like the one you want to administrate.

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

Press [Connect](#) if you want to administrate a remote computer. You will see the [Connect to...](#) menu. Here you have to enter the name or IP address of the host and your [complete email address](#) as user name and the password to login.

To disconnect from the remote computer press [Disconnect](#).

The MERCUR administration service has got a HTTP interface. This enables you to administrate the MERCUR Messaging 2005 with every known browser e.g.: MS Internet Explorer or Netscape Communicator as well as the Navigator. If your administration service is set to the standard HTTP interface (80) no connection has to be entered because your browser normally uses this one (see [Mercur Remote configuration with Browser](#)).

Only user with sufficient administration rights may administrate the MERCUR (see [Users](#)).

Dialog Domains

This feature is limited of 3 domains in the Standard Edition of MERCUR Messaging 2005.

This feature is limited of 1 domain in the Lite Edition of MERCUR Messaging 2005.

With every basic license from the MERCUR Messaging 2005 you may administrate as many domains as you like. The destination of every incoming mail will be controlled by MERCUR and send on there destination. Mails for remote domains will send on to the responsible server.

The dialog *Domain* will show you a list with all existing domains and names of these e.g.: *domain.com* and if existing a description. Here you got the possibility to change the alphabetical order by clicking on a column. The pointer will show the direction.

With the buttons **Add**, **Delete** and **Edit** in the symbol task line you administrate and edit your domains. These functions are also available in the domain general view. For editing an existing domain just double click on the item and you get shown the dialog *Edit domain*. Here you manage essential adjustments for the domain administrator, the domain list server and how to work out messages for unknown domain users. The members of a Windows NT/2000 user account may be used as local users of the respective domain.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

Domain settings

In this part you will set the main adjustments to the domain administrator, the domain list server, how to work out messages for unknown domain users and may enter the owners of a Windows NT/2000 user account as local users in the respective domain

Domain

The name of the mail domain, which should be used for the local email addresses, e.g. *domain.com*.

Description

A description string for this domain

Administrator

Here you will define the alias as well as further aliases for the mailbox of the administrator in this domain.

Mailbox name

The respective mailbox to which the messages for the domain administrator get send. The standard setting is *admin*. If you administrate more then one domain this has to be definite, e.g.: *domain.com/admin*. You are able to direct administrator messages to any local mailbox in MERCUR so as well you may enter here the name of the mailbox so you do not have to collect the mail from the administrators account, e.g. *domain.com/user*.

Standard Alias

The alias name of the administrator which normally is used for this domain, e.g.: *postmaster*. This declaration is important for generating messages to the administrator.

More Aliases

Registers in this list will provide you with more aliases for the administrator account. They are only used for identification from incoming messages. With the *Add* button you can add a custom alias to the list. The *Delete* button deletes a selected alias from the list. Contains a message send to this domain one of this aliases then the message will be send to the mailbox of the administrator.

List server

Here you will define the aliases for the listserver of this domain. The list server is used to work up the mailing lists. To send list server commands, e.g.: *subscribe*, *lists*, or *get* to the list server you have to enter the alias/aliases of the e mail address from the list server.

Standard alias

The alias name of the list server address which should get used on this system, e.g.: *listserv*.

Unknown users

In this field, you can define how incoming messages for unknown user accounts should be handled.

Reject mail

If this option is set, all incoming emails for unknown addresses will be rejected.

Send info to administrator

This option will generate messages for all rejected emails and send them to the administrator.

Forward to

If you even want to receive all emails for unknown addresses, you can specify a special destination address/domain or host to route these emails. If the *Original domain as hostname* option is selected, the domain name of the original address is used as hostname.

Send info to originator

This option will generate a message and send it to the originator if the mail has been transmitted to another address.

Windows NT/2000 user (*Enterprise Edition only*)

MERCUR may use the integrated security from Windows NT/2000 for administrating users. So members of a Windows NT/2000 user account may be used as local users of the respective domain. The alias and password will be the login data from the Windows NT/2000 user manager.

This feature is only available in the Enterprise Edition of MERCUR Messaging 2005.

Include Windows NT user manager for this domain

Select this option if you want to include Windows NT user manager with this domain. The Windows NT/2000 user will not be shown in the *Users* dialog but are on a par with shown users. If you like to use features from the MERCUR user adjustments for Windows NT/2000 user you have to register them.

Account

Choose the Windows NT user account, whose members should have mail permissions for this domain.

Domain

Enter here the name of the Windows NT domain controller or the Windows NT domain, which should be used to login. If your network contains only one domain controller, you can enter a single dot or period.

Dialog Users

MERCUR Messaging 2005 administrates a separate mailbox for every user in which the mail will be stored till it gets collected. These may be a local or remote mailbox. You may give several users a common mail account if you assign them for the same mail account. If you like to grant a user several mail accounts you have to give him several login names with several mail accounts.

The dialog *Users* will show you a list with the email address, login name and complete name of all users in the selected domain. The users will be sorted automatically in alphabetical order if you click on one of the fields *login name*, *name* or *email address*. The alphabetical order will be indicated by a small pointer left beside the field. The list box domain enables you to see the list of all users or just of one domain. If you choose all domains the users will be sorted alphabetical order with no attention from which domain they come from. With the *Filter* option the shown users will be restricted on the entered text. This enables you to find special users very quickly.

With the buttons *Add*, *Edit*, *Delete* and *Import System accounts* you will administrate and edit your users. To edit an existing user click on the *Edit* button, you may also double click on a entry. Here you may make general settings to the user, his mailbox, and the mail copies of this user, the user options and the remote mail accounts.

This feature is limited of 15 users in the Lite Edition of MERCUR Messaging 2005.

User settings

This chapter contains only information about settings in the register *User* in the dialog *Edit user*. Settings in the register *Option* will be explained in the chapter *User options*.

User

Here you may define general entries for the specific user account.

Alias

The alias part of the mail address: *info@domain.com*.

Domain

The domain part of the mail address: *info@domain.com*

Name

The complete name of the user. Used primarily as a reference point or description.

Login name

Name of the mail account. This name is used for POP3 or IMAP4 login. In most cases, this name is the same as the alias name. However if you have similar alias names under different domains (e.g. *sales@domain1.com* and *sales@domain2.com*) you will need to modify this field.

We recommend that you use the alias portion of the field plus the first portion of the domain name. (e.g. *salesdomain1* and *salesdomain2*)

Password

POP3 or IMAP4 password for the individual user. You need this password to download your messages from the POP3 or IMAP4 server. The password is encrypted and needs to be entered twice to confirm that the correct password was used when setting up the user account.

Forward to..

Local mailbox

The incoming messages will be stored in an individual user specific mailbox on the local server. Mailboxes are sub directories in the basic mail directory. A mailbox can be shared by multiple user account.

Type

MERCUR supports two kinds of mailboxes, POP3 and IMAP4. You can select what type of account you are creating (*POP3* or *IMAP4*).

Mailbox size unlimited

Here you will grant the user an unlimited mailbox size. If you use this option for multiple user make sure that you have sufficient hard drive space.

Limit mailbox size to

Enter here the maximum size of the mailbox in Kbytes. The mailbox cannot contain more data then allowed. If the mailbox is full, no more incoming mail will be accepted.

Remote address

If the user has no mailbox on the local system, you can specify a remote email address. MERCUR even accepts the incoming mail for this address and redirects it to the corresponding address. This address must correspond with the Internet-Standard Protocol for email addresses (e.g. *username@domain.com*).

Copies

Received messages

All incoming messages for this address will be copied to a predefined mailbox. If you enter more than one direction you have divide them by semicolons.

Sent messages

All outgoing messages from this address will be copied to a predefined mailbox. If you enter more than one direction you have divide them by semicolons.

User options

This chapter contains only information about settings in the register *Options* in the dialog *Edit user*. Settings in the register *User* will be explained in the chapter *Add/Edit user*.

Options

Here you administrate user options and their remote mail accounts.

Respond automatically with

Create a custom Auto-Responder profile to use as an automatic response of all incoming messages for a specific address. The incoming messages will be saved in the corresponding mailbox and immediately answered by the auto responder.

Add originator addresses to mailing list

The sender of an incoming mail can be added to a mailing list. With this feature you get an overview to all addresses received and it facilitates sending group messages all in one step.

Delete mail older than ...

Enter here the maximum duration of messages in this mailbox. All messages will be deleted after the set time passes. All email in this mailbox will be deleted, even uncollected mail.

Forward mail older than...

Enter here the maximum duration for messages to remain in this mailbox. All messages will be forwarded to the given email address if the user does not collect their email.

Info to administrator, if older then...

With this option the administrator will be send a message if no mail got collected from this mailbox in a defined time range.

User can send mails to local domains only

With this option you may permit the user only to send mail in the local system. The destination of all mail will be controlled. If the direction is not available in the local system the mail will not be send.

Administrator permissions

Use this button if you want to allow a user to configure the MERCUR services using the remote configuration services.

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

....all Domains

Use this button if you want to allow a user to configure the MERCUR services using the remote configuration services. The login must contain the complete email address and the password.

....this Domain only

Use this button if you want to allow a user to configure a local domain only using the remote configuration services. The login must contain the complete email address and the password.

Remote mail accounts

Insert one or more Remote Mail Accounts (POP3 or IMAP4), that require to be checked for this user account. These accounts must be defined as Remote Mail Account. This is an easy way to integrate mail accounts from external mail system into your local system (see Remote Mail Accounts).

Available mail accounts

Shows you a list of all available remote mail accounts of this domain. Domain accounts these are remote mail

accounts where the *Parse mail header* option is used are not available here. Push the *Add* button to add an account to the list.

Selected mail accounts

Shows you a list of all remote mail accounts of the user. Press *Delete* to delete an account from the list.

Mailing Lists

The integrated listserver enables you to create own mailing lists to send information's automatically to multiple destinations. You may enter as many members as you like to a mailing list. You only have to send your message to the mailing list and MERCUR will send on the message to all members of the selected list. Unknown users may *join* or *subscribe* in a list and *leave* or *unsubscribe* if you grant them this administration rights. The mailing list service contains many options to make your individual setting. Header settings like e.g. *Reply-To;* *To;* and *From;* may freely defined by you. Administration rights for owner, members and other users may set separately. The index administration enables you to attach text and binary files to mailing lists.

The dialog *Mailing list* will show you a list of all mailing lists with email address and description. The mailing lists will be sorted automatically in alphabetical order if you click on the field *name* or *email address*. A small pointer left beside the field will indicate the alphabetical order. The list box *Domain* will show you all domains (*-All Domains-*) or just special domains. With the *Filter* option the shown mailing lists will be restricted on the entered text. This enables you to find special auto responder very quickly.

You have as well the symbol bar items *Add*, *Edit* and *Delete*. With these you may edit add and delete mailing list. To edit a mailing list you may also double click on the name shown in the window. Then you may change the settings of the mailing list, the options and the file index.

Mailing List Settings

This chapter only explains the register *Mailing-List* of the dialog *Edit Mailing List*. The setting of the register *Options* will be explained in the chapter *Options*. The setting of the register *Members* will be explained in the chapter *Add Members*. And the setting of the register *File Index* will be explained in the chapter *File Index*.

Mailing-List

Here you will make settings to the address, owner and general settings of the mailing list.

Alias

The alias part of the mail address, e.g.: *info@domain.com*

Domain

The domain part of the mail address, e.g.: *info@domain.com*

Description

The name or a general description of this mailing list. This description is just for you and may free chosen.

List owner

Enter the list owner. All list activities are documented and sent to the list owner. If the list is not public, only the list owner can decide who becomes a member.

Alias

The alias part of the list owners email address.

Domain

The domain part of the list owners email address.

Options

Here you will define general options for the mailing list. More settings for the files and authorization you will find in the *Option* register.

Send message copy to list owner

This flag induces the mailserver to send a copy of all list messages to the list owner. This feature provides, the list owner with full control of any messages sent to the list without being a member of this list.

Deny EXPN command

Select this option if you do not want to execute an EXPN command. The EXPN command is used to show all members in a list.

Max. message size...

You can limit the maximum size of Mailing List message. This prevents large messages from being sent to list members. Enter the maximum size (in Kbytes) that a message size should not surpass.

Send with low priority

A Mailing List mailing often causes a high volume of outgoing messages. In order not to delay normal message activity, we recommend that you set the mailing list activity on a LOW Priority. This will allow normal mail activity to have a higher priority.

Max. number of recipients...

Enter the maximum number of recipients that a Mailing List may contain. This feature helps control the size of a mailing list and prevents a mailing list from growing too big.

Set list owner to 'From:' field

If this option is enabled, MERCUR will replace the *From:*-field of the message header with the address of the list owner.

Send info to list owner when a member joins the list

Use this feature to activate a short info message to administrator if a new member joins the list.

Send info to list owner when a member leaves the list

Use this feature to activate a short info message to administrator if a member leaves the list.

'To:' field contains

Depending on effort of the Mailing List, the header fields of the message can have different importance. Use this list to select what kind of information the *To:*-field should contain.

'Reply-To:' field contains

The *Reply-To:* field in a message header is very important field for managing responses. If a message was sent through a Mailing List, the reply address is not always accurate. If the field contains the email address of the list itself, then all members will get a reply. This can be a useful feature for discussions groups, but it is not recommended for regular information distribution.

List options and permissions

This chapter only explains the register *Options* of the dialog *Edit Mailing List*. The setting of the register *Mailing List* will be explained in the chapter *Add/Edit a Mailing List*. The setting of the register *Members* will be explained in the chapter *Add Members*. And the setting of the register *File Index* will be explained in the chapter *File Index*.

Options

Here you will make settings to files and authorizations.

Files

List members

Specify the name of the list file. All list members will be stored in this file. You can also choose an existing file to import new members.

File index

Enter the name of the file that should be used to store the components of the file index, or you can select an existing file. The file index is used to append files to a Mailing List. List members can then receive these files by sending a *GET* command to the listserver (see *listserver commands*).

Header for all messages

You can place a default header for all messages in a Mailing List. Enter the name of the text file that contains the header information.

Footer for all messages

You can add default footer for all messages in a Mailing List. Enter the name of the text file that contains the footer information.

Info to new members

Enter the name of a text file, which contains a greeting for all new members. This file will be sent when a new member joins the list.

Log list activities to file

Enter the name of a text file that will be used to log all mailing list activities.

Permissions

MERCUR allows administrators to setup detailed access permissions for each mailing list. The permissions section is subdivided into three different categories, Owner, Members and Anyone. The common definition anyone applies to all Internet users who are currently not a member or the owner of a mailing list.

Send message to the list

Enable this option if list members in a specific mailing list should have permission to send messages to the rest of the mailing list.

Add new members to the list

Enable this option, if new members can join the mailing list automatically. New members can join a mailing list by the *SUBSCRIBE/JOIN* command (see *listserver commands*). If this option is not enabled, then all new requests will be routed to the list owner. The list owner will have to manually add the new members to the mailing list.

Remove members from the list

This option allows members in a mailing list to remove themselves or other members from a mailing list.

Show members using REVIEW/RECIPIENTS

The *REVIEW/RECIPIENTS* command (see *listserver commands*) is used to request a list of all members. Select who should have permission to use this command.

Show file index using INDEX

The file index is used to append files to the Mailing List. Members can receive the index (a listing of files) by sending the *INDEX* command (see *listserver commands*). Select who should have permission to use this command.

Download file using GET

The *GET* command is used to receive files from a mailing list (see *listserver commands*). Select who should have permission to use this command.

Show the list on LIST command

The *LIST* command displays a list of all available Mailing Lists on the MERCUR Messaging 2005 (see *listserver commands*). Enable the setting to allow a mailing list to be displayed during a *LIST* query.

Add Mailing List Members

This chapter only explains the register *Members* of the dialog *Edit Mailing List*. The setting of the register *Mailing List* will be explained in the chapter *Add/Edit a Mailing List*. The setting of the register *Options* will be explained in the chapter *Options* and the setting of the register *File Index* will be explained in the chapter *File Index*.

Members

Here you will see a list where all members of the selected mailing list will be shown. You also may add and delete members of the mailing list. It is as well possible to import members from a text file.

Import

With this button you are able to import members from a text file. In the menu item you have to enter the file name from the file you want to import the members. As well you have to enter the order of the member data (e.g.:name, email address). Also you have to enter the separator and the text delimiter.

File Index

This chapter only explains the register *File Index* of the dialog *Edit Mailing List*. The setting of the register *Mailing List* will be explained in the chapter *Add/Edit a Mailing List*. The setting of the register *Options* will be explained in the chapter *Options* and the setting of the register *Members* will be explained in the chapter *Add members*.

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

Here you will see all available files in the mailing list. Press add if you like to add a new file. You will see a box where you have to enter the file name, the description and the file path. The file type may be text files (ASCII) or binary files. If you like to attach binary files you have to send them MIME encoded. Otherwise it is not possible to send these files.

Overview list server commands

List server commands

This list server feature is one of the most important components in a Mailing List. The list server is responsible for executing all list server commands. Each MERCUR domain can have its own list server address, e.g.: listserv@domain.com. All messages sent to this list server address will be parsed for commands. These commands will be executed if the correct permissions were enabled. This way, a list member is able to join a mailing list by sending message which contains the **SUBSCRIBE** command. The MERCUR list server supports the following commands:

JOIN or SUBSCRIBE

These commands are used by users, who want to join a mailing list. These commands are valid if the list owner enabled the permissions. Otherwise, the list owner will receive a request message from the new mailing list member and the list owner will have to manually add the new member to the mailing list.

Usage

```
join list address,[mail address],[full name]
or
subscribe list address,[mail address],[full name]
```

The values inside the braces are optional. If no mail address is given, then default values found in the email message will be used.

LEAVE or UNSUBSCRIBE

Users can leave a mailing list automatically by using the **leave** or **unsubscribe** command.

Usage

```
leave list address,[mail address]
or
unsubscribe list address,[mail address]
```

The values inside the braces are optional. If no mail address is given, then default values found in the email message will be used.

LISTS

Use this command to get a listing of all local public mailing lists that are available on the MERCUR Messaging 2005.

Usage

```
lists
```

This command has no arguments

WHICH

This command gives you listing of all mailing lists that you have subscribed to.

Usage

```
which [mail address]
```

The values inside the braces are optional. If no mail address is given, then default values found in the email message will be used.

INDEX

This command gives you listing of all available attachment files in the mailing list.

Usage

`index <list address>`

RECIPIENTS or REVIEW

Provides a listing of all members in a specific mailing list.

Usage

`recipients <list address>`

or

`review <list address>`

GET

The **get** command is used to receive document files from a mailing list via email. Enter the name of the mailing list and the file name.

Usage

`get <list address> <file name>`

HELP

Use this command to get a description of all list manager commands.

Usage

`help`

This command has no arguments.

Dialog Auto Responders

If you define an auto responder for a user then the auto responder will automatically answer all incoming mail from this user.

The dialog *Auto-Responder* will show you a list of all auto responder with names and domains. The auto responders will be sorted automatically in alphabetical order if you click on the field *name* besides the field *domain*. The alphabetical order will be indicated by a small pointer left beside the field. The list box *Domain* will show you all domains (*-All Domains-*) or just special domains. With the *Filter* option the shown auto responders will be restricted on the entered text. This enables you to find special auto responder very quickly.

You have as well the symbol bar items *Add*, *Edit* and *Delete*. With these you may edit add and delete auto responder. To edit an auto responder you may also double click on the name shown in the window. Then you may change the settings of the auto responder, the time range or determine users, which should not receive auto responder generated mails.

Auto Responder settings

Auto-Responders are used to create and send automatic replies for specific events. You can specify the text file that contains the message text, the log file or an address mask to exclude addresses from being processed.

Description

Name

Enter the name of the Auto responder. The name may freely chosen.

Domain

Global

The global domain specifies the range of the Auto-Responder. Choose Global, if the Auto-Responder is available for all users on the MERCUR Messaging 2005. Settings for the special domain option will not affect any other auto responder on the system.

Special Domain

You can configure a special domain to use an Auto-Responder. The range of the Auto-Responder is limited to a specific domain. This is a useful feature when a MERCUR Messaging 2005 has multiple domains with multiple auto responders with the same name.

Respond with

Text file

Choose a text file that contains the message text to be sent. Press the Edit button to edit this file. The file must be an ASCII file format. If the text contains special characters, you must use MIME to encode it before it is sent out. You may also enter variables found under [Add Field](#).

Text

If the Auto Responder requires only a short message (max. 230 Characters), then you can enter it directly in the text description field. Then no text file is needed. You may also enter variables found under [Add Field](#).

Options

Here you will set the options for the auto responder. You may determine if the call from the auto responder should be protocolled and in which text file this should happen. As well you will set the time range in which the auto responder is executed. You also may determine email addresses, which will not get any auto responder mails.

Log

Log responses to file

If this option is enabled, then all auto responder activity will be logged to this file. Push the [Select](#) button to choose an existing file.

Time range

Enter the time frame for the auto responder to execute. The auto responder is only executed, if the auto responder event occurs within the allotted time frame.

Delete Auto Responder after expiration

If this option is enabled, MERCUR will delete an auto responder automatically after the time frame has expired.

Exception

Enter an address mask that is to be excluded. Press the [Add](#) button to add a new entry to the list box. Use [Delete](#) to remove an entry from the list box. Wildcards are accepted.

Example: mailer-daemon*

All addresses with the string [mailer-daemon](#) at the begin will be excluded, e.g. [mailer-daemon@domain.com](#).

Enable duplicate response cache

All recipient addresses of this auto responder message are stored in this duplicate response cache, so that each address will get the auto responder message only once. All recipient addresses will not get furthermore this auto responder message until the duplicate response cache are cleared. MERCUR will not automatically clear the duplicate response cache.

Use the [Clear cache](#) button to remove all addresses out of the cache.

Dialog Executables

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

Trough sending messages to the mail address of a defined executable you may execute commands on your system. For example you may change passwords. The dialog *Executables* will show you a list of all executables with name and email address .The executables will be sorted automatically in alphabetical order if you click on the field *name* or *email address*. A small pointer left beside the field will indicate the alphabetical order. The listbox *Domain* will show you all domains (*-All Domains-*) or just special domains. With the *Filter* option the shown executables will be restricted on the entered text. This enables you to find special executables very quickly.

You have as well the symbol bar items *Add*, *Edit* and *Delete*. With these you may edit add and delete executables. To edit executables you may also double click on the name shown in the window. Then you may edit the executables.

Executable Settings

Executables are used to carry out commands or run applications on a local system or server. With the help of certain keywords, you can launch an application. This feature allows you to perform simple tasks via email (e.g. change password).

Address

Alias

The alias part of the command email address: [change~~pass~~@domain.com](mailto:changepass@domain.com)

Domain

The domain part of the command email address: [change~~pass~~@domain.com](mailto:changepass@domain.com).

Description

The name of the executable file.

Command

Application

Enter the name of the application, that you want launch with the executable profile. All executable files are accepted.

Parameter

Enter the arguments, which should be used to execute your application. You can use static values or variables. Variable names must begin and end with two percent signs (e.g. `%%subject%%`). You can define your own variable names. These names will be queried in the message text using the keyword definition. The following predefined variables are available:

The arguments must be separate by an empty space.

```
%%From:%%  
%%To:%%  
%%Subject:%%  
%%Date:%%  
%%Message-Id:%%  
%%Reply-To:%%  
%%MIME-Version:%%  
%%Content-Type:%%  
%%Content-Transfer-Encoding:%%  
%%X-Mailer:%%  
%%Messagefile-Name%%
```

The above variables are values from a mail header. The `%%Messagefile-Name%%` variable means that the file contains complete message.

Forward message to local mailbox

Under normal conditions MERCUR will not store executable type messages in the same local mailbox with other standard messages. All messages stemming from an executable command are assigned to a new local mailbox.

This is a useful feature if the contents of an executable message are to be used by an application.

Keywords

Execute without keywords

If this option is enabled, the executable command does not use any of the owner's defined variables. Instead the message text is only queried for predefined variables.

Use the following keyword definitions

With this option, the message body will be queried for additional variables. These variables must appear in the same format as defined in the keyword field.

Example: Name: %%username%%
Old Password: %%oldpass%%
New Password: %%newpass%%

This feature is very useful when you want to change passwords via email. The values for *username*, *oldpass* and *newpass* must match exactly with this format.

Executable HOLIDAY

The following MERCUR mail server executable can be used to add an auto responder via email. The application used should be *HOLIDAY.EXE* in the MERCUR directory. The field parameters must contain the following information in order to create and activate an auto responder.

Note: the parameters must be separated by a blank space.

The option *Execute without keywords* must be enabled.

This is an example of an email that will be sent to the executable, allowing MERCUR to add and activate a new auto responder for a user.

The email must be sent as a text/plain message (*no HTML based messages*). The content of the subject line is not important and can be left blank. The body text in the email must contain the auto responder text. This text should have a maximum length of 230 signs including blanks.

When this email is sent to the executable it will add a new auto responder for the user. The auto responder will be activated immediately.

Dialog Remote Mail Accounts

If your Internet provider does not send your mail automatically you may use the MERCUR Messaging 2005 to collect your mail. You are enabled to administrate several remote mail accounts on several mail server. The remote mail accounts may be granted separately or as a shared user account. In this case MERCUR will distribute the mail automatically.

The dialog *Remote Mail Accounts* will show you a list of all remote mail accounts with names, domains and servers from the remote mail account. The remote mail accounts will be sorted automatically in alphabetical order if you click on the field *name, domain* or *host*. The alphabetical order will be indicated by a small pointer left beside the field. The list box *Domain* will show the remote mail accounts from all of domains (*-All Domains-*) or just from special domains. With the *Filter* option the shown remote mail accounts will be restricted on the entered text. This enables you to find special remote mail accounts very quickly.

You have as well the symbol bar items *Add, Edit* and *Delete*. With these you may edit add and delete your remote mail accounts. To edit a remote mail accounts you may also double click on the name shown in the window. Then you may change the settings of the remote mail accounts, the login, the time range and or the options.

Remote Mail Account Settings

Remote Mail Accounts are user accounts on external POP3 or IMAP4 servers. You can assign MERCUR to check for waiting mails on the remote server. You can also receive mails from shared mail accounts and split these into multiple user mailboxes on your local system.

Remote Account

Description

This is the name given to a specific remote mail account.

Server

This is the name or IP address of the mail server, which should administrate the remote mail account.

Domain

Global

The domain specifies the range of the Remote Mail Account. Choose *Global*, if the Remote Mail Account is available to all users on the local system. Settings for the special domain option will not affect any other auto responder on the system.

Special Domain

You can allocate a special domain to the Remote Mail Account. In this case, the range of the Remote Mail Account is limited to the particular domain. This is a useful feature when a MERCUR Messaging 2005 has multiple domains with multiple auto responders with the same name.

Login

Use login name from user account

If this option is enabled, the login name and password from the user account is used. This option is only available, if this is *NOT* a shared account.

Use alias from user account

If this option is enabled, the alias and password from the user account is used. This option is only available, if this is *NOT* a shared account.

Special login

This login enables access to a shared POP3 or IMAP4 account.

Login name

Enter the login name, to log into the remote POP3 or IMAP4 host.

Password

Enter the password, to log into a remote POP3 or IMAP4 host.

Schedule

Setup the time intervals to initiate the Remote Mail Account. The scheduling feature in MERCUR allow for detailed time settings. You can update a Remote Mail Account frequently, e.g. *daily between 8:00 and 18:00 every 15 minutes, at night every 2 hours* and *at the weekend only twice a day*.

Press the *Add task*, button to add a new schedule entry. The Edit task screen is used to change a schedule entry. The available options are used as follows:

Add or Edit

Press the *Add* button to add a new schedule entry. The Edit task screen is used to change a schedule entry. The available options are used as follows:

Execute

Press the *Execute* button to immediately collect the mail from the selected remote mail account.

Weekdays

The schedule task is allocated to the selected weekdays. If no weekday selection is made, the task will not run.

Frequency

Once, at startup

Select this option to perform the task immediately on startup.

Once, at ...

Use this option to specify an exact time of day to perform the task. The value is represented in a 24 hour format.

Periodical every...

Enter here the time interval for a periodical update. This value must be in minutes or hours. You can also define if this task should run the whole day or only for a specific period. This value is also available in 24 hour format.

Message size

This option specifies a maximum message size. If you enter a maximum value, all messages larger than this value will stay on the remote server.

Options

Parse mail header for recipients (*Shared Mail Account*)

Enable this option, if this account is a shared POP3 or IMAP4 account. In this case, incoming mail will be saved to the corresponding user mailboxes on a local system. To use this option, you will require both a login name and password. You can also select the type of header fields to be parsed in order to determine validity of an email address.

Delete mail from server

Select this option if incoming mail should be delete on the remote server. If you use POP3, this option should be activated. If you do *not* use this option, then you should use the *Receive only unread message* option.

Receive only unread messages

Select this option, to turn on the message id checking. This prevents receiving duplicated messages. This option is very useful if *Delete mail on server* is *NOT* enabled.

Synchronize with Out Basket

If this option is enabled, the remote mail account will be checked whenever the out basket is updated. This is a very useful feature to use with an open dial-up connection. It is not recommended feature when using a network connection.

Dialog Static Routes

This feature is limited of 3 static routes in the Standard Edition of MERCUR Messaging 2005.

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

Static Routes are used to filter incoming mail and forward the incoming mail directly to other mail server or domains for further processing. This option is especially important to bigger networks. All available header fields can be used to filter messages. With using out baskets you are able to enter time frames to forward waiting messages via static routes. For the criteria definition all Header fields, host, message size and the destination is available. Static Routes have priority when processed and are processed prior to any user manager settings being processed. That means as well messages that have been processed by a static route do not have to be processed again.

The processing of static routes follows an alphabetical order. This means that routes with very special filters have to be on top of the alphabetical list to ensure that the mail is correctly filtered. The dialog *Static Routes* will show you a list of all Static routes with names, direction and type. The Static routes will be sorted automatically in alphabetical order if you click on the field *Name*, *Forward to* or *Type*. The alphabetical order will be indicated by a small pointer left beside the field.

You have as well the symbol bar items *Add*, *Edit* and *Delete*. With these you may edit add and delete Static routes. To edit a Static route you may also double click on the name shown in the window. Then you may change the settings of the Static route, the filter or the server options.

Static Route Settings

Static-Route

Name

Enter the name of the static route. The name may freely chosen. MERCUR will sort the static routes automatically in alphabetical order.

Activity

This is the task that the static route will execute or perform. The following options are available:

Forward to mail-address

If this option is enabled, all mail will be forwarded directly to a given email address.

Forward to mail-domain

If this option is enabled, all mail will be forwarded to a given mail domain. In this case, the alias does not change.

Forward to remote mail host

Select this option to forward incoming messages to another mail host. The register *Host Options* contains additional options to set a time frame for forwarding messages.

Forward to original domain as host

This option works as described above. In this case the name of the original recipient domain will be used as host name.

Delete !

If this option is enabled, the message will be deleted without any further processing.

Address

Enter the needed email address, mail domain or the remote mailserver. If you choose the option *Forward to original domain as host* you do not have to enter any information.

Filter

Here you enter the criteria for filtering incoming messages. The static route is only active if all the criteria are valid. You may use default or installable filters.

Use default filter

Enter the criteria for filtering incoming messages. This static route is only active if all the criteria are valid. You can select all header fields, as well as the sending host, the message size, the originator address and the recipient address.

Press *Add* to add a new filter entry, an *Edit Filter* dialog box will pop up.

Use installable filter

MERCUR support user defined filters. A user-defined filter is a library (*DLL*), which contains a special entry point. MERCUR calls this *DLL* to handle the filter processing. This is an easy way to insert user defined functions into the message chain. The creation of gateways (e.g. *Fax*) should not be a problem. The DLL must contain the following entry point:

```
BOOL WINAPI MCRFilterProc(MCR_FILTER_DATA FAR *data)
```

The definition of the MCR_FILTER_DATA structure as defined as follows:

```
typedef struct
{
char szOrigAddress[255];           // Originator address
char szRecipAddress[255];        // Recipient address(es)
char szFileName[260];           // Temp file, which contains the current mail
HANDLE hTempFile;               // Handle to the opened temp file
} MCR_FILTER_DATA;
```

The *MCRFilterProc* function can be used to modify the originator and the recipient address, as well as the whole message text. The return value is *BOOL* and works as follows:

FALSE MERCUR should not perform any further processing.

TRUE MERCUR must perform further processing using the changed data of *MCR_FILTER_DATA* structure.

Default Filter Settings

Here you set the criteria which incoming messages must match. The route is only active if all criteria are met. For the criteria definition all Header fields, host, message size and the destination is available. Push *Add* to add a new filter.

Operator

Operator

Use the *AND* as well as the *OR* buttons to specify the handling of multiple filter entries. This option may be activated after the second filter entry. If the *AND* is selected, *ALL* conditions must be valid to execute the static route. If the *OR* is selected, only one valid argument is sufficient.

Expression

Header-Field

You can select all header fields, the originator address and the recipient address. Select the correct setting if the field criteria must match a full or partial description.

From Host

Enter the name of the sending host. If the address of the sending host matches with this address, the argument is valid.

Message size

Enter here a maximum or minimum message size to use as criteria.

Server Options Setting

This register is only available if you choose the option *Forward to remote mail host* or *Forward to original domain as host* as execution.

Connection

Wait until the remote host opens the connection

If this option is selected, all incoming mail will be stored on the local system and forwarded only when the remote host opens the connection to the local system.

Wait until the remote host sends an ETRN request

Select this option, if the forwarding of a waiting message(s) is to be executed by an ETRN command. In this case, you need to enter the name of the out queue (*Nodename*).

Caution: The nodename within an ETRN command is transmitted without any kind of encryption. That means that ETRN does not provide 100% security.

Use dial-up connection

If a Remote Access connection is used, select the Remote Access profile here. The login name and password is used for the network.

Scheduling

Enter the time frame to forward waiting messages via this static route. The scheduling feature in MERCUR allows detailed time intervals. Therefore you can update a static route frequently e.g. *daily between 8:00 and 18:00 every 15 minutes, at night every 2 hours* and *weekends only twice a day*.

Press the *Add* button to add a new schedule entry. The *Edit Schedule Entry* dialog is used to modify and add new schedule entries. The available options for this feature are:

Weekdays

This selection allows complete freedom to select what weekdays you want the tasks to run. If there is made no selection the task will not run.

Execution

Immediately, when the mail arrives

Choose this option to forward messages immediately. If you use Dial-Up connection, it will be opened immediately.

If the out basket contains more than ... messages

This option forwards outgoing mail when a certain number of messages are waiting in the out basket.

Once at ...

Use this option to specify an exact time of day to update outgoing mail. This value is set in a 24 hour format.

Periodical every...

Enter the time interval for periodical updates. This value must be in minutes or hours. You can also set a task to run the whole day or only for a specified time period. This value is set in a 24 hour format.

Dialog Fax-/ Pager Gateway (Enterprise edition only)

Fax-Gateway

MERCUR Email-to-Fax Gateway is an interface between E-Mail and regular fax devices. In this way, it is possible to receive incoming messages and to then transmit to fax numbers according specific routes. In addition, faxes can also be received and forwarded via E-Mail.

The MERCUR Email-to-Fax Gateway is compatible with all standard *CLASS2-Modems* as well as ISDN adapters that support the *T.30 protocol*. The Fax transfer occurs in accordance with the *Group 4* specification.

Features

Sending fax messages using predefined profiles

With predefined profiles, you can define which kind of messages shall be accepted by the gateway and forwarded by fax. The gateway uses special filters to select incoming messages and forward it to predefined or automatically determined fax numbers.

Receiving fax messages to forward by E-Mail

In receive mode, the gateway gets fax messages from conventional fax devices and converts these messages to MIME coded E-Mail messages.

Use of templates

The individual fax profiles use predefined fax templates. The templates are text files within formatted text elements. Specific fields (e.g. originator address) can be integrated by variables into the fax document.

Support for analog Modems and ISDN boards

The gateway support analog modems and ISDN boards to transmit fax messages. If you use an ISDN board, you need to consider that this board supports the *T.30 protocol*.

Event-Logging

The MERCUR Email-to-Fax Gateway contains an extensive set of protocol functions that controls all events on the mailserver. The event-log provides information on possible errors and data transfer confirmations.

SMS/Pager-Gateway

The MERCUR SMS- Pager Gateway is an interface between E-Mail and SMS compatible mobile phones and pagers. In this way, it is possible to receive incoming messages and then transmit to mobile phones or pagers. The MERCUR SMS- Pager Gateway is compatible with all standard Modems as well as ISDN adapters. The message transfer occurs in accordance with the protocols *TAP* (Telocator Alpha-Paging Protocol) and *UCP* (*Universal Computer Protocol*).

Sending SMS messages using predefined profiles

With predefined profiles, you can define which kind of messages shall be accepted by the Gateway and forwarded to a mobile phone or Pager. The Gateway uses special filters to select incoming messages and forward it to predefined or automatically determined Pager ids.

Use of predefined providers

The individual Pager providers use different settings and device parameters. These values can be defined in special profiles for automatic determination of the responsible provider.

Support for analog Modems and ISDN boards

The Gateway support analog modems and ISDN boards to transmit SMS messages. If you use an ISDN board, you need to consider that the Pager provider supports the *X.75 protocol*.

Event-Logging

The MERCUR SMS- Pager Gateway contains an extensive set of protocol functions that controls all events on the mail server. The event-log provides information on possible errors and data transfer confirmations.

Fax Profile Settings *(Enterprise edition only)*

The forwarding of email messages to fax numbers and sms pagers occurs by predefined profiles. With these profiles, it is exactly specified which kind of messages shall be processed as fax message or as pager message and which profile is used.

The forwarding of E-Mail messages to fax numbers occurs by predefined fax profiles. With these profiles, it is exactly specified which kind of messages shall be processed as fax message and what fax number is used. For send mode (Email-to-Fax), at least one fax profile is needed.

The forwarding of E-Mail messages to mobile phones or pagers occurs by predefined profiles. With this profiles, it is exactly specified which kind of messages shall be processed as pager message and what destination number (Pager id) is used. At least one profile is needed.

You can add, edit or delete profiles using the buttons *Add*, *Edit*, and *Delete*.

Description

Name

This field contains the name of the profile.

Type

Here you will decide the profile. If you decide for the *SMS-/Pager Profile* your next option is *Provider*. If you decide for the *Fax Profile* your next option is *Template*.

Provider

Select here the provider definition, which shall be used with this profile. This definition contains all required information for sending messages using this provider. If the option *<Automatic detection>* is selected, the responsible provider will be determined automatically based on the prefix of the destination number.

Template

Select here a fax template, which shall be used with this fax profile. This template gives the fax document predefined design. If no template is selected, the message body will be processed without any special formatting.

Filter

Accept if...

This filter setting is needed to decide which incoming messages the Email-to-Fax Gateway shall process. The filter inspects the header of the incoming messages. If the gateway should forward all incoming messages for domain *fax.atrium-software.com* to a fax address, the filter has to look as follows:

Accept if: Recipient Address: *ends with* Search text: *fax.atrium-software.com*

If the gateway should forward all incoming messages for domain *pager.atrium-software.com* to a mobile phone address, the filter has to look as follows:

Accept if: Recipient Address: *ends with* Search text: *pager.atrium-software.com*

Take destination number from

Select here which part of the header of the original message should be used as destination fax number. If the item *Alias of Recipient Address* were selected, the further processing would be handled as follows:

Message to *06991398363@fax.atrium-software.com* is forwarded to fax number *06991398363*.

Select here which part of the header of the original message should be used as SMS. If the item *Alias of Recipient Address* were selected, the further processing would be handled as follows:

Message to 06991398363@pager.atrium-software.com is forwarded to mobile phone number [06991398363](tel:06991398363).

Forward to special number

Use this option to specify a special destination number for this profile. In this case, all faxes/sms will be delivered to this number. The service will not perform any kind of mail header checking.

Execution**Forward immediately**

If the option forward immediately is used, all waiting fax messages are transmitted immediately when the next update interval occurs.

Forward between..

Enter here a time range to transmit outgoing fax messages. This option is very useful to handle fax transmissions during low cost time ranges.

SMS-/ Pager Provider Settings *(Enterprise edition only)*

For sending sms/pager messages from different service providers are needed some determined settings. They may be set for each provider separately. You can add, edit or delete these definitions using the buttons [Add](#), [Edit](#), and [Delete](#).

Provider Name

This field contains the name of the service provider.

Access number

Enter here the required access number for this provider. This is the number the Gateway has to dial for sending SMS or Pager messages. A collective number, which is employed independent of the desired target number, is normally employed here. In some cases, the access number consists of the number indicated here and the actual destination number (*Pager ID*). In this case, the option [Append Pager id to access number](#) must be considered.

Destination number

Here you have to enter the destination number of your provider. This will be used for automatically determination of the responsible service provider. It is possible to enter more than one destination number but you have to separate them by semicolons.

Protocol

In general, two different protocols used for sending SMS or pager messages. You can choose here between the protocols [TAP](#) (Telocator Alpha-Paging Protocol) and [UCP](#) (Universal Computer Protocol).

Mode

This option allows you to select a special mode beside the real protocol. The values [Normal](#), [Scall](#) and [Skyper](#) are available here.

Append Pager id to access number

As described in section [Access number](#), the access number can consist of the actual number and the current pager ID. In this case, this option must be activated.

Remove prefix from Pager id

If this option is activated, the destination number (*pager id*) will be transmitted without the leading prefix.

Numeric page mode

Some Pager providers allow only numeric messages texts, e.g. *phone number*. Select this option, if this applies for the current definition.

Max. number of messages per session

In some cases (e.g. *when a collective access number is used*), the service provider allow to send more than one message in only one session. Activate this option if this provider allows this procedure.

Maximum Text length

Enter here the maximum allowed number of characters for the message text. This information is needed for preliminary handling of the message.

Authentication

In some cases, the service provider requires a login. This login can be processed by a special password or else the Pager is itself.

No authentication required

Activate this option, if no login is needed for this profile.

Use Pager id for authentication

Select this option to use the Pager id for login

Use the following authentication

Enter here a password, which shall be used to login for the service provider.

Device

Select here the device, which shall be used for this service provider. The serial modem port, defined in the *Options* section, and ISDN is available here. ISDN means a loaded CAPI 2.0 driver for an ISDN board.

Use T.70 prefix

Here you can enable the T.70 prefix. This is used by some providers, e.g. D1 Network of German Telekom. Other providers use the regular X.75 protocol.

Data bits, Parity and Stop bits

The settings for data bits, parity and stop bits are needed for the provider connection. The most providers use 8 data bits, 1 stop bit and no Parity.

Init string

Some modem types require a special initialization. This field provides space for you to type this commands.

Options Fax-/ Pager Gateway (Enterprise edition only)

Here you will do optional settings for the SMS Pager and the Fax Gateway.

SMS/Pager settings

Activate modem provider

When this option is chosen all messages may be send to modem provider.

Activate ISDN provider

When this option is chosen all messages may be send to ISDN provider.

Cut message text, if text exceeds maximum length

If this option is selected, all messages will be truncated to the maximum allowed number of characters. The allowed number of characters is defined in the individual provider settings

Reject, if message text exceeds maximum length

Use this option to reject all messages, those are too long.

Info to originator

This feature will send a message to the originator of the message that the SMS message was sent successfully to the specified address.

Update interval

The update interval indicates in which time intervals the forwarding of outgoing SMS messages should be processed.

Number of retries for delivery

Here you can specify how often the Gateway should try to deliver outgoing SMS messages. If the message could not be delivered in this time range, the service will send an info message to the originator.

Fax-Gateway-settings

Send attachments, if possible

Select this option, if all convertible attachments shall be attached as further pages to the fax document. The following files types are convertible: Text- and bitmap files of type BMP, PCX, TIF, GIF, JPG or WMF.

Reject, if attachments not convertible

If this option is selected, all incoming messages with not convertible attachments will be rejected on principle. If this option is not used, only the convertible attachments are processed i.e. not convertible items would be ignored in this case.

Info to originato

This feature will send a message to the originator of the message that the fax was sent successfully to the specified address.

Activate fax delivery (E-Mail to Fax)

If this options is selected no other entry is needed. The information is collected from the predefined profiles.

Activate fax receipt for following email address

If this options is selected you have to enter the email address to which the received fax should be send. You may use more than one address but you have to divide them by semicolons(e.g.:alias1@domain.com; alias2@domain.com).

Update interval

The update interval indicates in which time intervals the forwarding of outgoing faxes should be processed.

Number of retries for delivery

Here you can specify how often the gateway should try to deliver outgoing fax document. If the fax could not be delivered in this time range, the service will send an info message to the originator.

Modem Settings *(Enterprise edition only)*

In this register you got different options for your modem. You have to do these settings absolutely correct for a faultless function of the SMS/Pager and the Fax Gateway.

Modem for SMS/Pager

Port

Select here the default settings for your serial communication device. These values are only used as default settings for each provider profile. The provider property dialog allows you to set these flags for each profile separately.

Dial using

This option specifies which type of dialing to use. Specify pulse dialing only if this is the only type your phone line supports. This option is only available for analog modems.

Init string

Some modem types require a special initialization. This field provides space for you to type this commands.

Wait for dial tone before dialing

Enable this option, if your communication device should wait for a dial one before dialing. If your modem is connected with a telephone box it is possible that the dial tone is not accepted. In this case please deactivate this option.

Use line access prefix

In some cases the modem is connected to a telephone box then it normally has to dial an access prefix. You may enter this prefix here.

Modem for Fax-Gateway

Port

Select here communication port that your communication device is connected. In addition to the analogue ports COM1 to COM4, also a CAPI port is available. This is the CAPI 2.0 driver of an ISDN board. Please, note that the ISDN boards need to support the T.30 protocol to work with the Email-to-Fax Gateway.

Dial using

This option specifies which type of dialing to use. Specify pulse dialing only if this is the only type your phone line supports.

Init string

Some modem types require a special command to enable the fax features. This field provides space for you to type this commands.

Wait for dial tone before dialing

Enable this option, if your communication device should wait for a dial one before dialing. If your modem is connected with a telephone box it is possible that the dial tone is not accepted. In this case please deactivate this option.

To access outside line, dial...

In some cases, the communication device is connected to a phone box and needs to dial a special number to access an outside line. If you need to dial a number to access an outside line, please enter it here.

Fax Settings *(Enterprise edition only)*

This register contains some settings for the Fax delivery.

Settings

Speed

Select here the speed for the fax transmission. This value is not the modem speed but the real speed during the fax transmission. Please note that the speed depends also on the fax device on the remote side.

Station-ID

This fax number is used by the gateway to identify itself compared to the remote station. It is only used for receiving faxes and as default setting for sending faxes. If a fax template is used for sending, the local fax number of the template is used.

Resolution

The MERCUR Email-to-Fax Gateway supports the resolutions 200 x 100 DPI and 200 x 200 DPI. The *high* resolution needs to transfer the double amount of fax data as the *normal* resolution, but the received fax image looks much better with *high* resolution.

Header font style

Shows the actual chosen font of the header. To change this you have to push the select button.

Text font style

Shows the actual chosen font for the text. To change this you have to push the select button.

Fax template

Shows a list of all defined fax templates with name, station id and filename. You may add, edit or delete fax templates using the buttons *Add*, *Edit*, and *Remove*.

Edit fax template

The fax profiles will while sending messages work with predefined templates. These templates are text files, which include some text elements or formats. Through variables you may include some fields (e.g.:address of originator).

Description

Name

This field contains the name of the fax profile.

Local Fax Id

The gateway uses this fax number to identify itself compared to the remote station, when a fax is sent using this template.

Header

Left, Middle and Right

Each fax page contains a headline, which consists of three areas. The input fields *Left*, *Middle* and *Right* are used to specify the text for this headline. In addition to regular text entries, variables of the current profile can be used here. To insert a variable, press the button near the input fields. The following entries are available:

<code>%%recipnumber%%</code>	The recipients fax number
<code>%%originnumber%%</code>	The originators fax number
<code>%%origname%%</code>	The originators name
<code>%%origaddress%%</code>	The originators mail address
<code>%%subject%%</code>	Subject
<code>%%date%%</code>	The current Date
<code>%%time%%</code>	The current Time
<code>%%currentpage%%</code>	The Current page number
<code>%%numberofpages%%</code>	The number of pages

Template

File name

The file specified in this field contains the template for fax page itself. In addition to normal text entries, also the fields described above can be used.

Dialog Security

It happens often that so-called *Spammers* use the mail server of other people to forward mail to a high number of recipients. In this case, an incoming message contains maybe hundreds of recipient addresses and the mailserver must create for each recipient an outgoing mail. To prevent this, you can specify protection mechanisms against *Spamming* to protect your system against unauthorized use. After you have setup an option, please use the button *Apply* to save it.

Check name of sending host

This option verifies that the originator host is actually a valid HOST NAME. If you use this option it must exist an A-Entry in the name server for all local workstations. In other wise they wasn't accept by MERCUR. The destination of this option is, the access to your mail server is denied for computers they unknown by your name server.

Check open relay database by using DNS suffix

MERCUR queries the Open Relay database for each sending host if this option is set. The query uses the name server of the *Settings/Server* tab. This option is not available if no DNS server is given. The suffix value is used for the DNS query. It will be attached to the ip-address of the sending host (e.g. 69.132.20.212.relays.ordb.org). In this way, the DNS query reaches the server of the Open Relay database. If the server responds with a valid return value, the address is in the database. So, the connection will be refused.

The Open Relay Database can be used by anyone in the configuration of their own network or mail relay, toward the goal of limiting theft of resources by spammers. By accessing these open relay databases, system administrators are allowed to choose to accept or deny email exchange with servers at these addresses. Please note that such services are not always free. You will find more details at <http://www.ordb.net> for more details.

Reject mail, if originator domain has no MX record

All mail sent by an originator must have a traceable MX record. If MERCUR cannot find an MX-record for this mail message it will reject it. The destination of this option is, the access to your mail server is denied for originator domain they haven't an MX-record in your name server.

Do not relay, if the originator address is not local

In order to prevent *SPAMMER* from using your SMTP server to forward their mail. MERCUR verifies that the user account is actually registered with MERCUR. Some mail server will allow *FAKE* mail address to trick the STMP into thinking the address is local. The destination of this option is, the access to your mail server is denied for originator addresses they are not a valid local address.

Do not relay, if the originator domain is not local

In order to prevent *SPAMMER* from using your SMTP server to forward their mail. MERCUR verifies that the domain name is actually registered with MERCUR. Some mail server will allow *FAKE* domains to trick the STMP into thinking is a local domain. With this option the access to your mailserver is denied for originator domains if they are not valid local domains.

NOTE: *If both the originator address and domain are set, then MERCUR will verify both the alias and domain. This will provide administrators with more control over SPAMMING*

Reject incoming mail, if number of external recipients exceeds

It happens often that so-called *SPAMMER* use the mail server of other people to forward mail to a high number of recipients. In this case, an incoming message contains maybe hundreds of recipient addresses and the mailserver must create for each recipient an outgoing mail. To prevent this, you can specify a maximum number of external destination addresses. If this number will be exceeded, the message is rejected.

Info to administrator, if number of external recipients exceeds

This option works as described before. In this case, the administrator gets an info message. This enables you to recognize possible spam attacks.

Usage of Additional Options

Watchdog

The built-in *Watchdog* feature is used to check the MERCUR services at specific time intervals. If a service does respond, because it is not longer running, the Watchdog will initiate a restart for the appropriate service. The watchdog can be activated for the SMTP, POP3 and IMAP4 service only. The *CONTROL SERVICE* must be started from the local mail server.

Time range interval

Here you define the time range for the watchdog feature.

Options

Encrypt message files

This feature allows for messages stored on MERCUR to be encrypted. This feature is useful in preventing individuals with access to the mail server from accessing mail messages and reading them.

Save message encrypted

Every message will be stored encrypted so that it is not possible to read them with an editor. They can be read only by the used mail client.

Deny Telnet connections

MERCUR allows access to the mail server via *TELNET*. With TELNET an individual can have full access to all the MERCUR features. By setting the *DENY* button, TELNET access is no longer possible. A special detection algorithm allows administrators to switch over with the system is running. By default all file formats are detected automatically.

Deny VRFY

The SMTP *VRFY* command allows for mail address checking. As a security measure this feature should be set to *DENY*.

Firewall Settings

The register *Firewall* shows a list of all firewall settings with IP address, subnet mask and domain. You may sort them in an alphabetical order if you click on the field IP address, Subnet mask or Domain. The alphabetical order will be indicated by a small pointer left beside the field. Press the *Add* button to add a new firewall entry, the *Delete* button to delete a firewall entry or click the *Edit* button to change the settings of an existing firewall entry.

SMTP, POP3, IMAP4, configuration

Trough selecting the MERCUR services here the firewall settings will be shown. A *key* in front of an IP address means the access is granted. A *lock* in front of an IP address means the access is denied.

Edit Firewall

Permission

These flags are used to grant or deny the access to the selected service.

Originator address/domain

Select here, if an additional mail address/domain validation shall be performed or if the IP-address mask is valid for all mail domains. This option is used to limit access for mail addresses/domains to special IP-addresses or subnets.

All addresses/domains

The selected permission is valid for all mail addresses and domains from the local system.

Only domain

The selected permission is valid for the named local domain. Please insert a valid local domain name.

Only address

The selected permission is valid for the named local mail address. Please insert a valid local address.

Range of validity

Enter here the IP-address or subnet for this firewall entry. You can grant or deny the access to single addresses or whole address areas here.

Subnet-Mask

With the entry in this area you limit the range of an IP-Address area.

SMTP authentication required

Chose this option if you demand SMTP identification.

Notice: For user of a WIN NT/2000 user account no SMTP authentication is possible. You may avoid this problem if you add this users as well in MERCUR.

POP3 authentication required

Chose this option if you demand POP3 authentication. Then first POP3 authentication is required before mail is accepted.

Notice: For user of a WIN NT/2000 user account no POP3 authentication is possible. You may avoid this problem if you add this users as well in MERCUR.

Services

Select here the services for this firewall definition.

How can I close my open relay

The anti spamming and firewall options of MERCUR Messaging 2005 allow you to control relaying in different ways. The basic thing is to add the following entries to the SMTP firewall list:

- Add one entry to each subnet you have where the *No relaying* option is *DISABLED*
- Add one entry for the *rest of the world* where the *No relaying* option is *ENABLED*

Please make sure that the *world* entry is the last one in the list.

In this case:

- Users from inside of the local subnet can send emails to anybody
- Users from outside of the local subnet can send emails only to local email addresses
- Users which comes from outside of the local subnet can send emails to anybody *ONLY* if they using the authentication,

These settings required that users have to authenticate if they aren't in the local subnet. The mail client which should be use must support the *POP3 before SMTP* or *SMTP-Auth*. MERCUR Messaging 2005 supported the authentication only if the option *Use ESMTP* is enabled.

Example

Entry 1 (Allowed Subnet):
Permissions: Grant Access
Originator-Address/Domain: All Addresses/Domains
Range of Validity: IP-address area
 IP-address: 212.20.132.64
 Subnet-Mask: 255.255.255.192
Service: SMTP

Entry 2 (rest of the world):
Permissions: Grant Access
Originator-Address/Domain: All Addresses/Domains
Range of Validity: All IP-addresses
Service: SMTP, No relaying allowed

Exceptions of Addresses

Exceptions Dialog

MERCUR Messaging 2005 Version is able to support *BLACKLISTS* that deny access to the mail server. You can *DENY* access to your MERCUR Messaging 2005 by either ORIGINATOR ADDRESS or by ORIGINATOR HOST or IP ADDRESS. No mail from this addresses will be accepted.

To add an entry to the exceptions list simply enter the information in the ADDRESS MASK or the HOST/IP ADDRESS MASK and click on the *Add* button. It is also possible to import a list of email addresses or host/ip-addresses from a textfile. Use the button *Clear* to remove the corresponding list.

Delete Attachments

Because some type of virus or trojan cannot be detected you got the possibility to delete attachments from every message you like. As well you may store these attachments in a selected folder. Also you will predefine the setting of new auto responder.

Attachments

Delete Attachments from the Messages

MERCUR will monitor messages for attachments, and all attachments are automatically deleted. This also affects mail, which is send local. This option only is guilty for defined attachments in the list *Denied masks*. If the option *List contains allowed masks only* is selected, then the undefined attachments in the list *Allowed masks* will be deleted.

List contains allowed masks only

If this option is enabled then MERCUR will automatically delete all attachments which aren't defined in the list *Allowed masks*. This also affects mail, which is send local.

Delete Only If Larger Than

MERCUR will monitor all incoming messages for attachments and delete any attachment greater than the designated size.

Store Removed Attachments in a Folder

Administrators can select this option if they decide they want to have MERCUR automatically to store all attachments in a here chosen folder. In this way the attachments are still available. Please take note that MERCUR will not delete the stored attachments automatically.

Extension Mask

MERCUR will only monitor for attachments with specific extension names (**.exe, *.vbs, *.zip* etc.). This feature is very useful if you are using the FAX/PAGER options in MERCUR. Attachments sent with FAX/PAGER email messages will be excluded.

Exclude address mask for auto responders

Any mask added to the address mask will be exempt from all auto responders. All newly created auto responders will include this predefinition. You as well may change the setting of existing auto responders in the auto responder section. Here you define addresses, which will be excluded from all auto responder messages.

Example: mailer-daemon*

All addresses, with the string *mailer-daemon* at the begin will be excluded, e.g. *mailer-daemon@domain.com*.

Address mask

Here you may enter an address mask and add this scheme if you press the *Add* button.

Dialog Virus Control

The anti virus interface in MERCUR is able to interact with third party *command line* type ant-virus scanning software. The MERCUR interface allows the anti-virus scanner to manage and control every incoming mail based on the settings in both Mercur and the anti-virus application. Any infected email will be identified before it is processed and delivered. Infected files can either be stored in designated quarantine folder or MERCUR can be instructed to delete all infected email or attachments.

MERCUR's anti-virus interface is able to interact with any standard *command line* based ant-virus scanner that can send a return value back to MERCUR. It is crucial that a console application, e.g.: *Scan.exe from McAfee* be used so that it can send a return value to MERCUR only after the scanning procedure is completed.

Any anti-virus application that uses *On-Demand scanners* (e.g.: *Scan32.exe in McAfee*) is unsuitable for use with MERCUR. This type of anti-virus scanner produces a return value as soon as the scanning process begins, resulting in a false return value to the requesting application, before the actual scan is completed. Running the On-Demand feature through MERCUR may also cause data priority irregularities. These irregularities may eventually cause the SMTP service to crash or even slow down your entire system.

When using the MERCUR anti-virus interface feature the settings for the application parameters have to be accurate and match the actual required return values for the anti-virus application. The application must run in the *silent mode* and cannot make any user entries requests. The wrong parameter settings will cause the SMTP service to eventually crash or in a worse case scenario cause the entire system to crash frequently.

The MERCUR anti-virus status will be determined by the appropriate *return value* setting, (e.g.: *in McAfee the return value is 13*). The correct return value will notify the MERCUR SMTP service that a virus has been identified or that the message is clean. A wrong return value setting will cause the SMTP service to receive incorrect information, and that will allow infected email to be processed as clean email.

As a matter of a fact the problems caused by installing some anti virus packages on server versions of Windows NT/2000 are not functional problems. They have license reasons because some anti virus software distributors offer special server programs, which include also command line tools.

Enable Virus-Scan for MIME encoding messages

Here you may enter a third party anti-virus application, or the build-in interface of Norman Virus Control or the Symantec Anti Virus Scan Engine. In order for MERCUR to interact with an command line application you must select the entry *Custom command line scanner*. The correct setting of the *return value* is very important for a faultless function. The return value is written in the *description of your virus scanner*.

Scanner-Type

To activate the virus scan you have to choose a entry here. As default entries you will find the *Custom command line scanner*, *Symantec Anti Virus Scan Engine*, the *Norman Virus Control Engine* and other installed anti virus products which are detected by MERCUR, e.g. *F-Secure Anti Virus*.

If the entry *Norman Virus Control Engine* is selected the build-in interface of Norman Virus Control is be use for the virus identification for MIME encoding messages. Here you will also see additional information about the version of the Scanner Engine, the Signature-Date and Counter of the virus definitions files for Binary- and Macro-Viruses. If the Norman Scan engine is not installed you can't use this virus scanner.

If the entry *Symantec Anti Virus Scan Engine* is selected the build-in interface of Symantec is be use for the virus identification for MIME encoding messages. Here you have to enter the hostname/IP-address of the server where the Symantec Anti Virus Scan Engine is running. Enter also the Native Protocol Port which should be use. Here you will see the default port *7777* which are use by Symantec.

If Mercur has detected a installed anti virus product and you choose this entry than Mercur will provide you with the default settings of the corressponding command line scanner.

Use the entry **Custom command line scanner** to work with another third party application. In this situation you have to setup all settings manually.

To deactivate the virus scan in MERCUR select the entry *No virus scanner in use*.

Application

Select the designated path of the anti-virus application running on your system. This is usually an executable type file with an exe extension. Please make sure that you use the right application here. The application needs to run in silent mode and should not ask for user input. Wrong settings here can block the MERCUR services or cause crashes.

Execute hidden

Enable this option to disable the viewing of the Shell-window during the scan process.

Arguments

Here you may enter special parameters of your virus scanner. These parameters normally activate/deactivate acoustic signals and/or screen messages. The application must run in silent mode and cannot make any user entry requests. The wrong parameter setting eventually cause the SMTP service to crash or in a worse case scenario cause the entire system to crash frequently.

Return codes

Here you have to enter the return codes of your command line virus scanner. The return code of your virus scanner *is notated in it's description*. If you got problems here please connect the *publisher* of the virus scanner.

Activity on Virus Alert

Activity on Virus Alert

You can setup some parameters on how to handle infected email messages.

- **Delete Email**
Infected messages and attachments will be deleted without any notification.
- **Delete infected attachments**
Email message is delivered without the infected attachment. The attachment is either deleted or stored in a special folder.
- **Store infected attachments in the following folder**
All infected attachments can be stored in a designated folder. An administrator can delete these messages at a later date. In addition to handling infected email messages, you can send out a message regarding the results of the virus scan.
- **Info to Administrator**
MERCUR will notify the administrator every time an infected message is identified.
- **Info to Originator**
MERCUR will notify by email the originator of the message that the message sent was infected with a virus.
- **Info to Recipient**
MERCUR will notify by email the recipient of the message that the message received was identified as being infected with a virus.
- **Info to local recipients only**
MERCUR will notify only local recipients on the MERCUR system that a message sent to the recipient was identified as message infected by a virus.
- **Remark in original message**
MERCUR will add an annotation to the original message identifying that the message being viewed was identified as being infected with a virus.

Norman Internet Update

These options can only be use if an *MERCUR Virus Control license* was entered. These options are not useful if a full registered product of Norman is installed, because the signature file update will be process by the Norman application. Here you can setup the process on how to handle the Norman Internet Update.

Manually only

Enable this option if no automatically Norman Internet Update should be used.

Automatically every

Here you can setup some parameters on how to handle the automatically Norman Internet Update.

Update now !

Click this button to start the Norman Internet Update.

Examples of Command Line Scanners

The anti virus interface in MERCUR is able to interact with third party command line type anti virus scanning software. The MERCUR interface allows the anti virus scanner to manage and control every incoming mail based on the settings in both MERCUR and the anti-virus application. Any infected email will be identified before it is processed and delivered. Infected files can either be stored in designated quarantine folder or MERCUR can be instructed to delete all infected email or attachments.

MERCUR's anti virus interface is able to interact with any standard command line based anti virus scanner that can send a return value back to MERCUR. It is crucial that a console application (e.g.: *Scan.exe from McAfee*) be used so that it can send a return value to MERCUR only after the scanning procedure is completed.

Any anti-virus application that uses On Demand scanners (e.g.: *Scan32.exe in McAfee*) is unsuitable for use with MERCUR. This type of anti virus scanner produces a return value as soon as the scanning process begins, resulting in a false return value to the requesting application, before the actual scan is completed. Running the On Demand feature through MERCUR may also cause data priority irregularities. These irregularities may eventually cause the SMTP service to crash or even slow down your entire system.

When using the MERCUR anti virus interface feature the settings for the application parameters have to be accurate and match the actual required return values for the anti-virus application. The application must run in the *silent mode* and cannot make any user entry requests. The wrong parameter setting eventually cause the SMTP service to crash or in a worse case scenario cause the entire system to crash frequently.

The MERCUR anti virus status will be determined by the appropriate return value setting, (e.g.: *in McAfee the return value is 13*). The correct return value will notify the MERCUR SMTP service that a virus has been identified or that the message is clean. A wrong return value setting will cause the SMTP service to receive incorrect information, and that will allow infected email to be processed as clean email.

NOTE: We can't recommend to use command line scanner from Norton Antivirus (Symantec), because this is prohibited by Symantec.

Norman Virus Control

Scan application: NVCC.EXE
 Parameter: "<%%filename%%>" /Q /N /BS- /C /CP
 Return value: 1

McAfee Virus Scan

Scan application: SCAN.EXE
 Parameter: "<%%filename%%>" /NOBEEP /FAM /NOMEM /SILENT /UNZIP
 Return value: 13

F-Secure Anti-Virus

Scan application: FSAV.EXE
 Parameter: "<%%filename%%>" /ARCHIVE /NOBOOT /SILENT
 Return value: 23

SOPHOS

Scan application: SAV32CLI.EXE
 Parameter: "<%%filename%%>" -nc -nb -archive -mime
 Return value: 3

Dialog WebMail-Client (*Enterprise Edition only*)

The dialog [Webmail](#) provides you to setup all specific settings of the integrated Webmail. Here you are able to change the port used by the Webmail service. Additionally you have to define which SMTP service should be used for all outgoing messages of Webmail. For the usage of Webmail a OLE-DB-Database is required. Webmail doesn't support ODBC databases.

Server-Settings

Webmail port

This is the TCP/IP port on which Webmail should be run. The default port is *1080*.

Clear trash after XX days

Enter here a value after how many days the messages in the trash should be deleted automatically. The default value is after **5** days.

Logout user after XX minutes idle time

Define here a time range after a user session should be cancelled by the system. If the system has cancelled a user session a new login is required !

SMTP-Server

Use local MERCUR SMTP Service

Enable this option, if all outgoing messages from Webmail should be delivered to the local MERCUR SMTP service.

Use the following SMTP Server

Provides you to define another SMTP service where the outgoing messages should be delivered.

Hostname

Enter here the hostname or the IP-address of the other SMTP server.

Port

Enter here the SMTP port of the other SMTP server. The default value is *25*.

Database

For the usage of Webmail a OLE-DB-Database is required. Webmail doesn't support ODBC databases.

Provider

Register an OLE DB Database source, or select a suitable OLE DB Database source by selecting from a list of providers.

Database

Here you will see the selected OLE database or enables you to enter an OLE database that Webmail can use for storing all Webmail data, e.g. contacts and appointments.

Options

Provides you to enter required options for using the OLE-DB-Database.

Login name and Password

Enter the login name and password, which should be used by Webmail to logon into the database.

Dialog Settings

Server

Hostname

A name that identifies the MERCUR Messaging 2005 when he connects to other hosts, e.g. mail.yourdomainname.com.

Domain

Select a domain name that identifies this machine. Usually the primary domain of the machine is used.

Attention: This means the internet domain name not the Windows NT domain name.

Name server

The name of your DNS Server. The value is required if you want to use the DNS-Lookup option. You can enter several name server values, separated by semicolon.

Administrator Alias

The alias of the administrator, which normally administrates the system e.g.: postmaster. This administrator alias, will be generally used for all automatically generated administrator mail e.g.: undeliverable mail.

Administrator mailbox

The mailbox in which the messages of the MERCUR administrator get stored.

Protocol

Here you define which protocol the SMPT Service should use.

Use 'ESMTP'

Set this option to activate the usage of ESMTP.

Max. message size

This feature allows administrators to control the message size of mail users are allowed to send. Mail, which exceeds this size, will be rejected. This option is only available if *Use 'ESMTP'* is activated.

Send messages with ESMTP

If this button is set, MERCUR will try to use ESMTP to forward outgoing mails. If the destination host does not support this, the simple SMTP will be used.

Send message size

If sending mails per ESMTP MERCUR will send the size of a message to the receiving mail server.

Supported Authentication methods

Here you are able to select which authentication methods should be supported from MERCUR Messaging 2005. This option is only available if *Use ESMTP* is activated.

Adapter

Use this option to choose the adapter (IP-addresses), which should be used by the MERCUR services. This option is only available when the computer uses more than one IP address. If *Use any adapter* is selected, all adapters will be used.

Exchange Settings

Use this page to setup in which way MERCUR should update the outgoing mails. If no option is selected, no mail will be forwarded.

Forwarding

Use DNS-Lookup

If you activate this option, MERCUR determines the address of the destination host automatically. You must define a name server on the system page of this configuration utility to use this function. For all outgoing messages, MERCUR contacts this name server and uses a *DNS query* (Domain-Name-System) to get the IP-address of the corresponding mail server. In this way, the outgoing messages can reach directly their destination. If you do not use this option, you must set the name of an exchange-host. Otherwise, the mail exchange fails.

Use IP cache size...

The IP cache feature stores MX record in a cache file on the local system. Addresses often required are available without further query. As a result, an enormous rate advantage can be achieved during the effort of Dial-Up connection, especially if the name service is not available on the local system and the connection must be opened for MX lookup.

Clear cache

This button gives you the possibility to empty the IP-cache.

If no MX record available

Sometimes the query for DNS -information fails and the required MX-Entries are not available. You can specify here, what kind of additional DNS queries should be performed.

Use domain as hostname

In some cases the hostname is the same as the domain name. If this option is set, MERCUR will use the domain name as hostname and tries to deliver the mail in this way.

Search sub domains

In large networks, the mail domains are often sub domains of superior domains. Choose this option, if MERCUR should search for sub domains inside the domain name.

Example: If there is no MX entry available for the domain subdomain1.subdomain2.domain.com, MERCUR will also check the domain names subdomain2.domain.com and domain.com

Forward to Exchange-Host

In this field, you can specify the name of a fundamental exchange server. This option is very important, if you got no name server or if you want to handle the outgoing mail from a central point. If the DNS lookup option is set additionally and the corresponding mailserv gives no response, MERCUR tries to connect this exchange server. You can enter several entries, separated by semicolon.

Server requires a SMTP authentication

If your internet provider requires SMTP authentication you can activate this option here. You must specify your user name and password required by the remote host. Then by forwarding messages to an exchange server first the SMTP authentication will be send. This option is only available when an exchange host is used for sending messages. This feature uses the external SMTP port.

Server requires a POP3 authentication

If your internet provider requires POP3 authentication (*POP3 before SMTP*) you can activate this option here. You must specify the user name and password required by the remote host. This option is only available when an exchange host is used for sending messages. This feature uses the external POP3 port.

Login name

Here you have to enter your login name for the SMTP-/POP3 authentication.

Password

Here you have to enter your password for the SMTP-/POP3 authentication.

Update out basket

Here you see all scheduling entries. Interval, time range weekdays and priority will be shown.

Add a schedule entry

Press the Add button to add a new schedule entry.

Edit a schedule entry

Setup here the time intervals to update the outgoing mails. The scheduling feature of MERCUR allows detailed time patterns for each priority level separately.

Delete a schedule entry

Use this option to delete a selected scheduling entry.

Update Outbasket Settings

Setup here the time intervals to update the outgoing mails. The scheduling feature of MERCUR allows detailed time patterns for each priority level separately. For example updating the out basket, daily between 8:00 and 18:00 every 15 minutes, at night every 2 hours and at the weekend only twice a day.

Weekdays

The schedule task follows the pre-selected weekdays. If no settings have been set for weekdays, then the out basket service will be turned off.

Frequency

Immediately, when the mail arrives

Choose this option to forward incoming messages immediately. If you use Dial-Up connection, it will be opened immediately.

If the out basket contains more than ... messages

This option forwards to outgoing mail when a special number of messages are waiting in the out basket.

Once at...

Use this option to specify an exact time of day to update outgoing mail. This value is in a 24 hour format.

Periodical every...

Enter here the time interval for a periodical update. This value must be in minutes or hours. You can also define if this task should run the whole day or only for a special period. This value is also in a 24 hour format.

Priority

Depending on the volume of traffic on the mail server, administrators can determine how messages are to be delivered to their destination. MERCUR will attempt to deliver all messages in the out basket immediately. However if mailing lists have a priority then all mailing list messages get delivered first.

Connect only if outgoing mail is waiting

If this option is selected, the service opens the connection only when the out basket contains messages to forward.

Attention: Normally, this option is ALWAYS selected. You can unselect it when you get your mail via SMTP from your ISP and your ISP expects the connection is established by from your side.

Send ETRN request for node name...

When this option is activated it is necessary to activate the option Use ESMTP protocol in page Exchange. Use this option if you want to update a waiting loop on the internet service provider with the ETRN command. This proceed is used to tell the mail server from the other side that he should send all new messages with SMTP now. Therefore you must enter the name of the waiting loop (node name).

Attention: While the node name are not send by using encoding you have not 100% security by this proceed.

To exchange host

Send the ETRN-request to the exchange host that is defined in the point Forward to Exchange Host.

To host

Send the ETRN- request to the host that is defined here.

Delivery Settings Dialog

Undeliverable Mail

This section defines the handling of undeliverable messages. You can schedule a time interval for attempting to deliver a message. After this time period has expired messages will be treated as *UNDELIVERABLE*.

Send info to originator

If this option is set, the originator will receive an info message when the mail was undeliverable. The message will be send after the time range you set in the field *Mail is undeliverable after*.

Return message to originator

If this option is set, the originator will receive the original mail back with info than it was undeliverable. The message will be send after the time range you set in the field *Mail is undeliverable after*.

Send info to administrator

If this option is set, the administrator will receive a message if the mail was undeliverable. The message will be send after the time range you set in the field *Mail is undeliverable after*.

Attach original message

With this option the original message will be attached to the administrators info message.

Info to originator, during delivery problems after

If you got problems delivering messages you may send here a message to the originator that his message was not delivered till now. It is still possible that the message will be delivered because it is not treated as undeliverable mail. You should always secure that this time range is set closer than the time range for undeliverable mail.

Mail is undeliverable after

Here you may enter the time after the mail should be treated as undeliverable.

Keyword for Priority

Here you define keywords for your used mail clients. They will be used to indentificate the priority of the mail send. The mail with the higher priority will be send on first.

For example a header from Outlook 2000:

```
-----
Reply-To: <test@domain.com>
From: "test" <test@domain.com>
To: <test@domain.com>
Subject:
Date: Tue, 8 Aug 2000 14:49:33 +0200
Message-ID: <000101c00137$640bae10$108d1bd4@domain.com>
MIME-Version: 1.0
Content-Type: text/plain;
    charset="iso-8859-1"
Content-Transfer-Encoding: 7bit
X-Priority: 1 (Highest)
X-MSMail-Priority: High
X-Mailer: Microsoft Outlook CWS, Build 9.0.2416 (9.0.2910.0)
Importance: High
X-MimeOLE: Produced By Microsoft MimeOLE V5.00.2314.1300
-----
```

In this header you can find two entries with the word priority: *X-Priority: 1 (Highest)* and *X-MSMail-Priority: High*. Add these two entries to the priority keywords section. Now MERCUR will be able recognize different priorities.

Keyword

Here you are able to enter new keywords.

Connection Settings Dialog

Connection

Choose the network connection, when the connection to the Internet is accessible with your local network. This requires a static connection to your Internet service provider (*e.g. using a router*). If you do not have a static connection, choose the Remote Access profile, to be used for connecting to the Internet. MERCUR will open and close this profile automatically if required. As well enter maximum idle time interval you want the connection to remain open.

Ports

This allows you to specify the port numbers, used by the MERCUR services. The port can be changed separately for both internal and external use. This is useful when the service connects to a proxy server. Normally, there is no need to change any settings, but because the ports for SMTP (Port 25), POP3 (Port 110), IMAP4 (Port 143) and DNS (Port 53) are predefined in MERCUR, some settings may require modification.

Maximum number of threads for external SMTP connections

This feature allows administrators to control the number of multiple SMTP connections that are open. Depending on the volume of traffic and the machine resources (CPU's, memory, connection to the Internet), administrators may want to increase the number of simultaneous SMTP connections that MERCUR can use.

CAUTION: THE MORE SMTP THREADS ACCESSED BY MERCUR, THE MORE SYSTEM RESOURCES REQUIRED. IF YOUR SERVER RUNS LOW ON RESOURCES, YOUR SYSTEM WILL CRASH.

Database Settings Dialog (Enterprise edition only)

The administration of user data and event logs in databases offers an open system and the possibility of purposeful analysis to the administrator from use and costs. By the usage of powerful database systems, a fast access to a large number of user data is guaranteed.

User data

Enter the path where MERCUR should store the user data.

MERCUR default format

Select this option if you like to store the user data in a file on your hard disk. The data will normally stored in the file MERCUR\Config.

In ODBC database

Use this option if MERCUR should store the user data in an ODBC data source. Click on the button near the input field to choose from a list with all available system data sources. You can also use this to check or create the structure of the data source. In this case, MERCUR will create all required tables automatically. You can also specify the login name and password required for database login.

Attention: Please note, that only system data sources are usable. User data sources are NOT supported and therefore not available.

Event-Logs

Enter the path where MERCUR should store the event logs.

MERCUR default format

If this option is selected, MERCUR will store all SMTP, POP3 and IMAP4 events as text file on the hard disk. The data will be stored in the file MERCUR\Log.

In ODBC database

Enter here the name of the ODBC data source, which should be used for event logging. Click on the button near the input field to choose from a list with all available system data sources. You can also use this to check or create the structure of the data source. In this case, MERCUR will create all required tables automatically. You must also specify the login name and password, as well as a table name needed for database login. MERCUR will store all events of SMTP, POP3 and IMAP4 in this table.

Attention: Please note, that only system data sources (ODBC-data sources) are usable. User data sources are NOT supported and therefore not available.

Enable ODBC error logging

This option enables an ODBC debug log feature. If the option is enabled, an additional file with name MCRODBC:TXT is created in the MERCUR log directory. The file is used to log all kinds of ODBC error messages. It is not used for regular ODBC command logging. So, you should use this option only if you have serious database problems.

Statistic-Information

Here you will enter the ODBC data source, which should be used to store the statistic information. If you want to use the register *Statistic* you have to activate this option.

In ODBC-database

Choose this option to store the statistic data in an ODBC file of your decision. Click on the button near the input field to choose from a list with all available system data sources. You can also use this to check or create the structure of the data source. In this case, MERCUR will create all required tables automatically. You must also specify the login name and password.

Attention: Please note, that only system data sources are usable. User data sources are NOT supported and therefore not available.

Default Dialog

You can define here, how incoming messages for unknown user addresses should be handled. It is also possible to search for unknown aliases in other local domains or to forward them directly to another mail address.

Unknown users

Search alias in other local domains

If this checkbox is activated, MERCUR tries to determine the right destination address in all other local domains. If the destination of a mail message is for a local mail address, *user@domain1.com*, but the correct address is *user@domain2.com*, then MERCUR will deliver the message to the correct address.

Reject mail

If this option is set, all incoming mails for unknown user will be rejected.

Send info to administrator

This option will generate messages and send it to the administrator if a message has been rejected.

Forward to

If you even want to receive all mails from unknown addresses, you can specify a special destination address/domain or host to route these mails. If the *Original domain as host* option is selected, the domain name of the original address is used as hostname.

Send info to originator

This feature will send a message to the originator of the message that the mail address was forwarded to another mail address or domain.

Advanced options

Generate 'Reply-To:' entry if not exist

If this option is checked, MERCUR will check the *Reply-To:-* field of the mail header and add it if it does not exist.

Confirmation of receipt, at demand

This option sends a message to the originator of the mail message confirming that the mail message was delivered.

Info to administrator, if free disk space less than

This option warns administrators if their hard drive is running low on storage. Administrators can pre-set the minimum low hard drive space value.

Expiration time for POP3 authentication

The here entered time range is the period in which MERCUR stores a POP3 authentication so that no new authentication is required. Within this time range MERCUR will accept and work up all incoming SMTP messages. You have to enter the time range in minutes.

Settings Dialog

Here you set the adjustments for backups, time outs and files in which the data should be stored.

E-Mail Backup

This option allows you to set a directory for E-Mail Backup. So, a copy of all received and/or sent messages will be stored there. The directories for received and sent messages can be set separately. The backup system will create a subdirectory for each domain inside the backup directories.

***Please note that:** The stored copies are not automatically deleted by MERCUR. So, you need to take care that you have enough free disk space to store the backup copies*

Max. timeouts...

Time ranges direct all network activity with workstations and remote server. Exceeding this time ranges will be treated as mistake. Exceeding the time ranges has many possibilities. The connection may be slow or it is not possible to work up the commission. So changing the time settings has to be done with care.

...for client connections

This sets the maximum time client software has when accessing MERCUR. Some mail programs allow a connection for retrieving mail to remain open for long periods. In order to prevent the mail server from having an open feed to the client, if all messages have been sent or collected MERCUR will disconnect the client.

...in command mode

Access MERCUR using the *COMMAND* mode can allow a connection to remain open. If there is not activity with that connection MERCUR will disconnect.

...opening connections

When MERCUR opens a connection to a remote server or the Internet, if the connections is idle for more than the predetermined time, MERCUR is terminate the connections. This is especially useful for dial-up accounts. Here you should make sure the predetermined time is enough to ensure a good connection because dial-up accounts are often slowly networks.

...for name server requests

When a name server request is made, no connection over long time periods will be made. Single requests are made. The time range indicates how long to wait of responds from a name server.

Folders

These directories are used by MERCUR to store the required files on your system. You can enter a path or choose a path from a directory list.

Temporary files

This directory is used by MERCUR to store the temp files. (e.g.: C:\Programs\Atrium Software\Mercur\temp)

Mail folder

In this directory, MERCUR creates the subfolders to manage the user mailboxes. They normally will be stored in the mail file (e.g.: C:\Programs\Atrium Software\Mercur\Mail)

HTML-Files

This directory contains the HTML files used for configuration via web browser. They normally will be stored in the HTML file (e.g.: C:\Programs\Atrium Software\Mercur\Html)

Event-Logs

This directory contains all log files for SMTP, POP3 and IMAP4. They normally will be stored in the Log file (e.g.:C:\Programs\Atrium Software\Mercur\Log)

Dialog Statistic (Enterprise edition only)

The MERCUR Messaging 2005 enables the display of detailed statistics. To use this feature the option *In ODBC database* must have been activated some time ago. This setting you may change in the dialog *Settings* in the register *Database*. The MERCUR Messaging 2005 stores in general statistic information for the SMTP and Fax/Pager-Gateway service for local mailboxes.

Independent from shown statistics you may look up or print statistic reports that you may define. More information is available in the chapter *Display a Statistic Report*.

To display statistic reports choose a time range or define one. Then you have to choose the columns from which you like to see the statistic information. Available are date, time, event r/s, originator address, recipient address, domain, user, size and duration. You also have the possibility to save the statistic in a text file and export this files to other statistic programs.

Display Statistics (Enterprise edition only)

Time range

Here you will define the time range of the statistic report.

Date:

This shows the days of the selected time range. If the day in both boxes is identical the time range is the selected day.

Total time range

The time range from the first day you activated this option till today.

Display

You may restrict the statistic to certain domains, user, originators or recipients.

Domain

Restricts the statistic to the chosen domain. You can choose between local domains or all domains.

User

Restricts the statistic to the chosen user.

Originator

Restricts the statistic to the here entered originators.

Recipient

Restricts the statistic to the here entered recipients.

All mail

Choose this option if the statistic should include sent and received mail.

Only sent mail

Choose this option if the statistic should include only sent mail.

Only received mail

Choose this option if the statistic should include only received mail.

Number of messages

Shows the total number of all mail in the statistic.

Total KBytes

Shows the total kbytes of all mail in the statistic.

Display a Statistic Report (Enterprise edition only)**Statistic display****Date**

Shows the date when the entry was made, e.g.: *2001-07-15*.

Time

Shows the time when the entry was made, e.g.: *12:56:56*.

Event R/S

Shows the event *R/S* of the process. *R* means received, *S* means sent.

Originator Address

Shows the originator address from which the mail was send.

Recipient Address

Shows the recipient address to which the mail was send.

Domain

Shows the domain, which was used during the process.

User account

Shows the user account, which was used during the process.

Volume (Bytes)

Shows the total data volume of this process.

Duration (Sec.)

Indicates the complete duration of this process.

Number of messages

Shows the total number of all selected mail.

Total KBytes

Shows the complete size of all selected mail in kbytes.

Dialog License

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

Please use the command *Enter license key* out of the menu Help in MERCUR Messaging 2005 Lite Edition to enter your license key.

This dialog shows a list of all licenses you own. You have as well the symbol bar items *Add* and *Delete*. With these you may add and delete licenses. If you press the *Add* button you have to enter your new license number.

The MERCUR Messaging 2005 administrates for every user a separate mailbox in which the mail will be stored. Several users may share an account or a user may have several accounts. Only with the unlimited user mailbox license owner of a Windows NT/2000 user account may be imported in domains as local users.

MERCUR Messaging 2005

Lite Edition (without Premium Hotline/Support)

Program version of maximum 1 Domain and maximum 15 user mailboxes

MERCUR Messaging 2005

Standard Edition (without Premium Hotline/Support)

Program version of maximum 3 Domains and unlimited user mailboxes.

Maximum 3 Static Routes.

Including iNetQuery 2005 (Internet/Network Analyse Tool)

MERCUR Messaging 2005

Enterprise Edition (without Premium Hotline/Support)

Program version of unlimited Domains and unlimited user mailboxes.

Including integrated Webmail-Client.

Including ODBC-Connectivity.

Including Fax-/Pager-Gateway.

Including Statistic functionality

Including Windows NT/2000 User accounts.

Including iNetQuery 2005 (Internet/Network Analyse Tool)

Each Edition are also available with included 12 Month Premium Hotline Support Contract .

License-information

Here you will see your basic license and all your upgrade licenses.

MERCUR Remote Configuration

This feature is not available in the Lite Edition of MERCUR Messaging 2005.

The MERCUR control service contains a *HTTP interface*. This allows administrators to edit the MERCUR configuration settings using a regular Browser, like Microsoft Internet Explorer 5 or Netscape Communicator 4.7 or higher.

You can open a connection with your browser to your MERCUR configuration service when you enter the host name or IP address of your mail server, followed by the port number for the configuration service, e.g. *32000*.

Example: `http://Domain.com:32000`
`http://mail.Domain.com:32000`
`http://IP address:32000`

If your MERCUR control service uses the regular HTTP port (*80*), you do not need to enter the port number after the host name.

Example: `http://mail.domain.com`

Login

If a connection is established, you will get a login dialog box. You must enter a username and password configured in the MERCUR user manager. The username must be your complete email address. Please note that the user accessing any administrator tools must have administrator permissions. Otherwise the login will fail.

... all domains

If this button is activated the user may configure the MERCUR Messaging 2005 from a remote computer. The login has to be with your complete email address as username and your password.

... only this domain

If this button is activated the user may configure only the domain he belongs to. The login has to be with your complete email address as username and your password.

Dialogs

The HTTP configuration tools are HTML documents and the contents correspond to the MERCUR configuration utility contents. However due to the limitations with HTML scripting, the HTML version looks different than the standard MERCUR configuration and user manager utilities.

MERCUR Tool MCRSEND

MCRSEND.EXE is a simple application to forward messages. You may attach files then the ISO-8859-1 BASE 64 encoding is used. You can also use the command line tool MCRSEND.

Usage of dialog window

The MCRSEND utility can be launched by using the windows explorer and under the MERCUR directory double clicking on the MCRSEND icon. You can also use the command line feature and enter MCRSEND. The following window will be displayed.

Settings

First you have to configure the MCRSEND utility with the following settings for a connection to open.

Delivery

Forward to SMTP Server

Enable this option, if the messages send by MCRSEND should be deliver to a specially SMTP server. Enter here the hostname or IP address of your SMTP server. The port field must contain the port number used by your SMTP server to accept messages. If the SMTP server required a SMTP authentication please enter here the login data and enable the option *Server requires SMTP login*.

Hostname

Enter here the hostname or the IP-address of the remote SMTP server, e.g. *mail.atrium-software.com* or *145.253.96.128*.

Port

The SMTP port of the remote SMTP server which should be use. As default you will find the SMTP port *25*.

Server requires SMTP login

Enable this option, if the remote SMTP server required a SMTP authentication. Enter the login data which should be use for a required authentication on the remote SMTP server.

Login name

The login name which should be use for the logon into the remote SMTP server.

Password

The password which should be use for the logon into the remote SMTP server.

Forward directly using DNS

If you enable this option, MCRSEND determines the address of the destination host automatically. In order for this feature to work, you must define a name server. MCRSEND contacts this name server and uses a *DNS query* (Domain-Name-System) to get the IP-address for the corresponding mail server. This way, all messages send with MCRSEND can reach their destination directly. If you do not use this option, you must use the option *Forward to SMTP server*, otherwise mail delivery will fail.

Name server

Enter here the hostname or the IP-address of the name server which should be used for the DNS-queries, e.g. *ns.atrium-software.com*.

Options

Keep application open

Normally the application MCRSEND will be automatically closed after successfully delivery of a message. Enable this option if you would like to close the MCRSEND manually.

Write event log

Enable this option and enter a log path where MCRSEND should store a log file. Use the [Select](#) button to select a directory.

Recipient information**From**

Insert the originator email address.

To

Insert the recipients email address. If you use more than one recipient then each recipient must be separated by an empty space.

Cc

Insert the recipient's email address that will receive the carbon copy. If you use more than one recipient then each recipient must be separated by an empty space.

Subject

Insert a brief description identifying the topic for this message.

Message Text

Here you can insert your message text.

Attachments**Add File/Remove File**

Use the [Add](#) button if you want add an attachment to the message. When an attachment is added, an icon will appear. You can delete an attachment by using the [Remove](#) button.

Help

Displays a help screen.

Usage as command line application

You can also use the command line tool MCRSEND. The following parameters are available. The parameters must be separated by a blank

Options:

- h** Name or address of the SMTP server
- n** Name or address of the DNS server
- p** The SMTP-Port (Default is 25)
- f** Originator address (From)
- t** Recipient addresses (To); separate by empty space
- w** Carbon Copy addresses (Cc); separate by empty space
- s** Subject
- a** Attachment files (separate by empty space and with full path)
- l** Creates a log file (no additional information required)
- ?** Shows a help screen

If no **-t** option is used, then the header of the message file must contain all recipient addresses.
If **-h** (Forward to SMTP Server) option is not given, [Forward directly using DNS](#) will be used.

MERCUR Tool MCRPASS

The **MCRPASS** is a little utility to change user passwords. When you create an executable for this program you can change the user passwords via email. You access MCRPASS by using the window based dialog box or by using the command line with the correct parameters.

Dialog

Execute MCRPASS in the MERCUR path by double clicking from your windows explorer or launch the program on the command line by using MCRPASS.

Options

First you have to configure the MCRPASS settings option.

Server

Insert the IP address or host name for the server that MERCUR is installed.

Port

Insert the port number that the password service is using (standard is *106*). If you are not sure which port setting is being used, then go to the *Connection* tab in the dialog *Settings* in the MERCUR configuration panel, the setting must be identical.

Change POP3 keyword

Username

The user name belonging to user you want to change password.

Old password

Insert the old password.

New password

Insert the new password.

Confirm Password

Insert the new password again, for password confirmation.

Change/Cancel

Use the *Change* button to apply the changes to MERCUR. The *Cancel* button closes the MCRPASS program window and changes are not applied to MERCUR.

From command line

You can use the command line tool MCRPASS₂ to change the user password. Call the program with the login name, the old password and the new password as parameter. The parameters must be separated by a blank.

These parameters are available:

-h	The IP address from the server
-p	The port (Standard is 106)
-m	Disabled the displaying of the program message
-?	Shows a help screen

The parameters must be separated by a blank here indicated by the **#**.

Example: MCRPASS -h 200.28.135.23#-p 106

After the parameter you have to enter the username then the old password and then the new one. The confirmation is not required. The parameters must be separated by a blank.

The following examples will demonstrate two MCRPASS command lines. Required blanks are indicated by the #.

MCRPASS -h 200.28.135.23#-p 106#demouser#old#new#[new]

MCRPASS -m#-h200.28.135.23#-p106#demouser#old#new#[new]

MERCUR Tool HOLIDAY

HOLIDAY is a program that generates an Auto-Responder. For example, when you are away from your computer and you want to send an automatic reply message to the originator of an incoming email. You can add, remove or edit an Auto-Responder message, but before you can activate this auto responder, you must create an executable in Mercur. The address can be for e.g. *holiday@domain.com*. Your Holiday executable can be activated or deactivated via email.

Activate Holiday via E-Mail

1. Create an executable with the address e.g. *holiday@domain.com*.
2. Write an Auto Responder text with e.g. *Notepad* and save it
3. Send a message to the holiday address and add the Auto Responder text as an attachment.

Deactivate Holiday via E-Mail

Send a message to the holiday address without an attachment.

Holiday at command line

You can also use the command line tool Holiday. The parameters must be separated by a blank.

Usage

Holiday <account> <file name> (-b<yymmdd>) (-e<yymmdd>) (-d) [-n<Name>] (-?)

- <account> The account for that the Auto-Responder should be used(e.g. demouser@domain.de).
- <File name> The file name with the Auto-Responder text.
- b<yymmdd> The specify date from which the Auto-Responder works. (e.g. 001015 equal 15.10.00).
- e<yymmdd> The specify date of the end that the Auto-Responder works (e.g. 001030 equal 30.10.00).
- d Delete this responder automatically after its expiration time.
- n<Name> Name of the Auto-Responder (Optional).
- ? Shows a help screen.

Deactivate the Holiday Auto-Responder by sending a message without text or without an attachment.

Event Log Dialog

The MERCUR Messaging 2005 may protocol all action during he is activated. You are able to decide which actions are logged. So errors and problems are easier to locate and even easier to understand. As well all the data transfer may be listed. All the event logs created from MERCUR will be stored in the MERCUR log file. If you open a log it is shown in the Notepad. Here you may copy, save it or save only selected parts of it.

Options

Here you set the configuration of your event logs and how long you want to store them. They will be deleted automatically after expiration of the time range of your settings.

Logging level

Here you set the main options of your event logs.

- no logging
no logs are made
- error level
only errors will be logged
- Warning level
additional to the errors warnings will be logged
- information level
additionally logins and logouts from user as well as forwarding mail and updating the out basket will be logged
- Debug level
login of all SMTP, POP3, IMAP4 commands and modem commands without the sent message. This setting is most likely because support requests with this logging maybe analyzed easier and so we may proceed them faster.
- extended debug level
logging of all SMTP, POP3, IMAP4 commands and modem commands with the send message text.

Delete logs older days

Enter the time duration for MERCUR to delete old log files.

Support Dialog

Use this Dialog to create a detailed support question. In the section parameter you can select the required settings and event logs which will be attached to the support mail. These parameters will be needed to analyze your problems and help you as fast as possible. You may send your message immediately if you press the button send or as well you may save your message if you press the save button.

Required parameter

Choose all parts, which are affected with the problem from the setting: domain, user, mailing list, auto responder, executables, remote mail accounts, static routes and options. All your event logs are also available. Please enter as well the time range of the attached event log.

E Mail Address

Please control the following entries. The email address is support@atrium-software.com. Please enter the email address on which we should respond your question.

Problem description

Please try to explain the problem here and as well if possible your affected settings. A detailed description will help us to precede your question faster and without further query.