



The GMS Administrator's Guide

Fourth Edition

Gordano Ltd

The GMS Administrator's Guide

Copyright © Gordano Ltd, 1995-2016. All rights reserved. Printed in the United Kingdom.

Published by Gordano Ltd, Unit 1, Yeo Bank Business Park, Kenn Road, Kenn, Clevedon, Somerset, UK, BS21 6UW

Printing History:

Oct 2002 First Edition

May 2003 Second Edition

May 2015 Third Edition

June 2016 Fourth Edition

ISBN

GMS, Gordano, Gordano Ltd and their logos are trademarks of Gordano Ltd.

Many of the designations used by manufacturers and sellers to distribute their products are claimed as trademarks. Where those designations appear in this book, and Gordano Ltd was aware of a trademark claim, the designations have been printed in capitals or initial capitals

Written by Brian Dorricott, John Stanners, Dean Fenton, Jason Hall and Dean Packer.

Copyright © Gordano Ltd, 1995-2016

GMS

WARNING: YOU SHOULD CAREFULLY READ THE LICENCE AGREEMENT PROVIDED WITH THIS MANUAL BEFORE USING THIS SOFTWARE PACKAGE. INSTALLING THE SOFTWARE ONTO YOUR COMPUTER INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT WISH TO ACCEPT ALL OF THESE TERMS, YOU SHOULD STOP INSTALLING THIS SOFTWARE NOW AND DESTROY ALL COPIES OF THE SOFTWARE AND ALL MANUALS AND OTHER DOCUMENTS SUPPLIED WITH IT.

NTMail is a registered trademark of Gordano Ltd.

The Gordano Logo is a registered trademark of Gordano Ltd.

Juce is a registered trademark of Gordano Ltd.

NT is a registered trademark of Northern Telecom Ltd.

Windows NT is a trademark of Microsoft Corporation in the USA and other countries.

All other trademarks are acknowledged.

Patents

Gordano owns a number of patents on its software as listed below:

Autoport

Gordano's "Autoport" technology is patented in the United Kingdom under patent number GB2391649.

A patent application has been filed in the United States and is pending approval.

Maintaining software and data (Automatic Updates)

Gordano's "Maintaining software and data" technology is patented in the United Kingdom under patent number GB2374163.

A patent application has been filed in the United States and is pending approval.

Anti-spam filter (Sender Verification)

Gordano's "Anti-spam Filter" technology is patented in the United Kingdom under patent number GB2385965 and in the United States under patent number 7574476.

Transitory E-Mail Addresses

Gordano's "Transitory E-mail Address" technology is patented in the United Kingdom under patent number GB2398399.

Table of Contents

1	Introduction	1
1.1	About GMS	1
1.2	Who Should Read this Guide?	2
1.3	This Guide	2
1.4	Other GMS Guides	2
1.5	Additional Gordano Products	3
1.6	Conventions	3
2	Internet Mail Concepts	5
2.1	How Does the Internet Work?	6
2.2	What is a Post Office?	7
2.3	What Does a Message Look Like?	7
2.4	How is the Mail Server Found?	8
2.5	How is the Message Transferred?	9
2.6	Collecting E-mail and Replying	10
2.7	SMTP Issues	11
2.8	Methods of Collecting E-mail	12
2.9	Sending Files by E-mail	12
2.10	System Components	13
	GMS Mail	13
	GMS WebMail	13
	Other GMS Components	14
2.11	Connecting to the Internet	14
2.12	Why is a Web Proxy Useful?	15
3	Setting Up a Mail Server	17
3.1	Installing TCP/IP	17
3.2	Naming Your Server	17
3.3	Setting up MX Records	17
3.4	Installing Internet Mail Software	18
4	Installation	19
4.1	Sizing Your Server and Connection	20
	Processor and RAM requirements	22
4.2	Other Software Requirements	22
4.3	Before Installation	22
4.4	Installing GMS on Windows	24
4.5	Installing GMS on Linux	26
4.6	What Installation Does	31
	Windows	31
	Linux	32
4.7	Changing the time zone	33
4.8	Removing Gordano products	33
	Windows	33
	Linux	33
5	Upgrades & Upgrading	35

5.1	Upgrade Policy	35
5.2	Determining Which Version You Have	35
5.3	Adding products to an existing version	35
5.4	Obtaining an upgrade installation file	35
5.5	Applying an upgrade	36
5.6	User Interface Changes from Version 3	37
5.7	Obtaining Notification of Upgrades	37
6	The User Interface	39
6.1	Introduction.	39
6.2	Logging on to Administer GMS	40
6.3	Standard Page Layout	41
	The Control Panel	42
	The Toolbar	42
	Dialog Components	43
	Status dialog	43
	Status bar	43
6.4	The Effect on the Interface of User Privileges	44
6.5	What a Standard User Sees	45
	User logon	45
	Options	45
7	Day-to-day Management	47
7.1	Accounts Overview	48
7.2	Managing Accounts	48
	Adding one or more accounts	48
	Adding Accounts using mail.exe	50
	Changing an accounts password	50
	Emulating a user	50
	Removing an account or obsolete accounts	50
7.3	Account Attributes	52
	Robot accounts	52
	DLL accounts (Windows only)	53
	Mail Manager (Windows only)	53
	List Manager (Windows only)	54
	MML Scripts	54
	Aliases	55
	Forwarding accounts	55
	"Moved" messages	56
	Autoresponders	56
7.4	Expiring Users	58
7.5	Account Reports	59
7.6	Maintaining Users Quarantine Folders	59
7.7	Groups	60
	Domain and System Groups	60
	Adding new groups	60
	Adding users to a group	62
	Calendar Access	62
	Address Book Access	64
	Folder Access	64

	Journal Access	64
	Notes Access.....	64
	Tasks Access.....	64
	Tasks Access.....	64
	Editing a group.....	64
	Deleting a group.....	64
7.8	Manage Calendars.....	65
7.9	Mailing All Users in a Domain	66
7.10	Managing Logs	67
	Specifying log levels	68
	Configuring log handling	68
	Disabling Domain and Relay logs.....	69
	Deleting, compressing or e-mailing a log.....	69
	Searching logs	70
7.11	Regular Expressions	71
8	Authentication Options.....	73
	Windows:	73
	Linux, Solaris and AIX	74
8.1	Authentication methods.....	74
8.2	LDAP authentication configuration.....	75
8.3	SQL authentication parameters.....	79
8.4	Using Windows ADSI for Authentication	81
8.5	Using Windows NT SAM database accounts.....	82
8.6	Using UNIX database accounts.....	83
8.7	Authenticating against GMS from external sources.....	84
9	Domain Management	85
9.1	Types of Domain.....	85
	Full domains	85
	Virtual domains.....	86
	POP domains	87
	Robot domains	89
	Alias domains	89
9.2	Adding a Domain.....	90
	Setting up MX records	90
	Setting up domain parameters	90
	Setting up domain aliases	92
	Setting up an Unknown User Action	93
9.3	Maintaining Domains	94
	Listing domains.....	94
	Checking domains	94
	Deleting domains	94
	Configuring account size limits and archiving	94
	Purging domain e-mail	95
	Advertising/customising the user interface	95
	Domain welcome message	96
	Access	96
	Usage Policy	96
	Interfaces	96

Email	97
10 Profile Management	99
10.1 Domain and System Profiles Overview	99
10.2 Making a new profile.....	100
10.3 Editing Profiles.....	100
Account Settings	101
Access Rights - setting user access rights	101
Configuration Rights - Setting configuration access	102
Privileges - setting user privileges	103
Preferences - setting configuration appearance	108
Preferences - configuring Anti-Spam settings	108
AV Preferences - configuring Anti-Virus settings.....	108
10.4 Changing a User's Profile.....	110
10.5 Profile Examples.....	110
11 Advanced Management	113
11.1 Tuning System Performance.....	114
Using the Watch utility to monitor performance.....	114
Incoming e-mail.....	115
Outgoing e-mail.....	117
E-mail collection (POP3)	119
Configuring Smart Routing	121
Configuring outbound delivery rules (Smart Delivery).....	124
SMTP DLLs (Windows only)	126
SMTP Shared Libraries (Unix)	126
11.2 Other Advanced Areas.....	127
Reducing use of IP resources	127
Changing the ports used by services.....	127
Using ESMTP features	130
Generating server messages.....	131
Changing RFC compliance	134
Controlling Services (Windows)	135
Controlling Services (Unix)	136
Setting up an SMTP logon message	137
Changing POST and POP timing settings	138
Listing and starting outgoing mail queues	139
Setting up DNS servers and the DNS cache.....	140
Editing Global, Domain and User variables	141
Changing use of threads	141
Using ETRN	142
11.3 Reports	143
Account Report (domain)	144
Undeliverable Mail (domain and system).....	144
Quarantine (domain and system)	144
Virus Scan Report (domain and system)	146
Virus List Report (domain and system)	147
Search Email (domain and system)	147
Licensing (system)	148
Zero Hour (system).....	148

Current Activity Report (system)	148
Domains Report (system).	150
Mail Queue Size (system)	150
Reported Junk Mail (system)	151
Alerts (system)	151
11.4 Monitoring via SNMP	151
Password	152
Allowed IPs	152
11.5 Allowing Relay	152
11.6 Shared and Public Folders	154
Enabling Access Control Lists	154
Access control modes	155
Access Control Rights	155
11.7 Porting Accounts from other Mail servers	155
AutoPort for Messaging Servers	155
11.8 Allow LDAP directory services access to Address Books	157
12 Customisation.	159
12.1 WebMail Customisation	159
12.2 Cascading Style Sheets	159
12.3 Product Logo	160
12.4 Embedding WebMail Express into a website.	161
12.5 Custom logon and logoff pages	161
Additional variables.	161
13 IP address and Port Flexibility	163
13.1 Use only IP address	163
13.2 Use specified IP addresses.	163
Configuration options.	163
13.3 Use IP Connection file	164
Configuration options	164
13.4 Sockets	165
13.5 Adding and deleting a service.	166
13.6 Adding a comment	166
13.7 Default Ports used by GMS.	166
14 Security	169
14.1 Introduction	169
14.2 E-mail and Security	170
Everything on the Internet is plain text	170
GMS storage files	170
User mailboxes	170
Logging all throughput	170
14.3 Legal Implications.	171
Spam	171
Viruses	171
Using footers as disclaimers	171
Acceptable use policies	171
14.4 Standard Security Precautions.	172
Password policy	172

Password Expiry	173
Restricting access to the Web server	173
Checking who is logged on	174
Enabling or enforcing APOP logon	174
Disabling the Finger server and Password server	174
Authenticated SMTP	175
Adding addresses to the Local IP list	175
Authenticated POP3/IMAP users	175
Post Authentication	176
Imposing limits	176
Imposing a WWW session timeout	176
Limiting sessions from a single host	177
Using service timeouts to stop denial of service attacks	178
Disabling other functions	178
Protecting the SMTP STAT command	179
Setting up Configuration Server session control	179
14.5 MX Backup	180
14.6 Firewalls	180
14.7 Network Address Translation (NAT)	180
15 Secure Sockets Layer (SSL)	183
15.1 Entering the SSL activation key	183
15.2 Assigning a certificate	183
SSL Key Certificate Generator (keycert.exe)	183
15.3 Configuring GMS to use SSL	185
ESMTP settings	185
Setting the secure ports	185
Setting the POST SSL mode	186
Configuring clients	186
Restricting Weak Connections	186
16 GMS on Complex Networks	189
16.1 Multiple SMTP Hosts	189
Potential problems and their solution	190
Multiple site setup	191
16.2 Configuring GMS as an MX Backup Server	191
16.3 Installing GMS on a Bastion Host	192
16.4 Configuring GMS as a Firewall	193
16.5 Multiple Servers Sharing a Domain	194
Normal forwarding	194
Resource utilisation	194
The round-robin setup	194
16.6 Using Multiple MX Records	195
16.7 Load Sharing	196
Enable Load Sharing	196
Primary Server Location	196
Redirect WWW Requests	196
Logon Redirected WWW Requests	197
Maximum number of WWW redirects	197

Rules.....	197
17 Providing Web Access	199
17.1 Facilities Available.....	199
17.2 Configuring the Forward WWW Proxy Server	200
Parameters	200
Cache.....	202
Authentication	202
MIME types.....	203
Dial-up	203
17.3 Configuring the Forward FTP Proxy Parameters.....	204
Enable Proxy Server.....	204
Use FTP Shortcuts	204
17.4 Configuring Forward SSL Proxy Parameters.....	205
17.5 Configuring Forward Proxy Content Scanning.....	205
Bypass sites.....	206
Banned Sites.....	206
Banned Requests	207
Banned Responses	207
Virus Scanning	207
17.6 Configuring the Reverse WWW Proxy Server	208
Parameters	209
Cache.....	210
Hosts	210
17.7 Configuring Proxy Compression	212
Requests.....	212
Responses.....	213
Bypass Requests	213
Bypass Responses	214
18 E-mail Clients	215
18.1 POP3, IMAP4 or Web Browser?	216
18.2 Thunderbird	218
Additional Features.....	219
18.3 Microsoft Office Outlook Setup	220
18.4 MS Outlook Express Setup	220
18.5 Mobile Device Mail Clients	221
18.6 Virtual domain users.....	224
19 SMS and Pager Gateway	225
19.1 GMS Mail configuration	225
Enabling the DLL	225
Sending Messages	227
19.2 GMS WebMail configuration	228
Enabling the Outbound SMS Gateway	228
Enabling the Inbound SMS Gateway.....	228
Sending messages.....	229
19.3 Allowing users access to SMS.....	229
20 GMS Instant Messaging.....	231

20.1	Installing GMS Instant Messaging	231
	Installing the software	231
	Activating Instant Messaging	231
20.2	Profile options - Access to Instant Messaging	231
20.3	Setting the Instant Messaging port	231
20.4	Logging Instant Messages	232
20.5	Location Map	232
21	GMS Anti-Spam	233
21.1	Concepts	233
	What is UCE?	233
	Spamming Techniques and Countermeasures	234
	Forging a message's source	235
	What GMS Anti-Spam Can Do for You	236
	Message Content	237
	Connections	238
	Scripts	239
	Identity checks	239
	Artificial Intelligence — the AI module	240
	Bypasses	240
	Anti-Spam filters (GMS WebMail)	241
21.2	Setting Up GMS Anti Spam	241
21.3	Messages and reply codes	241
	SMTP reply codes	242
21.4	Checking Message Content	243
	Word based checks	243
	Restricted Words	243
	Restricted Words	244
	Scored Restricted Words	245
	Regular Expressions	246
	Restricted Word Mode	248
	Restricted Word Bypass	250
	Bayesian filter (System Level)	250
	Zero Hour	251
	Reading Zero Hour information	252
	Setting up filters	253
	Message Quality	254
	Configuring Actions	261
	Domain Actions	262
	Configuring Alerts	262
	Domain Alerts	262
21.5	Attachments	262
	Ban attachments	262
	Content Types	264
	Actions	264
21.6	Connect Options	265
	Checking servers against a DNSBL	265
	Local clients	266
	Allowed IPs	267
	Maximum recipients	268

Outbound message sizes.....	269
Relay.....	270
Maximum messages.....	270
Authenticate.....	271
Authenticated IPs.....	272
Scripts.....	272
Connections.....	272
21.7 Checking Identity.....	273
Sender of message.....	273
Receiver of message.....	273
Machine name.....	273
SPF.....	274
21.8 AI Checks.....	277
Quick configuration.....	277
Details.....	277
Defining "unusual traffic".....	277
Tuning the setup.....	278
21.9 Anti Spam Log entries.....	279
21.10 Anti-Spam Filters (User Level).....	280
Junk Mail Filter.....	280
Anti Spam filter.....	280
Bayesian filter (User Level).....	281
Blocklist filter.....	281
Confirmation filter.....	282
White List filter.....	282
21.11 Spam Reporting Account.....	282
22 Anti Virus.....	285
22.1 Concepts.....	285
What is a Virus?.....	285
The Cost of Virus Attacks.....	285
Viruses and E-mail.....	286
How the Anti Virus Operates.....	286
22.2 Setting Up Anti Virus.....	287
Configuration.....	288
Actions.....	290
Configuring Alerts.....	291
Domain Actions.....	291
Domain Alerts.....	291
User Level Actions and Alerts.....	291
Virus Reports.....	291
Reading Zero Hour information.....	292
23 Automatic updates.....	293
23.1 What are automatic updates?.....	293
23.2 How updates work.....	293
23.3 General Update information.....	293
23.4 Anti Spam.....	294
23.5 Anti Virus.....	295
23.6 Zero Hour Proxy.....	295

Use Proxy server	295
Address	296
Port	296
Authentication Method	296
23.7 Freebusy	296
24 GMS Collaboration Server	299
24.1 What is GMS Collaboration Server?	299
24.2 Collaboration free/busy	300
24.3 Email only mode	300
24.4 Automatic client updates	300
Client Updates	301
How do I obtain updated client files	302
24.5 GMS & Microsoft® Exchange ActiveSync	302
What is EAS?	302
How do I use EAS?	302
EAS Troubleshooting	303
24.6 CalDav and CardDav Functionality	304
What is CalDav and CardDav?	304
How can I use CalDav and CardDav?	304
24.7 GMS Drive & WebDav	304
What is GMS Drive & WebDav?	304
How Can I use GMS Drive/WebDav	305
25 GMS Archiver	307
25.1 Setting up GMS Archiver	307
Adding a GMS Archiver profile	307
Adding a mail account	309
Disabling the mailbox	309
Configuring the GMS Archiver robot	310
Sending the message logs to the GMS Archiver robot	311
25.2 Retrieving messages from the archives	312
Interface method	312
Email method	314
26 Troubleshooting	317
26.1 Preparing to Find Faults	317
26.2 Testing the Installation	318
26.3 Checking the Network	318
Using ping	318
Checking connectivity between mail and DNS servers	319
26.4 Checking your DNS	320
Checking that DNS works	320
Does DNS have the correct mail domain information?	321
26.5 Checking How Mail is Sent	322
26.6 Checking Collection of Mail via POP3	323
Available telnet commands	324
26.7 Checking Domain and Server Automatically	324
Check MX	324
Check Server	325

Check SPF.....	325
27 Contacting Support	327
27.1 Reporting Problems to Support.....	327
27.2 Support Details.....	328
e-mail support	328
8x5 telephone support	329
13x5 telephone support	329
24x7 telephone support	329
Tailored solutions	329
27.3 Support Contract	329
27.4 Third Party Support.....	329
27.5 Contacting Support from the interface	329
How to email support from the interface	330
What information to include.....	330
How to change your support email addresses	331
Reading responses to support questions	331
27.6 Passing Suggestions to Gordano Ltd.	331
28 Frequently-asked Questions	333
29 Disaster Recovery.....	343
29.1 The Backup File Setup.txt	344
29.2 Standard Backup Procedure	344
29.3 Setting up the Recovery File	345
29.4 Saving a Domain's Mailboxes and Logs.....	345
29.5 Saving other configuration files	346
29.6 Recovering your Mail System	346
29.7 Moving GMS to Another Machine	346
30 Jargon	347
Index	351
Licence Agreements.....	361
Installation and Contact Information	371

1 Introduction

This guide introduces administrators to the Gordano Messaging Suite (GMS), the multi-platform messaging server of choice. GMS gives the maximum power and flexibility for messaging on the Internet. This guide:

- Introduces Internet mail concepts for those who are new to this area.
- Describes how to install GMS, or upgrade from an earlier release.
- Shows how to manage your mail server, first for simple networks then for more complex configurations.
- Describes the security benefits GMS offers.
- Shows how to set up GMS as a proxy Web server.
- Gives tips on setting up some of the main mail clients.
- Gives comprehensive troubleshooting and FAQ information.
- Explains GMS' disaster recovery procedures.

This guide covers the needs of both the following:

- Administrators in companies who use GMS themselves.
- Administrators working for Internet Service Providers (ISPs) and Internet Access Providers (IAPs), who provide e-mail as a service to their own customers.

1.1 About GMS

GMS takes only a couple of minutes to install. It has low management overheads because you can:

- Add large numbers of users at once.
- Manage it remotely using a Web browser.
- Allocate different levels of administrator privileges to senior users.

GMS delivers large quantities of e-mail messages quickly and efficiently. It does this by using sophisticated queuing algorithms to re-use connections, and by using Enhanced SMTP and other features. This means you do not need a top range server to run GMS.

GMS reduces the bandwidth needed to deliver and accept messages to and from the Internet. You can limit the bandwidth used for outgoing mail to avoid saturating a low bandwidth link.

1.2 Who Should Read this Guide?

This guide will be of interest to anyone interested in mail servers and how they work, but particularly to the following GMS administrators (a small system may only have the first):

- System administrator — has overall control of the system, installs GMS and adds domains.
- Domain administrator — in a multiple domain system, looks after one domain.
- Logs administrator — has access to transaction and message logs.
- GMS Anti-Spam and GMS Anti-Virus administrator - has access to the GMS Anti-Spam and GMS Anti-Virus product areas so can manage all the features of those products.

1.3 This Guide

This guide covers the administration of the following products:

- GMS Mail
- GMS WebMail
- GMS WebOrganiser
- GMS Collaboration
- GMS Instant Messenger
- GMS Anti-Spam
- GMS Anti-Virus
- GMS Archive

1.4 Other GMS Guides

The following guides provide additional information:

- *GMS User Guide* - provides detailed information on all user facing aspects of GMS. This guide describes mail client settings, GMS WebMail and GMS WebOrganizer users interfaces. It also describes the use of GMS Collaboration and GMS Instant Messenger and the integration of these two products into Microsoft Outlook.
- *GMS Communication Server Guide* - provides detailed information on all aspects of GMS Communication Server, Gordano's leading list management program. GMS Communication Server is a set of Customer Relationship Management (CRM) Tools including advanced features such as Personalised Message Targeting, Automated Voting Support, ODBC connectivity, and Job Concentration Technology. GMS Communication Server enables you to efficiently manage your lists of email addresses.
- *GMS Reference Guide* - provides detailed technical information for those wishing to use any of the available simple or

advanced programmer interfaces. This guide describes Mail.exe and other useful tools, describes all GMS database parameters, and gives example code for robots and DLLs. It provides full details of the files generated and their formats.

- *GMS MML Programmers Guide* - MML or Mail Meta Language is the language that Gordano has used to write much of its software. This language is now shared so that users of Gordano product's can customize their installations to meet their requirements. Some of the possibilities include customizing the GUI, targeting list postings to specific list members and the automatic adding of users.

1.5 Additional Gordano Products

More information about additional products can be found on our Web site. They are all integrated and work well together as a suite or as separate installations, making management seamless and easy, and each has its own guide. The products are:

- GMS Communication Server — GMS' feature rich companion software which manages lists of e-mail addresses. See the *GMS Communication Server Guide*.
- Mail Meta Language (MML) — the language you can use to write scripts for GMS, for example to produce filters. This is described in the *MML Programmer's Guide*.
- Gordano Accessory Pack — a set of utilities including NTMetrn and NTMail Inspector among others.
- Vanguard Server — provides enterprise class anti virus and anti spam protection to multiple internal mail servers, including the Gordano Messaging Suite, Microsoft Exchange and IBM Lotus Notes/Domino.

1.6 Conventions

The following conventions are used in this guide:

Convention	Used for
Courier	NT Registry keys, lines of code and DNS records.
<i>Italic</i>	Other products / services.
<value>	Reference to information you must provide.
Node > page	The ">" abbreviates a sequence of actions. For example, "Choose Users > Processing" means click the Users node in the menu tree, then choose the Processing page.
CTRL + click	Hold down the CTRL key on the keyboard while selecting multiple items by clicking on them with the left mouse button

SHIFT + click	Hold down the SHIFT key on the keyboard while clicking on the first item in a list you wish to select and dragging the pointer to the last item you want selected. This will select all items between the start and end items
<\$path>\	Denotes the base directory for the installation. On UNIX installations the default is /opt/gordano/mail/ and on Windows installations C:\Gordano\. Wherever a file location is described in the guide back slashes "\" will be used. If your GMS installation is on UNIX substitute these back slashes with forward slashes "/".

The following symbols are used in this guide:



Tip - gives you optional extra information you may want to act on. You can ignore these if you wish.



Information - gives additional explanation of points. You should read these.



Warning - warns of areas where you could damage some element of your system. You must read these.

2 Internet Mail Concepts

This section introduces Internet Mail Systems — how they work, what the jargon means and what additional information you may require. We examine how a message is delivered. This information is not GMS-specific - it applies to all Internet Mail.

If you have only used Internet Mail and have never installed or maintained an Internet Mail Server, this section will help you to understand the essential background concepts. If you cannot describe what DNS, SMTP, POP3, an MX record or a proxy is, then read on!

This section covers these elements:

- How the Internet works.
- What a post office does.
- What a message looks like.
- How the mail server is found.
- How the message is transferred.
- How to collect e-mail and reply to it.
- Simple Mail Transfer Protocol (SMTP) issues.
- Methods of collecting e-mail.
- Sending files by e-mail.
- GMS system components.
- Connecting to the Internet.
- Why a Web proxy is useful.

2.1 How Does the Internet Work?

The Internet is a collection of interconnected computers, each identified by a unique number or Internet Protocol address (IP address). For convenience, these addresses are given as four numbers in the range 0 to 255, separated by dots, for example "194.205.1.39". The number ranges from 0.0.0.0 to 255.255.255.255. The Internet lets each computer exchange information with any other computer, provided that each has a unique number and knows the other's number. Different computers communicate in their own languages, called protocols, in much the same way as humans from different countries. There are many different communication protocols in common use today.

When the Internet was first designed there was a single computer which handled the mapping of computer names to their numbers. This quickly became unmanageable and a special program, Domain Name Service (DNS), was written to perform this task. Today DNS successfully manages millions of computers, all with different numbers (addresses). DNS converts computer names to addresses, and vice versa.

You may be familiar with the World Wide Web (WWW) address (or Uniform Resource Locator - URL) which looks something like:

`http://www.gordano.com`

This contains:

- The protocol name, which in this case has the code HTTP for HyperText Transmission Protocol, the means by which Web browsers get pages from other computers.
- The name of the computer — "www.gordano.com".

The first job your Web browser has to do is convert the name of the computer into its IP address or unique number. To do this, it uses the DNS protocol - it asks for the unique number for the absolute name (or A record) "www.gordano.com". The DNS will have some configuration information so it knows how to respond to this request. In this case, the record might look like:

`www.gordano.com. IN A 216.13.182.19`

This tells DNS that when a request is made for the A record for www.gordano.com, it must reply with the IP address "216.13.182.19".



DNS may use a Canonical Name (C Name) instead. This is an alias for an A record — a C Name should always point to an A record.

Once the browser has the IP address, it knows it must send a request using the HTTP protocol. It tries to establish a connection to the remote computer and (using HTTP) asks for the page to be sent.

The above is termed a "client-server" transaction. The Web browser (or client) requests information and the Web site (or server) provides the information (or service) requested. Many different services can be provided, including e-mail.

2.2 What is a Post Office?

A post office (in Internet Terminology) is a computer that has been assigned to handle Internet Mail. Its basic task is to accept messages and decide whether they are for a local user or for someone whose post office is on another computer. If the e-mail is local, it is retained at the post office until the local user is ready to collect it.

To distinguish between people at a post office and the post office itself, the "@" sign is used. The general form of an e-mail address is:

user@post-office

The user and post office names can include any alphanumeric character and a few special characters. They are case-insensitive, so e-mail sees "sales@gordano.com" and "sales@GORDANO.com" as equivalent.



In practice, the Internet Mail protocol supports a larger range of characters than is normally used.. The characters used are restricted so that "mail gateways" that transfer mail to other systems can work correctly.

The user name is defined by the person running the post office. The name of the post office is allocated by an external authority such as the Internic. This ensures that all people use a unique post office name, so that all e-mail can be routed correctly. GMS is an example of a very powerful but easily managed post office.

2.3 What Does a Message Look Like?

Now we know what an e-mail address looks like, it's time to study a standard e-mail message. E-mail messages have two parts, body and header, separated by a blank line, as shown below:

```
From: Customer <customer@company.dom>
To: Sales <sales@gordano.com>
Subject: System recovery in GMS
Date: Sat, 12 Sep 1998 17:59:00 +0000
```

The first four lines are headers.

Hi,

How do I update my licence?

Customer

The message body starts after the first blank line.

There are two parts to this Internet Mail message:

- The message header, the part above the first blank line. This contains information about message delivery. The header shown contains the minimum required for an Internet Mail message — the specification is contained in Standards (STDs) and Requests For Comments (RFCs):

There are two e-mail addresses, telling you where the mail is from and where it is going to (these are termed the From clause and To clause). In addition, there is a Subject line and a Date. The subject is entered by the person sending the message and the message is automatically date stamped.

- The body of the message, containing the message itself. This follows the first blank line:

2.4 How is the Mail Server Found?

This section describes the basic principles of delivering an e-mail message. The message in the previous section had this destination:

To: Sales <sales@gordano.com>

This message must be delivered to the post office which runs e-mail for "gordano.com". When the message is delivered to this post office, it is stored for the sales staff to read at some time in the future. So how does the message get delivered?

The mail server that is sending the message must find out the IP address of the post office so that it can deliver the message to it. It asks DNS to provide the IP address for mail delivery to the domain "gordano.com".

Besides A records (mentioned earlier), DNS provides Mail Exchange (MX) records. These have an additional option, a priority for e-mail delivery. The DNS entry for this mail server might be:

```
gordano.com.      IN MX 10 mail.gordano.com.  
                  IN MX 20 gate05.gordano.com.
```

```
gate05.gordano.com. IN A 216.13.182.18  
mail.gordano.com.   IN A 62.172.232.100
```

For this mail server there are two MX records.

The two MX entries tell the sending mail server that there are two possible places to which it can deliver e-mail for this domain. They are "mail.gordano.com" and "gate05.gordano.com". Both of these places are actually absolute names and there are two more entries which define how these A records are translated into the IP addresses which the sending server needs. So the sending server knows that it can deliver this message to either the machine at IP address 62.172.232.100 or to 216.13.182.18.

As mentioned earlier, the MX records have a priority assigned. This tells the sending server which machine to connect to first. So, since the machine at 62.172.232.100 has a higher priority (10) than the second machine (20), the sending server delivers the message to it. If the first machine is not available (for example, because the network is broken), the sending server delivers the message to the second machine (at 216.13.182.18) instead.



Your Internet Service Provider (ISP) will probably provide your DNS for you, though if you have a permanent connection you may decide to run your own DNS. Many people install a copy of bind, a free port of the DNS software used on many Unix systems. If you decide to run DNS yourself, check its documentation for more information about how to configure your particular system. Bind is maintained by The Internet Software Consortium.

When changing DNS records, do not forget to update the serial number and do not omit the "." from fully qualified domain names.

For details of more complex use of MX records, see "Using Multiple MX Records" on page 195.

2.5 How is the Message Transferred?

We now know which machine we must send the message to. Next we need to transfer the message itself.

Messages are transferred using the Simple Mail Transfer Protocol (SMTP). When the sending server (or client) connects to the destination server, it receives this response (actually on a single line):

```
220 mail.gordano.com GMS (v4.00.0021/AB0000.00.719cfeeb) ready for
ESMTP transfer
```



To make the communication clearer in the following text, we put the letter "S:" in front of this line, indicating that it is from the destination server. In a similar way, we use "C:" to denote the client (or sending server).

The client "signs on" to the server using the HELO command:

```
C: HELO mail.company.dom
```

The server responds:

```
S: 250 mail.gordano.com mail.company.dom
```

The client must now tell the server who the mail is coming from and who it is going to. It does this using the MAIL and RCPT clauses. This transaction will look something like:

```
C: MAIL From:<customer@company.dom>
S: 250 OK.
C: RCPT To:<sales@gordano.com>
S: 250 OK.
```

Now the message (both header and body) must be sent. The client uses the DATA command to tell the server the message is about to be sent:

```
C: DATA
S: 354 Start mail input, end with <CRLF>.<CRLF>.
C: From: Customer <customer@company.dom>
C: To: Sales <sales@gordano.com>
C: Subject: System recovery in GMS
C: Date: Sat, 12 Sep 1998 17:59:00 +0000
C:
C: Hi,
C:
C: How do I update my licence?
C:
C: Customer
C: .
S: 250 OK
```



The blank line between the header and message body must be present. The message must end with <CRLF>.<CRLF>.

In this case, the server has replied "250 OK", indicating that the message has been accepted and delivered successfully.

2.6 Collecting E-mail and Replying

Messages arriving at the post office are stored until someone collects them. Usually a mail reading application, a mail client, is used to collect the e-mail. This is a program that lets you read messages, compose new messages, reply to messages, etc.

For example, one of Gordano's sales staff will use a mail client to read the message that has been sent and send a reply, for example:

```
From: Sales <sales@gordano.com>
To: Customer <customer@company.dom>
Subject: Re: System recovery in GMS
Date: Sat, 12 Sep 1998 19:23:04 +0000
```

```
>Hi,
>
>How do I update my licence?
```

Here is your licence key. Update from GMS' licence page.

Simon

This message will be sent to the local post office using SMTP. The local post office will realise that e-mail to "company.dom" is not local and queue the message for sending to the customer.

Exactly the same sequence of events takes place to deliver the reply to the customer as when the message was sent.



In the response, each line of the original message has a ">" inserted. Most mail clients use this to show the original message so that the reply is easy to find. This mechanism is one of the reasons that Internet Mail is so much faster to respond to than traditional paper mail.

2.7 SMTP Issues

The Simple Mail Transfer Protocol, as its name suggests, is very simple. Its simplicity means that there are several issues you should be aware of. These affect all Internet Mail:

- All e-mail is transferred in human readable format called "plain text", so anyone can read the message that you send (unless you encrypt it in some way).
- Anyone can "fake" a message. Any Internet Mail message might have been created by someone other than the person who appears to have sent it. The GMS Anti-Spam product has features to help prevent people faking your e-mail.
- Messages can be lost or duplicated. In practice, the vast majority of messages sent are delivered. GMS employs an internal system so that mail is never lost during transfer (it will retry later if required). Most lost messages are those that need to go through a "mail gateway". A mail gateway translates Internet Mail into another e-mail form, such as MSMail, ccMail, X-400, etc. This conversion process is usually complex and prone to error.
- Content can be changed. Anyone can tamper with the content of an e-mail message without your knowledge.

SMTP has a series of extensions which address some of these issues. These are denoted by Extended SMTP (ESMTP). GMS complies with a range of ESMTP options and has additional packages to help resolve the other issues mentioned above.

2.8 Methods of Collecting E-mail

There are three methods of collecting and reading e-mail, listed below. Decide which method(s) best suit your organisation. Here is a short description of each method; for a list of advantages and disadvantages, see "POP3, IMAP4 or Web Browser?" on page 216.



Different solutions may be applicable to different people — for example, most users might use Web Mail, but the system administrator might use Web Mail and IMAP4.

- Using a POP3 mail client
POP3 dictates how a mail client obtains e-mail from the post office (or mail server). It lets all the e-mail be collected from the server and removed from the server's storage space. Once the e-mail has been downloaded, the user can read it on their local machine.
- Using IMAP4
IMAP4 dictates how e-mail can be manipulated on the server by a mail application. As for POP3, the mail client lets messages be read and replied to, but here all the e-mail is maintained on the mail server rather than the local machine. The advantages of this are that you can access your e-mail from anywhere in the world, and can implement *hot-desking* in your office.
- Using your Web browser/Web mail
GMS lets you access your e-mail directly from your Web browser, so you can access your e-mail from anywhere in the world. The browser lets you read messages, reply to e-mail, etc. GMS WebMail. provides an advanced WebMail client. This allows multiple mail boxes, address books, etc.

2.9 Sending Files by E-mail

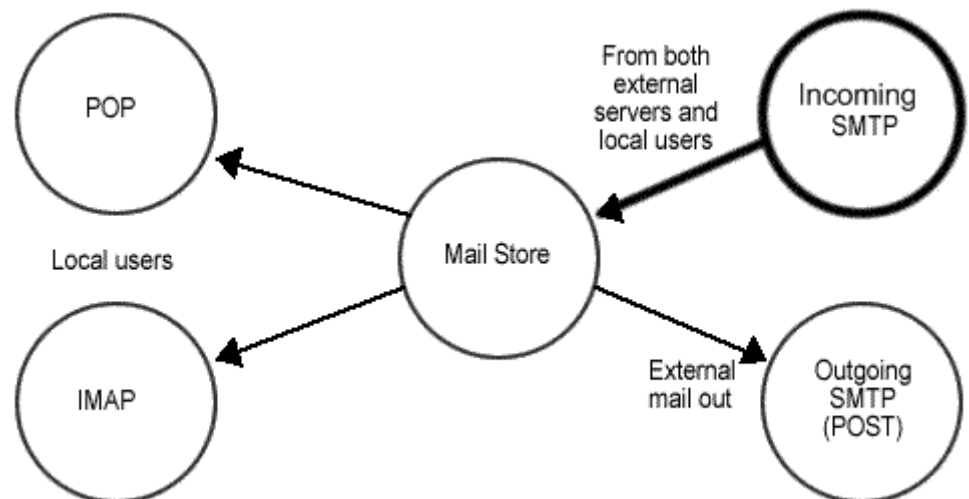
Users can attach files to e-mail messages. Their mail client encodes the file into the required format, MIME-encoded or Unencoded. The file becomes part of the message body (see the client's documentation).

GMS complies with the MIME (Multimedia Internet Message Exchange) standards.

2.10 System Components

GMS Mail

This diagram gives an overview of the system components of GMS Mail:

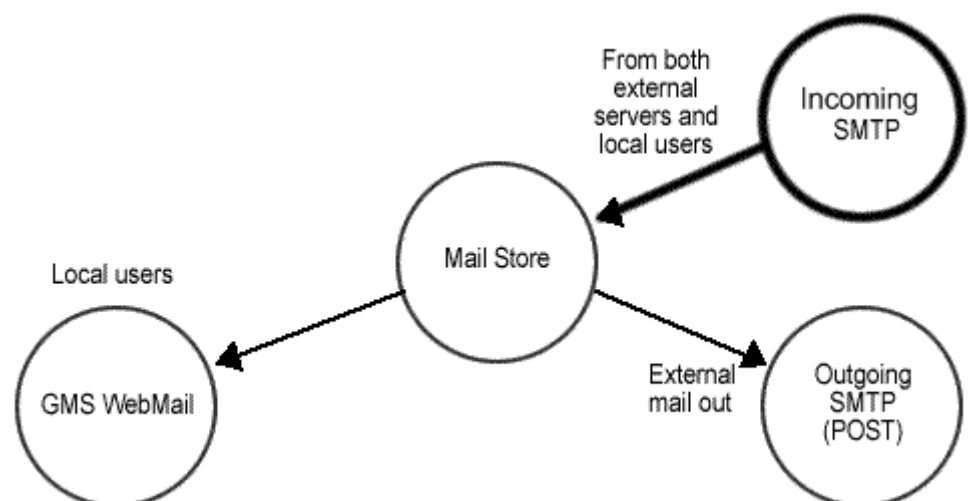


The components are:

- SMTP server — accepts incoming mail from the Internet and from local mail clients.
- POST server — also called outgoing SMTP, this uses SMTP to post mail to non-local domains.
- POP server — lets a Post Office Protocol version 3 (POP3) client collect mail from GMS.
- IMAP server — lets an Internet Message Application Protocol version 4 (IMAP) client collect mail from GMS.

GMS WebMail

This diagram gives an overview of the system components:



The components are:

- SMTP server — accepts incoming mail from the Internet and from local mail clients.
- POST server — also called outgoing SMTP, this uses SMTP to post mail to non-local domains.
- GMS WebMail server — Allows the collection of mail using the GMS WebMail browser client.



Note: POP and IMAP are not available if GMS WebMail is installed as a stand alone product without GMS Mail or another mail server that provides these services.

Other GMS Components

In addition to GMS Mail and GMS WebMail other components such as GMS WebOrganizer and GMS Collaboration can be used by mail clients such as Microsoft Outlook, Apple iCal etc. These are described in a later section of this guide.

2.11 Connecting to the Internet

Your company will be connected to the Internet in one of two ways:

- Dial-up — this is also known as intermittent connection. The equipment at your end will be a modem, an ISDN terminal adapter or a dial-on-demand router. This dials into your ISP at times which you specify (using a "schedule"), and stays up long enough to send and receive all waiting e-mail. It then disconnects. (A dial-on-demand router does not have to be scheduled, but this is the best way to cut your connection costs if you use one.)

Dial-up installation is described separately as it's more complex and you also need to set up Windows NT's Remote Access Service (RAS).

- Permanent Connection — there are several types of connection, the commonest being leased line. The connection should always be up, so incoming or outgoing e-mail is processed immediately it arrives.

2.12 Why is a Web Proxy Useful?

GMS provides a Web Proxy server. This:

- Fulfills the two most important requirements for users — delivery of Web pages and e-mail.
- Reduces bandwidth requirements by caching. Pages which have been read are stored (*cached*) by the server. If they are requested again within a set time, they are retrieved from the cache rather than obtained from the external Web site.
- Protects your Web Server. The reverse proxy will allow the web server to remain behind a firewall. When a client makes a request to your site, the request goes to the proxy server. The proxy server then sends the client's request through a specific passage in the firewall to the content server. The content server passes the result through the passage back to the proxy. The proxy sends the retrieved information to the client, as if the proxy were the actual content server.

The proxy server is used as a go-between in Internet connections. That is, the user connects to the proxy and the proxy connects to the Internet and carries out their request. A proxy has the advantage that it lets all users browse the Web through a single line, which is especially useful if you use a dial-up connection to an ISP.

3 Setting Up a Mail Server

For those who have never set up an Internet mail system, this section provides an overview of this process.

There are four stages to setting up an Internet mail server:

1. Installing the Internet (TCP/IP).
2. Naming your server.
3. Setting up Mail Exchange (MX) records.
4. Installing Internet mail software, such as GMS.

These are covered in turn below.

3.1 Installing TCP/IP

We assume at this stage that you have installed your TCP/IP and have it running correctly.

3.2 Naming Your Server

You can choose any name for your mail server, for example "mail".



It is important that you set up both a hostname and a domain name for your mail server under its TCP/IP configuration to prevent problems with outbound mail delivery. It is also helpful to make the hostname of the server match the hostname that you use in DNS for SMTP.

On a large system, try to plan for future expansion now. The DNS gives you another option that may "future proof" your installation. It lets a single machine have many names. You can use this to give each part of the mail service a unique name, for example:

- mail.company.dom — where to send e-mail to.
- pop.company.dom — where users collect e-mail from.
- imap.company.dom — the name used by power users with IMAP clients.
- mx.company.dom — a backup MX mail server.

All of these could point to the same physical machine, but by giving them separate names you can separate the functions and help your users.

3.3 Setting up MX Records

The most complicated part of setting up a mail server is establishing correct (MX) records, yet this has nothing to do with GMS. As described in "How is the Mail Server Found?" on page 8, MX records dictate where mail is delivered. They also provide information on backup mail systems in case your mail server is down.

Mail Exchange information is held by the DNS as MX records in this form:

```
company1.dom.  IN MX 10 smtp.company1.dom.  
               IN MX 20 mx.isp.dom.
```

Providing setup information for all of the different varieties of DNS software is beyond the scope of this guide, but for more information see the book *DNS and Bind* by Paul Albitz & Cricket Li. This is published by O'Reilly & Associates, Inc. (for purchase information see www.ora.com).

Your ISP should be able to help you set up your MX records correctly. If they do set up your DNS, once you have installed GMS you may wish to check that they have done this correctly. See "Troubleshooting" on page 317 for details of how to do this.

3.4 Installing Internet Mail Software

Installing GMS normally only takes a few minutes (see "Installation" on page 19). Once it's installed you should have a fully functioning Internet mail system with just the default account, postmaster.

The next step is adding users (or configuring GMS to authenticate to the correct location of your user database). You can do all this using your Web browser.

4 Installation

This section is for administrators installing GMS for the first time (not upgrading from a previous version). It describes:

- How to size your server and connection.
- Other software you require.
- What to do before starting to install GMS.
- Installing GMS at sites with permanent connections.
- Installing GMS at sites with dial-up connections (Windows only).
- Testing the installation.
- Changing time zone.
- A summary of what installation does.

Things you will need to have set up before installing GMS:

- TCP/IP

4.1 Sizing Your Server and Connection

The size of server and network link you need depends on how your users will use e-mail. This affects your system in several ways, but this section gives guidelines based on average use of a mail system.

Two formulae are important:

Disk space (MB) =

$$\begin{aligned} & \text{Number of users} \\ & * \text{Average number of messages daily per user} \\ & * \text{Average message size} \\ & * \text{Time mail is stored on server} \\ & / 1024 \\ & * 1.01 \text{ (1\% allowance for transaction logs)} \end{aligned}$$

Network
bandwidth (bps) =

$$\begin{aligned} & \text{Number of users} \\ & * \text{Average no. messages per day per user} \\ & * \text{Average message size} \\ & * \text{Ratio of messages sent outside} \\ & * 1024 * 8 / 86400 \end{aligned}$$


Note that if your installation is also using other GMS components such as GMS Collaboration you will need to make an additional disk space allowance on the server. This is a more finite amount than that required for mail storage and should require no more than 1Mb allowance per user.

This table shows the meaning of the parameters in the above formulae:

Parameter	Description
Average number of messages daily per user	The average of all e-mail users. A typical figure might be 10 messages per day.
Average message size	Although most messages will be short, attachments such as spreadsheets and documents increase the average size. Users sending graphics increase it dramatically. A typical value might be 24KB.

Parameter	Description
Time mail is stored on server	This depends on how your users read their e-mail. If they use POP clients, mail may only be present for half a day. If they use Web and IMAP, they tend to leave mail on the server for longer periods. We'll assume an average of 30 days for Web and IMAP. For a comparison of POP and IMAP, see "POP3, IMAP4 or Web Browser?" on page 216.
Ratio of messages sent outside	Number of messages sent to/ received from outside this server, divided by the total number of messages. A value of 0.25 (one message in four goes outside) is reasonable, though this will fall as the number of users increases.

The following table shows the network bandwidth needed for the connection to the Internet. This is based on the assumption that once the connection is made 100% bandwidth is used (this requires that local mail is delivered to an ISPs mail server for delivery).

It assumes that:

- Average number of messages sent daily per user = 10.
- Average message size is 32KB.
- Mail for POP3 accounts is left on the server for half a day.
- Mail for IMAP accounts is left on the server for 20 days.
- Ratio of messages sent outside = 0.25.

Disk Space Required (MB)			Bandwidth required for continuous connection (baud)	Time required (hh:mm:ss) at		
Users	POP3	IMAP4		28.8 baud	64 baud	256 baud
10	2	63	85	00:04:16	00:01:55	00:00:29
25	4	158	213	00:10:40	00:04:48	00:01:12
50	8	316	427	00:21:20	00:09:36	00:02:24
100	16	631	853	00:42:40	00:19:12	00:04:48
250	39	1578	2133	01:46:40	00:48:00	00:12:00
500	79	3156	4267	03:23:20	01:36:00	00:24:00
1000	158	6313	8533	impractical	03:12:00	00:48:00

Disk Space Required (MB)			Bandwidth required for continuous connection (baud)	Time required (hh:mm:ss) at		
Users	POP3	IMAP4		28.8 baud	64 baud	256 baud
2500	395	15781	21333	impractical	impractical	02:00:00
10000	1578	63125	85333	impossible	impossible	08:00:00



IMAP requires more space than shown in the last column, because messages are stored on the server.

For POP3, the disk space figure does not include the space needed by users storing e-mail messages on their PCs.

Processor and RAM requirements

For entry level systems up to 1000 users, Gordano recommends a minimum server specification of at least 2 physical CPU and 8GBs or RAM. Performance will also be affected by Hard disk specification depending on any given scenario.

4.2 Other Software Requirements

GMS may need the following software on your system:

- A Web browser. GMS can be configured using Internet Explorer 6 or later along with any other browser of your choice. We recommend that you use the latest version of Internet Explorer, Firefox and Google Chrome.
- PDF reader — Adobe provides a free PDF (Portable Document Format) reader. All GMS documentation uses this format.

4.3 Before Installation

Start GMS installation by downloading the file containing GMS from the Gordano Ltd. Web site.

Before you install GMS, you must install a network card and TCP/IP on the server. You will need to know the following information:

- Your domain name and your server's IP address. This must be a static IP address — you cannot install a mail server on a machine with a dynamic IP address, for example using DHCP.
- Your company name.
-



Use the table on the back page of this manual to record this information in case you require it later.



Dial up internet connections are not supported for Linux, Solaris or AIX platforms.



The dialog in the installation procedure have an 'Explain' button giving help on what you need to enter. Use this if you are unsure how to proceed.

4.4 Installing GMS on Windows

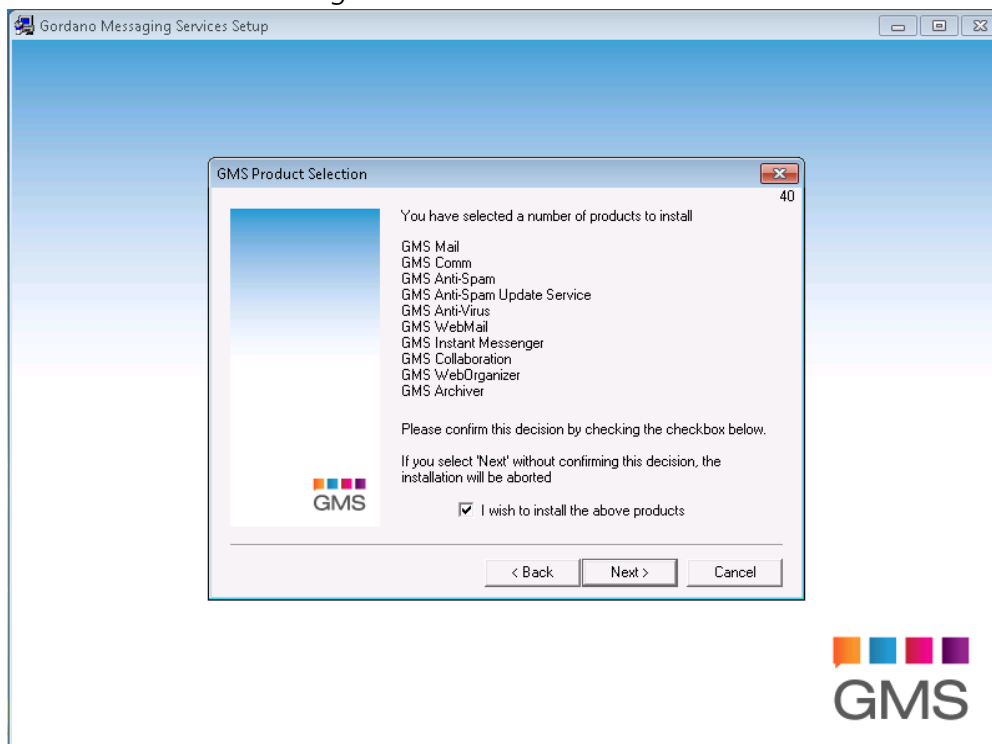
To install GMS for a permanent connection, do the following:

1. Use Windows Explorer or the Start > Run menu to run the downloaded GMS installation program. This guides you through installing the full GMS product suite. Read the online licence agreement before continuing.
2. A 28 day licence (by default for 43 users and unlimited domains) is automatically generated.



If you require a larger licence Trial keys are available from our Web site at www.gordano.com, from your channel or by contacting sales. See the contact details at the back of this guide.

3. The installation will ask you to choose which products from the Gordano Messaging Suite you would like to install. You can choose to install them all to trial then only purchase those that you want or select only the desired product at this stage.
4. The next page will list the products you have elected to install and ask you to confirm your choice by ticking the check box before clicking "Next >".



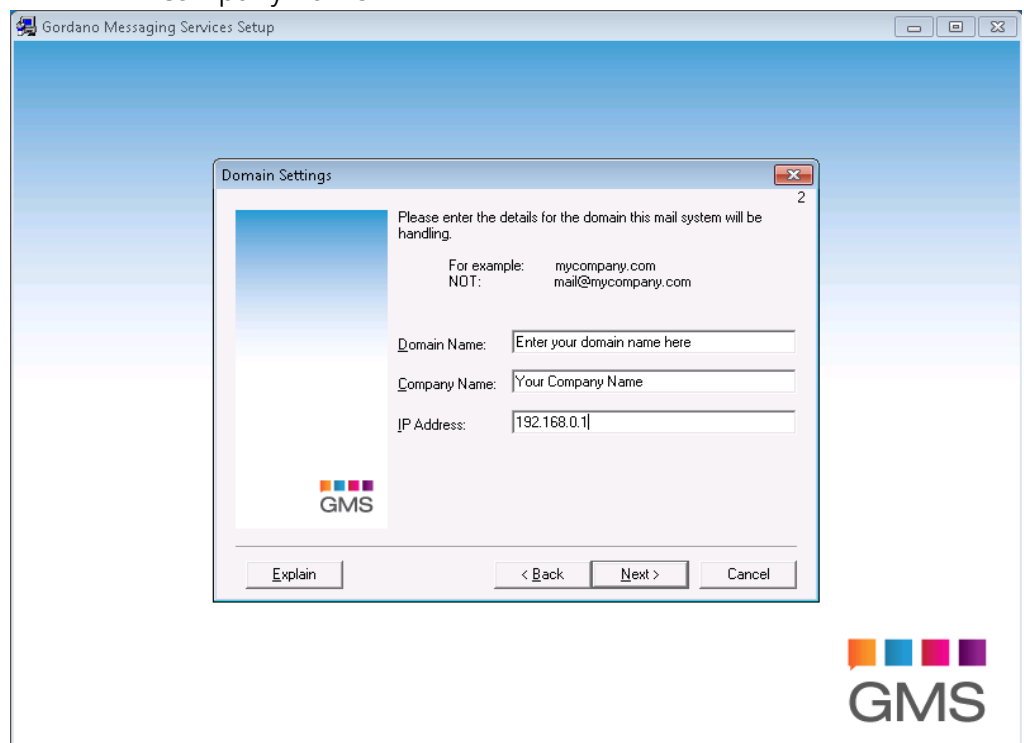
5. You will then be asked where you want to install your Gordano products, if you do not want to use the default location, C:\Gordano, specify another using the "Browse" button.
6. When Gordano products are installed, a mail account called "postmaster" is created, with full administration privileges. You will use this account to configure your system using a Web

browser. The next page will ask you to enter a password for this account. Make sure you make a note of this password.



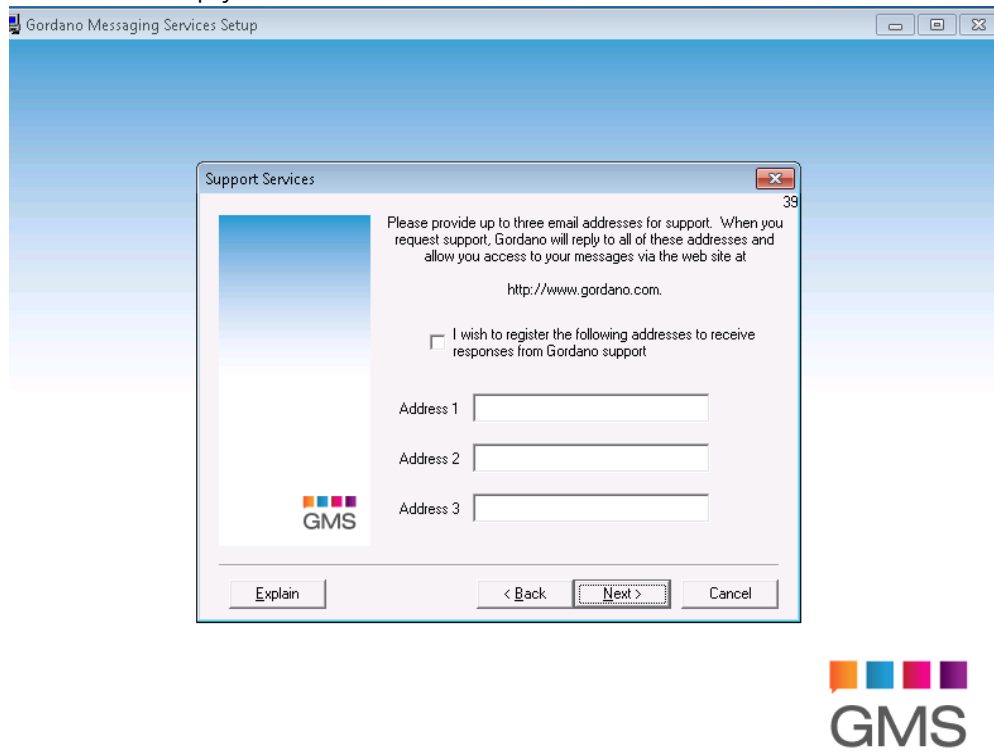
The security of your system can be compromised if you choose a poor password; see "Password policy" on page 172 for hints on choosing passwords.

7. You will then be asked to select how your users will be authenticated. i.e. where user information will be held so that the software can check users exist and validate their passwords and access rights. The default is to use just Gordano's proprietary database. You can however de-select this and use another option or combine it with an NT database and an optional external database such as the Active Directory. Once you've made your selection click on "Next".
8. If you selected one of the authentication options other than Gordano's proprietary database the next screen gives you instructions on how to configure that method of authentication.
9. You will then be asked for your domain name, IP address and company name:



10. For the domain name, if you are using an ISP then type the name they gave you. Otherwise, type the domain name registered for your company, for example "mycompany.dom".
11. Type your IP address (from your network card) and company name.
12. You are then asked if you would like to provide up to three email addresses that you would like to use for contacting support. Entering an address or addresses here will help you get

the fastest possible response from the Gordano support team simply tick the text box and enter between 1 and 3 addresses.



13. On the next screen press next to start the install.

14. The installation is complete. You can now test it, as described in "Testing the Installation" on page 318.

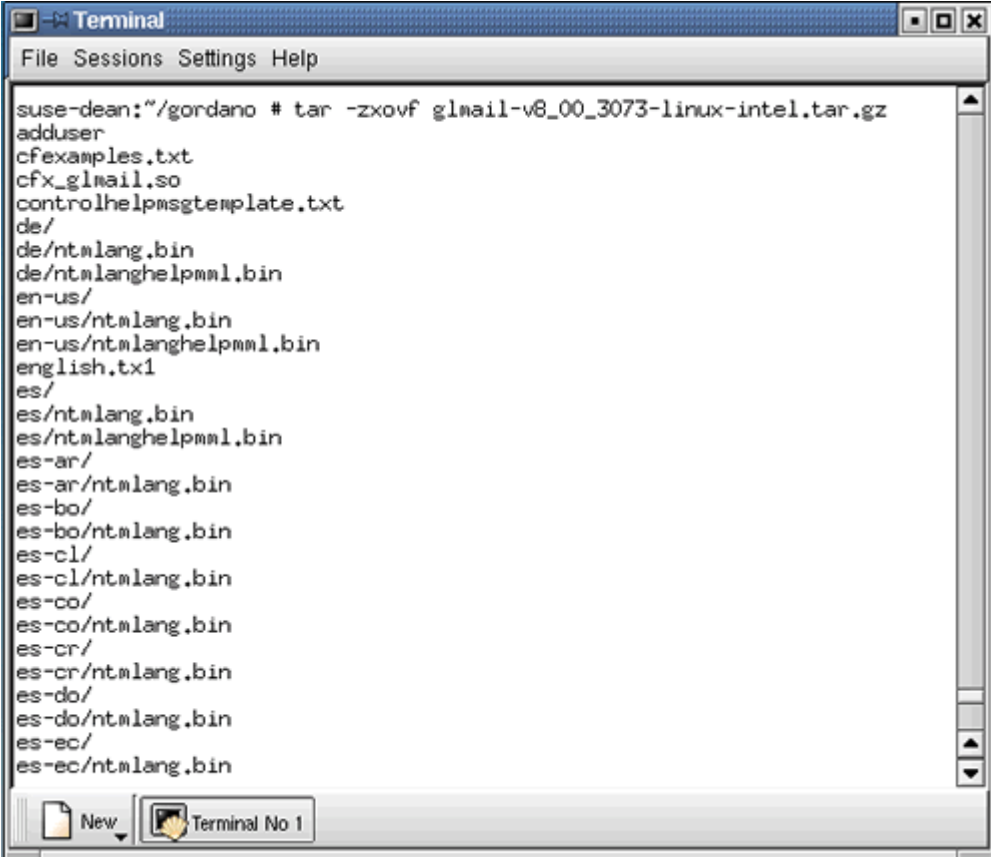
4.5 Installing GMS on Linux

The install process is similar for Solaris ,AIX and Linux. To install GMS, do the following:



You must be logged on to your machine as root when installing GMS.

1. Download the installation file and copy it to a suitable directory on your machine. For example "/install".
2. The install file comes packaged as a .tar file which has been compressed into a gzip file (.gz). From a terminal window, the files can be unpacked by typing:
tar -zxovf filename

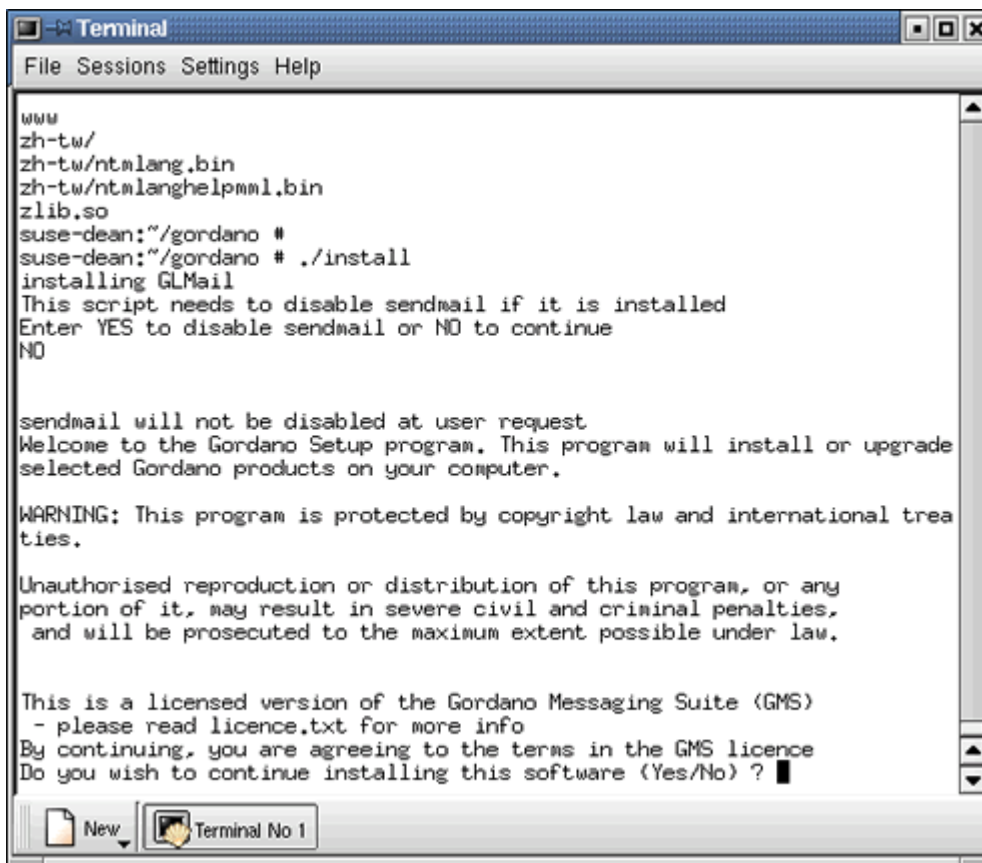
A terminal window titled "Terminal" with a menu bar (File, Sessions, Settings, Help). The command prompt shows a user at a suse-dean machine running a tar command to unpack a file. The output lists various files and directories being extracted, including language-specific binaries and help files for different locales like de, en-us, es, and es-ar.

```
suse-dean:~/gordano # tar -zxovf glmail-v8_00_3073-linux-intel.tar.gz
adduser
cfexamples.txt
cfx_glmail.so
controlhelpmsgtemplate.txt
de/
de/ntmlang.bin
de/ntmlanghelpmml.bin
en-us/
en-us/ntmlang.bin
en-us/ntmlanghelpmml.bin
english.txt
es/
es/ntmlang.bin
es/ntmlanghelpmml.bin
es-ar/
es-ar/ntmlang.bin
es-bo/
es-bo/ntmlang.bin
es-cl/
es-cl/ntmlang.bin
es-co/
es-co/ntmlang.bin
es-cr/
es-cr/ntmlang.bin
es-do/
es-do/ntmlang.bin
es-ec/
es-ec/ntmlang.bin
```

This unpacks the files required for installation into your install directory. The console will display the filenames as the files are unpacked as shown in the picture above.

It is advisable to read the file `releasenotes.txt` which contains details of updates in the version being installed.

3. You are now ready to initiate the install by typing `./install` from within your install directory.
4. It is a necessary part of the install process to disable Sendmail if it is installed on your machine. The install script will ask you to confirm that Sendmail can be permanently disabled on your system. If you agree to this, type YES in capital letters and the install will continue, otherwise the install will be aborted.



```
Terminal
File Sessions Settings Help

www
zh-tw/
zh-tw/ntmlang.bin
zh-tw/ntmlanghelpmm1.bin
zlib.so
suse-dean:~/gordano #
suse-dean:~/gordano # ./install
installing GLMail
This script needs to disable sendmail if it is installed
Enter YES to disable sendmail or NO to continue
NO

sendmail will not be disabled at user request
Welcome to the Gordano Setup program. This program will install or upgrade
selected Gordano products on your computer.

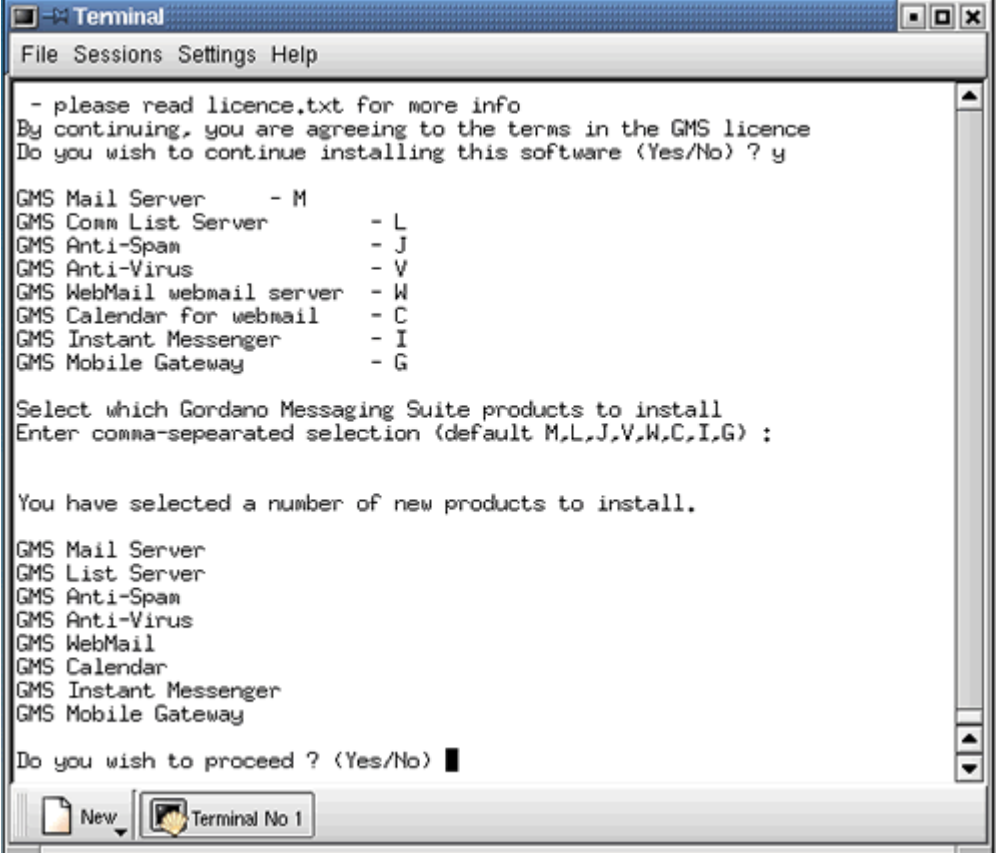
WARNING: This program is protected by copyright law and international trea
ties.

Unauthorised reproduction or distribution of this program, or any
portion of it, may result in severe civil and criminal penalties,
and will be prosecuted to the maximum extent possible under law.

This is a licensed version of the Gordano Messaging Suite (GMS)
- please read licence.txt for more info
By continuing, you are agreeing to the terms in the GMS licence
Do you wish to continue installing this software (Yes/No) ? █
```

5. Next you will be asked to read the licence agreement contained in the licence.txt file. If you agree to the terms of the licence agreement type "yes" when prompted.
6. Next you will be asked which products from the Gordano suite you would like to install. To install the whole suite (default) just hit the Enter key. To install just one or two of the products type a comma separated list of products. For example M,J will install

GMS with JUCE. You will be prompted to confirm your selection.



```
- please read licence.txt for more info
By continuing, you are agreeing to the terms in the GMS licence
Do you wish to continue installing this software (Yes/No) ? y

GMS Mail Server      - M
GMS Comm List Server - L
GMS Anti-Spam        - J
GMS Anti-Virus       - V
GMS WebMail webmail server - W
GMS Calendar for webmail - C
GMS Instant Messenger - I
GMS Mobile Gateway   - G

Select which Gordano Messaging Suite products to install
Enter comma-seperated selection (default M,L,J,V,W,C,I,G) :

You have selected a number of new products to install.

GMS Mail Server
GMS List Server
GMS Anti-Spam
GMS Anti-Virus
GMS WebMail
GMS Calendar
GMS Instant Messenger
GMS Mobile Gateway

Do you wish to proceed ? (Yes/No) █
```


7. The install will then ask you to provide the following information:
 - Install directory. To install to the default /opt/gordano directory just press the Enter key.
 - The password to be used for the postmaster account. You will need to type this twice to confirm you have entered it correctly.



The security of your system can be compromised if you choose a poor password; see "Password policy" on page 172 for hints on choosing passwords.

- The domain name that your machine is to host mail for. For example yourcompany.dom. The domain entered here should have an MX record set up in DNS.
- The IP address of the machine GMS is being installed on. To accept the suggested address press the Enter key.

- Enter a space separated list of IP addresses for the DNS servers that GMS should use for domain name resolution. To accept the suggested address press the Enter key.



```
Terminal
File Sessions Settings Help

Enter initial configuration password (at least 6 characters) : xxxxxxxx
Re-enter configuration password : xxxxxxxx

Enter Internet Domain name (default company.dom) : company.dom

Enter Host IP address (default (192.168.132.25) : 192.168.132.25

Enter IP address of DNS server (default 192.168.132.20) : 192.168.132.20

Enter port for SMTP server (default 25) : 25

Enter port for WWW Configuration server (default 8000) :

GMS Mail database - G
UNIX database - U
External database - E

Select Authentication methods to be used
Enter comma-separated selection (default G) :

Enter name of user to own mail system files (default mail) :

Enter name of group to have access to mail system (default other)

Please provide up to 3 email addresses for support. When you
request support, Gordano will respond to all of these addresses
and allow you access to your support messages on the website at

www.gordano.com

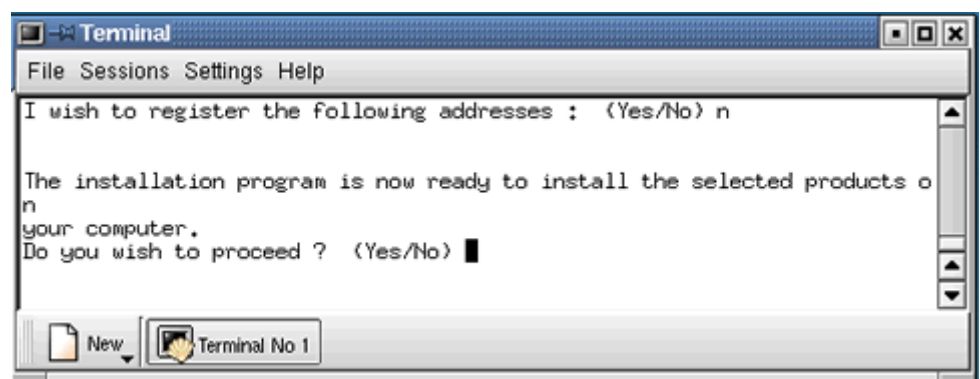
I wish to register the following addresses : (Yes/No) █
```

- The port to be used by the SMTP service. To use the default port 25 press the Enter key.
- The port to be used for configuring GMS using a WWW browser. To use the default port 8000 press the Enter key.
- Select the Authentication method to be used. There is a choice of GMS' proprietary database (G), the UNIX user database (U) and an External database (E). If you select E for an external database you can choose from L for an LDAP database and S for an SQL database. See "Changing an accounts password" on page 50 for more information.



If you choose an external database you will need to configure the parameters GMS needs to access the data. This is done from the administration interface by selecting the system level Authentication branch. Additionally on multiple domain systems each domain may have its own individual authentication settings.

- The name of a user on your system that will own all mail files. To accept the default of "mail" press the Enter key.
 - The name of a group that is to have access to the mail system. To accept the default of "other" press the Enter key.
8. You are also asked to optionally provide up to 3 email addresses which will be registered with Gordano support. The addresses entered here will be the ones that Gordano support will respond to should you contact them.
 9. You will then be asked for final confirmation that you wish to complete the install. Typing "yes" installs the products you selected and starts the GMS services. Your server is now ready to receive and send mail and can be configured straight away using a web browser by typing `http://<server_IP_address>:8000` in the address bar on any machine and `http://127.0.0.1:8000` on the server itself..



10. You can now test your installation as detailed in "Testing the Installation" on page 318.
11. The install comprises a fully functional 28 day demonstration of GMS Office (50 users). If you require a larger version contact sales@gordano.com for a separate trial activation key.



Trial keys are also available from our Web site at www.gordano.com, or from your channel.

12. If you have purchased an activation key for GMS follow the instructions sent with the key to enable the full licence.

4.6 What Installation Does

Windows

This section summarises the elements installation adds to your Windows NT or Windows 2000 machine.

The main additions are:

- GMS program and data files, stored under the directory specified during the installation.

- MySQL database required for vCard, Addressbook and Calendaring functionality.
- Registry entries for GMS stored under this key:

HKEY_LOCAL_MACHINE/Software/InternetShopper/Mail

Installation installs and starts the following Gordano services:

- Configuration Server — allows configuration of GMS using a Web browser.
- POP, POST, IMAP, SMTP, GMSSQL and LIST servers.

Installation also:

- Configures GMS with the default settings for domain and IP address which you specified during the install.
- For dial-up sites, specifies how mail is to be sent to and from the ISP. (Many of these details can be changed later, if required.)
- Adds a single account called postmaster@<yourDomain>. To comply with RFCs, all mail servers must have a postmaster account available at all times.

By default, this account can send and receive mail, and can be used to configure GMS and other Gordano products using a Web browser by pointing to `http://<your IP>:8000`. This account has system, domain and logs administrator permissions (see “The Effect on the Interface of User Privileges” on page 44). You should not delete this account.

Linux

This section summarises the elements installation adds to your machine.

The main additions are:

- GMS program and data files, stored under the directory specified during the installation.
- The GMS install scripts are copied to the install directory specified during the installation.
- Startup scripts in /etc:
 - /etc/rc0.d/K30GMS
 - /etc/rc1.d/K30GMS
 - /etc/rc6.d/K30GMS
- Configuration Database entries for GMS stored in hidden .reg files under this directory:

<BaseDir>/Mail

Installation installs and starts the following GMS services:

- Configuration Server — allows configuration of GMS using a Web browser.
- POP, POST, IMAP, SMTP and LIST servers.

Installation also:

- Configures GMS with the default settings for domain and IP address which you specified during the install.
- Adds a single account called `postmaster@<yourDomain>`. To comply with RFCs, all mail servers must have a postmaster account available at all times.

By default, this account can send and receive mail, and can be used to configure GMS using a Web browser by pointing to `http://<your IP>:8000`. This account has system, domain and logs administrator permissions (see "The Effect on the Interface of User Privileges" on page 44). You should not delete this account.

4.7 Changing the time zone

Once you have installed GMS one of the first things you might want to do is adjust the time zone for your local area. This is done from the System Administration > Settings > General page of the GMS interface.

4.8 Removing Gordano products

Windows

To remove GMS you can use the Add/Remove programs option under the control panel or run the uninstallation program from `Run>Programs>Gordano Messaging Suite>Remove products`. A popup dialog box will ask you to confirm. select OK to confirm or Cancel to abort the removal.

Linux

To remove GMS navigate to the `/basedir` directory (default is `/opt/gordano/mail`) and type `./uninstall now`. This will issue a warning asking if you are sure you want to remove all Gordano products. Entering YES in upper case will continue to remove all Gordano products from the machine. Entering anything other than YES in upper case will abort the removal.

5 Upgrades & Upgrading

This section is for administrators who are upgrading from a previous version of Gordano software. If you are installing GMS for the first time, read the Installation section instead.

This section describes:

- The different types of upgrade and their numbering.
- Determining which version you already have.
- How to obtain an upgrade.
- How to apply an upgrade.
- User interface changes since Version 3.0.
- How you're told upgrades are available.

5.1 Upgrade Policy

To upgrade GMS you will require a valid maintenance key. To determine if your current maintenance key is valid go to the Licensing page of the interface where the expiry date of the maintenance key is displayed.

Since the release of GMS 3028 there is an exception to this rule whereby releases denoted as Hotfixes can be installed without a maintenance key.

5.2 Determining Which Version You Have

There are two ways to display the GMS version number:

- Look at the top of the home page in the user interface
- Open a command prompt, go to the directory `Gordano\bin` and type any service name (SMTP, POP, etc.) followed by '-s'.

5.3 Adding products to an existing version

If you want to add for example GMS WebMail to an existing GMS installation this is very straightforward. Just contact sales@gordano.com for a GMS WebMail key or purchase one from the Gordano website. The key will arrive via an email which will tell you how to enter the key on the Licensing page of the interface. That's all there is to it.

5.4 Obtaining an upgrade installation file

To obtain an upgrade install file, go to the web site <http://www.gordano.com> or use ftp from [ftp.gordano.com](ftp://ftp.gordano.com). In addition to downloading the software you will have to have a valid maintenance key that has not expired. This can be obtained from sales@gordano.com or by phoning the number at the back of this guide.

5.5 Applying an upgrade

The upgrade you receive will be a single file and in fact is the same file used for first time installs.



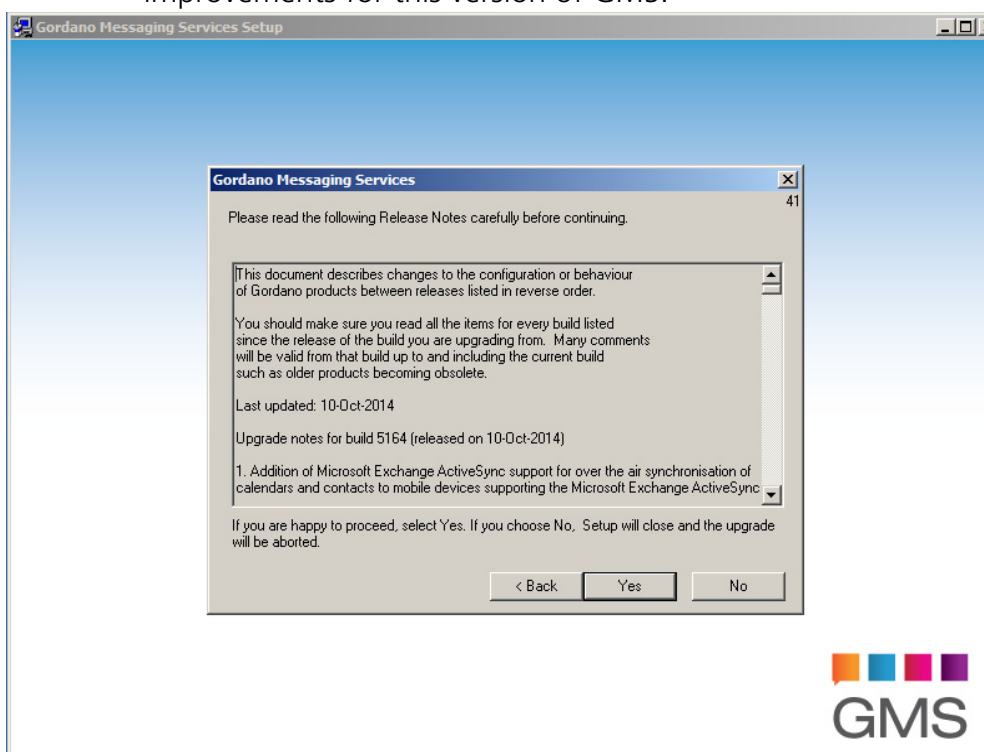
You cannot install an earlier version over a later version.

You must have obtained a maintenance key before you can install the upgrade

Prior to upgrading it is advisable to create a system recovery file, see page 345, and take a backup copy of the entire Gordano File structure

To upgrade, do the following:

1. Copy the new executable into a temp directory.
2. Run the new executable, either by double-clicking on the downloaded file or by selecting Start, Run and typing in the program name, then clicking OK.
3. You will then be asked to confirm that you agree to the licence agreement before you can continue.
4. A dialog box will be displayed showing the enhancements and improvements for this version of GMS.



5. Then you will be prompted to confirm that you wish to upgrade your Gordano products.



Upgrading is a one way process.

6. Your current keys will then be listed along with any expiry dates that may be applicable. Check that a maintenance key is listed and that it hasn't expired.
7. If a valid maintenance key is listed then you can click on "Next" without entering any keys.
8. If there is no maintenance key or it has expired you will need to enter a new maintenance key which can be obtained from sales@gordano.com or via Gordano's website, <http://www.gordano.com>.
9. If you need to enter a key you first have to enter the "Customer Reference" this will be in the format "XX1234.00" (The two digits after the dot refer to the machine number, if you are unsure what this is check the System>Key page on your server or the email that the key came in). Once you have typed in the number press Enter. Then you will have to type in the key itself. Be very careful not to make a mistake. Press Enter when you have finished typing.
10. When you have finished entering keys or if you already have a maintenance key that is in date, click on the "Next" button. The install will then check to make sure there are no potential upgrade problems.
11. Next you will be asked if you want to go ahead and complete the upgrade. Click on "Next" and the upgrade will take place.
12. Should you encounter any problems upgrading contact sales@gordano.com with details of what has gone wrong.

5.6 User Interface Changes from Version 3

If you have upgraded from Version 3, note that there are no CPLs now. All configuration is done using a Web browser, whether you are located locally or remotely.

5.7 Obtaining Notification of Upgrades

Gordano runs mail lists to notify you of new information available on its server. These use a GMS Communication Server list to deliver the information to customers.

To join or leave a mailing list:

- To subscribe, send a message to the list with a to address of <listname>-join@listdomain.dom. For example to join discuss@gordano.com you would send a message to discuss-join@gordano.com.
- To unsubscribe, send a message to the list with a to address of <listname>-unsubscribe@listdomain.dom. for example to leave the discuss@gordano.com list send a blank email to discuss-unsubscribe@gordano.co.uk.
- Alternatively you can visit the Support page of the Gordano website and join or leave a list from there.

You will receive a mail message confirming that you have been added or removed from the appropriate list.



You can also subscribe/unsubscribe other people to/from a list; see the GLCommunicator Administrator's Guide.

The following mail lists are maintained:

- **Discuss@gordano.com** — used to discuss the addition of new features and other GMS related topics. It is also a useful source of technical help from other GMS users.
- **MML@Gordano.com** — used to discuss issues associated with the Mail Meta language (MML). It is a useful source of information for MML programmers

These lists are monitored by the Gordano Support team, but they do not respond to support requests made via the lists.

6 The User Interface

This section introduces Gordano's user interface. All administrators should read this section, including those who are upgrading from earlier versions, since the new interface is very different.

- Logging on for administration.
- The screen and page layout.
- The effect on the interface of different administrator privileges.
- The effect on the interface of different user privileges.
- User plans.

Gordano's user interface can only be accessed using a Web browser, preferably Firefox or Internet Explorer, although other browsers such as Chrome should also work. Gordano products can be configured remotely over the Web, subject to security measures; see "Restricting access to the Web server" on page 173.

6.1 Introduction

The Gordano browser based GUI:

- Lets all your users read their e-mail using their Web browser. They can read, forward, reply and delete their mail from anywhere they have access to the Internet. This also lets you hot-desk within an office.
- Allows configuration of Gordano products from anywhere using a standard web browser.
- Configuration pages have online context-sensitive help.

6.2 Logging on to Administer GMS

To start up the Administration GUI, do the following:

1. Open your Web browser, either Netscape or Windows Explorer.
2. In the Location or Address field, type **http://127.0.0.1:8000**



127.0.0.1 is the server's loopback address and 8000 is the port used by the Configuration server, if you are running your browser on a separate machine replace 127.0.0.1 with the actual IP address of the GMS server.

3. Press ENTER. The GMS logon screen should appear:

4. Type **postmaster@<domain>** in the User Name box and the postmaster's password you set up during installation in the Password box.
5. Select the required option from the Interface drop down menu. Depending on the products installed some of these options may not be displayed.

Administration - Logs the user into the Administration interface. The options displayed and available to the user will depend upon their access rights. Logging in as Postmaster will provide full access to all products

GMS WebMail Professional - Logs the user into the GMS WebMail Professional interface. GMS WebMail is an advanced web based mail client that brings the power of a traditional workstation based mail client to your web browser. It will empower you to receive, reply and manage your e-mail securely from anywhere in the world. Like all Gordano products is easy and familiar to use, combining reliability with high performance. It includes an extensive range of features including unlimited address books, Aliases, Filters and Folders for filing messages.

GMS WebMail Express - Logs the user into the GMS WebMail Express interface. The WebMail Express Client provides a low bandwidth solution ideal for users accessing their email from locations with limited resources.

GMS WebMail Mobile - Logs the user into the GMS WebMail Mobile Interface. If you wish to access your mail via a Personal Digital Assistant (PDA) or your Internet connection is particularly slow you can log on to the mobile interface which is especially designed to meet those needs.

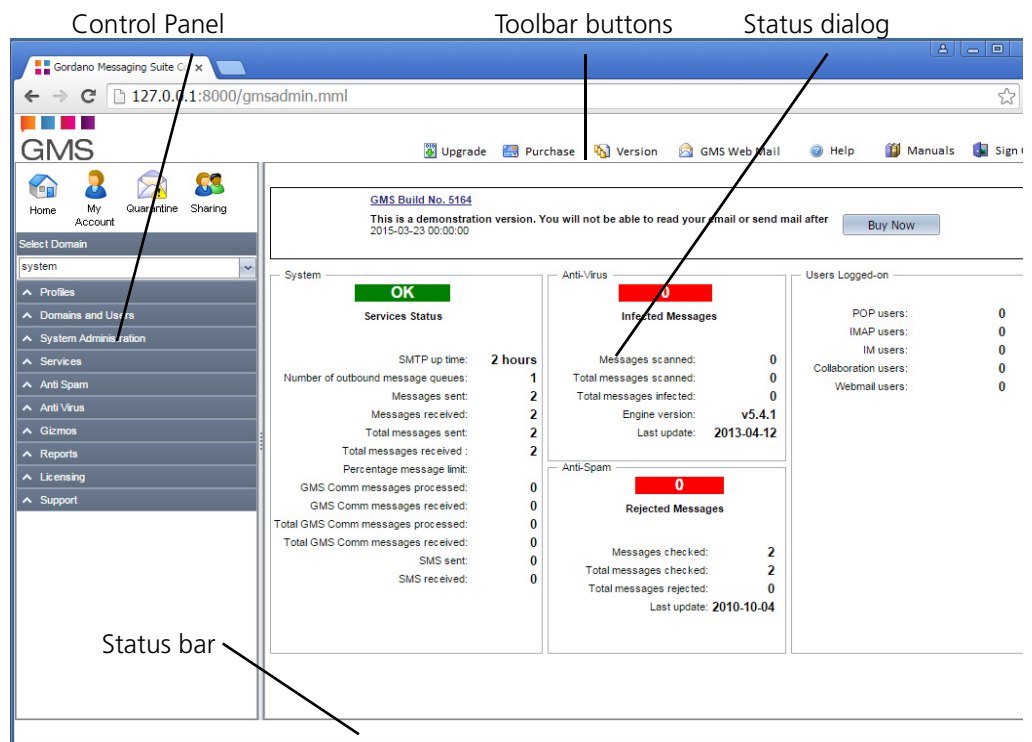
Instant Messaging - Logs the user into Instant Messaging and opens an Instant Messaging window. Instant messaging allows you to have realtime text conversations with other users on your email system. It allows you to talk to single or multiple contacts at once.

Anonymous List - Use this option to log on with a list account name and password. Anonymous List access provides the user full access to configure the specific list but no further access to other areas of the server.

6. Press the Login button.

6.3 Standard Page Layout

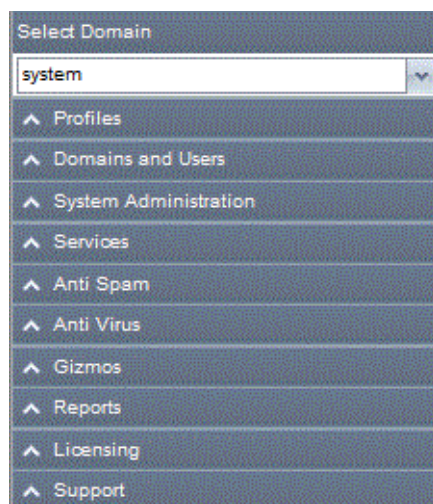
The screenshot below shows a typical GMS administration screen. In this case a user with administrator privileges has pressed the Account button on the toolbar, then selected the Forward page page:



You can customise the user interface. For details, see "Customising the User Interface" *GMS Reference Guide*.

The Control Panel

The left hand pane of the screen contains the Control Panel. The topmost part is common to all users and allows access to the items for the specific logged on account. The remainder of the panel will vary depending on the rights held by the logged on user. The remainder of the panel consists of a number of selectors which allow you to navigate through the available options. If an item in the panel is expandable it has a "^^" next to it. Simply click on the item to open it and reveal further options. The "^^" will then rotate through 180 degrees and items can be hidden again by clicking on the item. Additional products can be found under the Services item. If a particular product is not licensed, it will not appear in the list.



The Licensing node in the panel is for ordering Gordano products if you're using a trial version or adding additional products.

The Toolbar

Across the top of the screen is the tool bar. The tool bar contains a number of useful buttons. The first button allows you to check that you are running the most up to date version of the software. The "GMS WebMail" button will take you to the WebMail client if installed. The third button links to the online help. There is a help file for each dialog explaining what the features do. Next to this is the manuals icon. Clicking on this gives you access to pdf versions the Gordano manuals. The final button logs off your current session.

Some items within the Panel will also have secondary toolbar containing options specific to the functionality of the page.

Dialog Components

Within the dialog itself, you can use the following components to perform an action or to enter information:

- Radio button — where several options are alternatives, each has an adjacent radio button. Select the button next to the option you want.
- Check box — an option which simply has two states, selected and deselected, has a check box. If it's selected, there is a tick in the box. To select or deselect it, click on the box.
- Text box — this is a standard clear box for entering text. It may be a single line or a larger box, depending on the parameter concerned.
- Update button — selecting radio buttons, check boxes or entering text has no effect until you press the Update button at the end of the page, if there is one of these. Some complex entries have multiple pages, in which case the button at the bottom each page except the last page is named Next.

Status dialog

The status dialog allows you to see an overview of the status of GMS each time you log on. Once an option in the panel on the left is selected the Status dialog will be replaced with a screen pertinent to the option selected.

Status bar

Status messages and warnings are displayed in this area.

6.4 The Effect on the Interface of User Privileges

Depending on a user's level of privilege, the following actions are allowed:

- System administrator — has access to all the system areas and the option to contact Support.
- Domain administrator — in a multiple domain system, looks after one domain, adding users, creating domain profiles, etc. Has access to his user's area only.
- Log administrator — has access to the Logs area so can manage transaction and message logs.
- GMS Anti-Spam and GMS Anti-Virus administrator — has access to the GMS Anti-Spam and GMS Anti-Virus product areas so can manage all the features of those products.
- User — cannot perform any management tasks, so just has access to user areas (for details, refer to "What a Standard User Sees" on page 45).

The postmaster account has system, domain and logs administrative permissions.

Access to actions is controlled in three ways:

- If a product (for example, GMS Anti-Spam) is not licensed, its node in the panel is not visible.
- If a user is not permitted to perform a complete set of actions, the panel is not visible.
- If a user has access to just a subset of pages under a button, the tabs for the remaining pages are greyed out.

6.5 What a Standard User Sees

This section describes the user interface seen by users rather than administrators, and how this is changed by changing user options. Each of the features of the User Level administration interface are covered in the GMS User Guide.

User logon

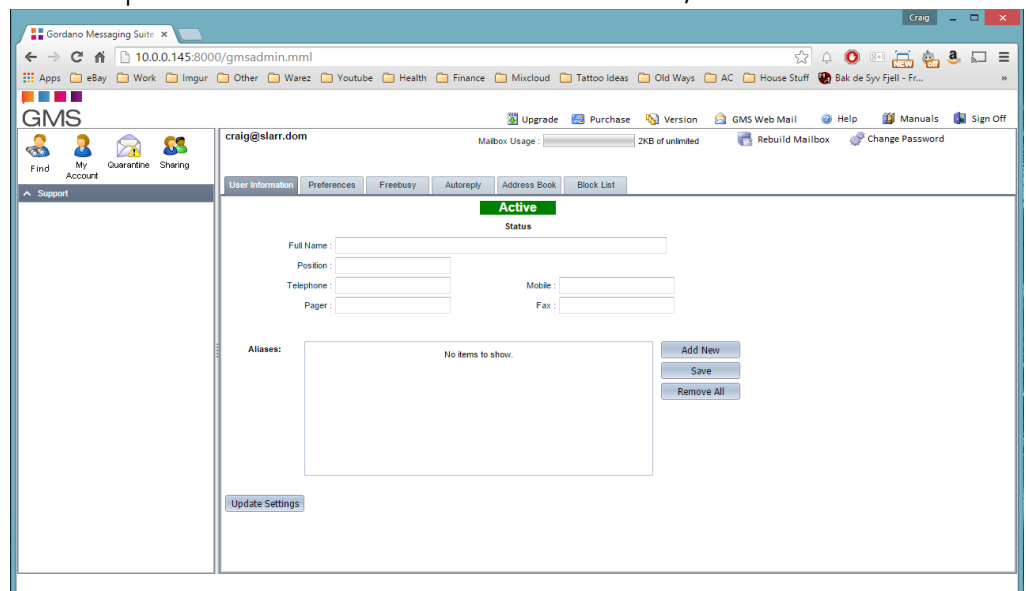
A user sees the same logon screen as shown for an administrator at the start of the chapter.

To log on the user must:

1. Type their name in the User name box. Unless specifically connecting to the IP address that the users domain runs on, they must use a fully qualified user name, so it is always best to get in the habit of using this format, for example "user@domain.dom".
2. Type their password in the Password box.
3. Select the required option from the Interface drop down menu. In this instance they have selected the Administration option.
4. Press the Login button.

Options

A user who has been given standard permissions will see far fewer options available than for an administrator, as shown here:



The main differences from the administrator screen shown earlier are:

- This user only has the Find, My Account, Quarantine, Sharing and Support options and GMS WebMail available via the Email icon in the product bar. (Note if the user required access to a GMS Communication Server list they could select the Anonymous List option when logging on in page 41).

- They have far fewer options in the panel. Of those which are shown above, the Find option may also be disabled by an administrator.
- On individual pages they may see more options unavailable (greyed out).
- They have no access to the Administration options in the panel, as shown in “The Effect on the Interface of User Privileges” on page 44

The individual user settings are fully described in the User Interface section of the GMS Users Guide.

7 Day-to-day Management

This section is for all administrators. It describes the main tasks you'll carry out on a regular basis. Operations like customising the user interface are described in the Domain Management chapter.

The following areas are covered here:

- Accounts overview.
- Managing accounts - includes adding multiple accounts and those from the NT SAM and LDAP/ADSI databases. It also covers alternative authentication methods.
- Account attributes - user robot accounts, DLL accounts, aliases, forwarding accounts and "moved" messages.
- Setting up Autoresponders.
- Groups overview - how to create groups, add members and post to a group.
- Managing Calendars
- Mailing all users in a domain.
- Maintaining logs - specifying log levels, configuring log handling, deleting/compressing and e-mailing a log, searching logs.
- Regular expressions

After making changes, we recommend that you make a setup.txt file for use in disaster recovery; see "Setting up the Recovery File" on page 345.

7.1 Accounts Overview

GMS delivers e-mail to accounts. Accounts have a set of attributes including a password and a creation date, and possibly an autoresponder, forwarding information, aliases, profiles etc. A user is a human who has access to an account.

Account information can be stored in several places such as an ADSI/UNIX or SQL database. Other options include LDAP and NT SAM. See "Authentication Options" on page 73 for more information.

7.2 Managing Accounts

This section describes the basic account operations.

Adding one or more accounts

As well as adding single users, you can add multiple users at one time.

If you are adding lots of employees to your mail system, try to use a systematic naming convention. For example, Brian Jones could be represented in any of these ways:

b.jones jonesb brian.jones jones-b brian brianj

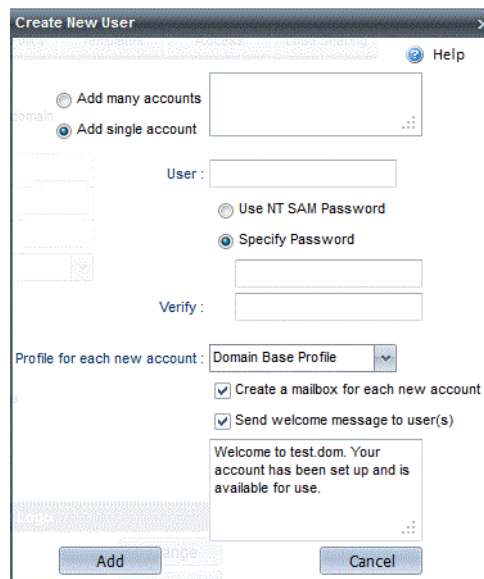


Set up an autoresponder for common names (for example, John), so people who e-mail the account in error have a list of correct e-mail addresses returned to them.

When choosing an account name, we recommend that you use numerals, letters, "." and "-" only. Although GMS can use other symbols correctly, other mail systems may not.

To add one or more new accounts:

1. Choose Domains & Users, select the domain you would like to add the user to, then press New User in the secondary toolbar to display this page:



2. To add a single account, select Add Single Account and enter the user name and password. For hints on creating passwords, see "Password policy" on page 172.
3. To add multiple accounts, select Add many accounts and enter the details for each user on a separate line in this format:

user-name,password[,real name[,account size in KB]]

For example, you might enter:

brianj,brian,Brian Jones,100

You can import from a database by cutting and pasting using the clipboard. When you have added all the accounts, press the Add button.



If you allocate simple passwords here, ask users to change these as soon as possible.

4. Select which profile you want the new user(s) to adopt from the drop down list. See "Profile Management" on page 99 for more information on Profiles.



If you are logged on as a domain administrator you will not be able to add a user with any of the system level profiles. i.e. You can only specify a profile that has been set up for the domain you are an administrator for.

5. If you want new users to receive a welcome message when they first log on, select this check box and type in your own message or use the pre-selected default message.
6. If you do not want a mailbox to be created for this account, deselect the Create Mailbox check box.

7. Press the Add button to create the new account(s).

Adding Accounts using mail.exe

Multiple accounts can also be added using the mail.exe program included with the Gordano install. For more information on this refer to the *GMS Reference Guide*.

Changing an accounts password

From time to time you may need to change the password of one of your users accounts. You can do this from the Domains & Users, Domain, Users page by pressing Change Password in the secondary toolbar, it is not necessary to know the current users password unless you are using the NT SAM database. Simply enter the new password for the user twice.

Emulating a user

From time to time you may need to edit a users personal settings. Perhaps they have set up sharing and need to change the settings but are unable to do so themselves for whatever reason.

You have the option to temporarily become that user even though you have logged on as an administrator. While acting as a user you will be able to see exactly what that user sees, including all of their GMS WebMail information, settings, email etc.

To switch into the user mode go to the Domains & Users, Domain, User page and select the user you wish to emulate then click on the **Switch with user** button in the secondary toolbar. You can then proceed to carry out any operation on that account you wish exactly as if you were the user themselves.

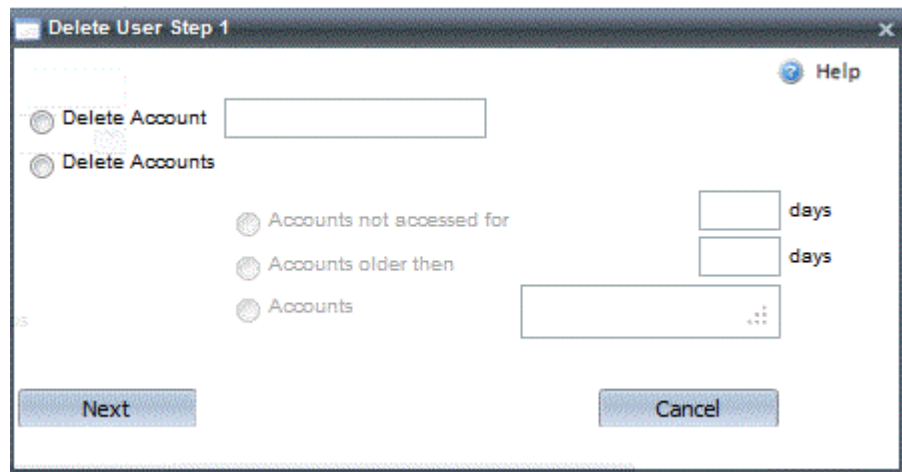
While emulating another user you will see a **Revert** button in the toolbar at the top of the screen in the administration interface. Clicking this at any time will revert you to the user you originally logged on as. If you are in the WebMail interface you will need to switch back to the admin interface in order to **Revert**.

Removing an account or obsolete accounts

You can remove all accounts which are of a certain age, or which have not been accessed for a specified time. You can specify whether their mailbox is left on the disk or is also deleted.

To delete one or more accounts:

1. Choose Domains & Users, select the domain you wish to remove users from and press Delete User in the secondary toolbar to display this dialog:



2. If you want to delete one account, select Delete Account and type the name of the account into the box. Press the Next button then press the Delete button.
3. If you want to delete obsolete accounts, select Delete Accounts and specify the account age or the time since the last access. Press the Next button and, when the accounts found are shown, remove any that you actually want to keep from the list. Press the Delete button to confirm deletion of those which remain in the list.
 - If you would like to delete multiple accounts at once, select the Delete Accounts option, then Accounts and enter a list of addresses, one per line, once they are all entered press the Next button to remove them.

7.3 Account Attributes

There are many account attributes, for example:

- An account can have a mailbox and a robot, allowing all e-mail sent to the robot to be saved in a mailbox.
- An account can have a mailbox and an autoresponder.
- An account may be an alias of another account, in which case any e-mail is delivered to both locations. GMS iterates e-mail addresses to a depth of five, so one forwarding account can forward to a second forwarding account.

This section looks at the different account attributes: user robots, DLLS, aliases, forwarding accounts, etc.

Robot accounts

A robot is a program which is started when e-mail arrives at the account. The robot may process the message and can generate a message for delivery to up to 100 e-mail addresses in return. Robots may be written by Gordano Ltd. or provided by other users. Check our Web site for information on robots currently available. Users cannot set up robots on their own accounts.



Another type of robot is the "domain robot" which accepts mail for an entire domain; see "Robot domains" on page 89.

See "Robots" in the *GMS Reference Guide* for example C code for a robot.



Some robots are provided free in the Gordano Accessory Pack.

To set up a robot account:

1. Choose Domains & Users, Domain and select the user (which you must already have added). Then select the Mail Processing tab, the Robots drop down list shows available robots.
2. If you want to run one of the listed robots, select it and press Configure. (Refer to each robot's documentation for details of what you need to do.)
3. If you want to set up a custom robot, select Custom and press Configure. Type in the command line to run and specify whether to send/accept messages to/from the robot, as follows:
 - Pass message to robot — only select this if the robot is going to use the header in some way.
 - Accept message from robot — the robot passes the message back after processing it. For example, it might post a response.
 - Sometimes — the server expects a message back from the robot, but does not post an error if it does not receive one.

4. Press the Update button to complete the account.

DLL accounts (*Windows only*)

A DLL is started by an e-mail message arriving at this type of account. Move any DLLs you want to use into the `Gordano\bin` directory. Users cannot set up DLLs on their own accounts.



The e-mail to fax DLL is provided free and, when used in conjunction with LGFax, allows e-mail messages to be faxed.

To set up a DLL account:

1. Choose Domains & Users, Domain, User then select the Mail Processing tab (you must already have added the user). The Select DLL list shows available DLLs.
2. If you want to run one of the listed DLLs, select it and press Configure.
3. If you want to set up a new DLL, select Custom and press Configure. Type in the full path of the DLL to run then press the Update button.

Mail Manager (*Windows only*)

GMS provides a Mail Manager DLL `ntmmgr.dll` that allows an email interface to some of the basic user functions, such as setting a users plan or holiday message.

To change his plan a user would send an email to the account containing their username and password followed by a blank line and then the text they want displayed in their plan, i.e.

```
plan <username>
password <userpassword>
<blank line>
This the plan for username
```

To remove an existing plan send

```
noplan <username>
password <userpassword>
```

Similarly to set an autoresponse message the user would send a message similar to

```
holiday <username> [responserate 1]
password <userpassword>
<blank line>
```

I will be on holiday until the 25th and will respond on my return.

The optional `responserate` variable dictates how often, in days, a response should be sent to a message arriving from a single sender. A value of 0 means that a response will be sent to every message arriving at the account.

To remove an existing autoresponder send

```
noholiday <username>
password <userpassword>
```

The mail manager can also be used to add entries for a user to the redirect file, i.e. it allows them to set their own filters as to who they want to receive mail messages from.

To block mail from an unwanted sender, send a message to the mail manager account

```
block user@domain.dom sender@other.dom  
password <userpassword>
```

This will set up an entry in the system redirect file similar to this

```
sender@other.dom * user@domain * T F "500 You are not allowed to mail  
this user"
```

To remove the block simply send

```
noblock user@domain.dom sender@other.dom  
password <userpassword>
```

List Manager (*Windows only*)

GMS provides a List manager DLL `ntlmgr.dll` that provides an email interface for list creation. You will need to have `GLCommunicator` or `GList` installed to create lists. Send a message with the following syntax to the account that you have set up to use the list manager DLL:

```
password <password>  
addlist  
domain <domain>  
listname <listname>  
joinaccess <joinaccess>  
listaccess <listaccess>  
postaccess <postaccess>  
listmanager <listmanager>  
[listowner <listowner>] (optional - sender used by default)  
members  
<user1@domain1>  
<user2@domain2>  
<user3@domain3>  
..  
<usern@domainn>
```

If you have entered the information correctly the list will be created and you will be sent a confirmation message. Refer to the GMS reference guide for information on the values that are valid for parameters such as `joinaccess`.

MML Scripts

There are two different methods in which MML scripts can be used under user accounts, Delivery and Post Delivery. Delivery Scripts act on mail as it is delivered to the account, they can interact with any stage of the SMTP process. Post Delivery Scripts can act on the message after it has been determined where it will be delivered to and just prior to it being written to the users mailbox. These

options can be configured from Domains & Users, Domain, User Mail Processing. For further information on the use of MML Scripts please see the MML Programmers Guide which is included in the GMS Accessory Pack.

Aliases

A user can have up to 20 aliases and multiple users can have the same alias. For example, if joe@test.dom and bill@test.dom both have the alias sales, they will both receive messages sent to sales@test.dom. Users can be denied the privilege to set their own aliases.

To set up an alias:

1. Choose Domains & Users, Domain, User, Account Information. The Aliases box shows their existing aliases.
2. Press the Add New button and type the new alias into the text area that appears and then press Enter to add it to the Alias list. Remember to press Save once you have entered all of the Aliases.
3. To remove an alias, select it and press the red cross next to the alias to remove it from the list. To remove all the user's aliases, press the Remove All button.
4. If you want to give other users the same alias, repeat steps 1 and 2 for each user.

Forwarding accounts

Mail messages can be forwarded automatically to a maximum of 20 alternative destinations, if required. This is useful when people leave the organisation or are temporarily located at another site, or if you want mail forwarded to a group of people, for example the Sales department. You can choose whether to let users set up their own forwards.

Note the following:

- Users can set up forwarding for their own account.
- E-mail can be forwarded to any valid e-mail address — it doesn't have to be in the local domain.
- One maildrop can be forwarded to many addresses — simply by repeating the steps below. (You could produce a small distribution list for your e-mails in this way.)

To set up a forwarding address:

1. Choose Domains & Users, Domain, User then select the Preferences tab and scroll down to the Forwarding section.
2. To add a new Forward press Add New and type the destination address into the text box (make sure you type the fully qualified user name). Then press Enter. Repeat for each entry.

3. Press the Save button to confirm all the entries made in Step 2.
4. To remove an address, select it and press the Red cross to remove it from the list. To remove all the addresses press the Remove All button.



Take care not to create a "forward loop" by forwarding to yourself.

If you let users set up their own forwards, warn them not to forward to themselves.

"Moved" messages

When a user's e-mail address becomes obsolete, for example when they leave the company, you can tell GMS to report an error response which is sent to anyone who mails the old address. This response can contain the user's new username and address.

No messages are accepted for the old account, whatever other attributes are set. Users cannot set moved messages on their own accounts.



This disables all other features of the account and displays the message at the protocol stage. No messages are accepted for the old account.

To set up a moved message:

1. Choose Domains & Users, Domain and select the user account in the list.
2. Select the "Move User" option from the secondary toolbar.
3. Type the message you want those who mail the user account to receive, then press the Move button.

If a user account is being moved within your organisation:

1. Choose Domain, Add User and add the user account with their new username.
2. If you want to forward messages sent to the old user account to the new user account, choose Domain, User, Preferences, Forward and enter the new user account and click Save. Then click on Update.
3. If you don't want both accounts to keep copies of messages select the old user account. Then choose the "Save nothing locally" option under Preferences, Mail Backup. Once you click on Update only the new user account will keep copies of messages sent to the old user account.

Autoresponders

An autoresponder sends a reply message to anyone who sends e-mail to its account. It can be used to reply automatically to mail messages sent to a user who is on holiday or to tell the sender that

their message is in a queue and will receive a full reply as soon as possible. Users can set up Autoresponders on their own accounts.

To make the autoresponder keep the original message, enable the mailbox. To discard messages, disable it. If the period value is non-zero, the autoresponder only replies once (per sender) during this period of time. If this value is 0, the autoresponder responds to all messages.

You can:

- Change the header of a message and use fields (Subject:, Date:, etc.) from the original message in the reply. For a complete list of header options, see "Template File Format" in the *GMS Reference Guide*.
- Set standard header fields for the message by selecting appropriate entries from the drop down lists.
- Send binary files that will be automatically encoded, MIME-compliant, e-mail messages. This is done by specifying the filename in the user variable called "Autoresponder". For details see the *GMS Reference Guide*.

☐ Send an automatic reply to incoming mail

Header Clauses :

From: %date% Add

☒ Only reply to each sender once in 1 days

☐ Start time Aug 20 2012

☐ End time Aug 20 2012

Update Settings

To set up an autoresponder:

1. Choose Domains & Users, Domain, User, Autoreply.
2. Select the "Send an automatic reply to incoming mail" checkbox.
3. Use the Header clauses window to amend a message header (probably the Subject), or to add new ones (probably the Sender).
4. Type the message you want to be sent.

5. Specify how often the message is to be sent (in days), or set the value as 0 to reply to all messages. If you are on a mailing list, set this to a high number.
6. Press the Update button.

7.4 Expiring Users

The Expiry option can be used to expire accounts in various ways.

Logon Expiry means that the user will no longer be able to access the account, however it will still continue to accept incoming mail. This is a useful feature in particular for ISPs whereby a customer can be denied access to an account while they have not paid their bill but the account can be re enabled at a later time without any loss of email at all. In addition to expiring access the mailbox the functionality of Autoresponders (holiday messages), quarantine and forwards can also be expired.

Account Information | Preferences | Autoreply | Quarantine | Mail Processing | Variables

Active
Status

User Name : three@test.dom

Full Name :

Position :

Telephone : Mobile :

Pager : Fax :

Account Expiry :

Logon Expiry :

☐ Expire mailbox

☐ Expire quarantine mailbox

☐ Expire forward

☐ Expire autoresponder

Account Profile : Domain Base Profile

☒ Licenced Account

Aliases :

No items to show.

Add New

Save

Remove All

The account expiry option will totally disable the account altogether, any incoming messages destined for the account will be rejected with a "550 No such maildrop defined" permanent error message.

To disable either Logon or Account access simply enter the date you wish this to take effect from, or use the date selector, and click on the **Update** button.

If you wish to re enable the account at a later time simply remove the date from the relevant text box and click on the **Update** button.

To expire an account with immediate effect click on the **Expire User** button in the secondary toolbar then on **Expire**.

7.5 Account Reports

The Report option allows you to collect information on an individual account including Email Addresses, Personalities, Servers and Mailboxes configured under the selected account. Each of the individual reports will show further information on the selected option.

Simply select the report you wish to run and click on the **Show** button to display the report details.

7.6 Maintaining Users Quarantine Folders

System and Domain administrators can access the Quarantine folder for each user on the system they have the permission level to see. Accessed from the Domain & Users, Domain, User, Quarantine page this provides a list of all messages in the folder and allows any of them to be Accepted or Deleted. Additionally the folder can be emptied completely of messages by clicking on the Delete All button.

If a message is accepted it is moved from the users quarantine folder to the users inbox.

7.7 Groups

GMS allows you to set up groups to which you can join users. When you send a message to a group every user that is a member of that group gets a copy of the message. For example every domain has a group called "Everyone" and all the users in the domain must belong to that group. So if a message is sent to everyone@company.dom then every user in the domain company.dom gets a copy. Groups can be very useful in company environments where different departments can have their own groups for example Sales@company.dom,

Managers@company.dom.



Groups can be password protected so that only users who know the password can post messages to them.

Domain and System Groups

You can have two levels of groups namely system groups and domain groups. It is not possible to create new system groups. Domain groups can only have members who are users in the same domain as the group. For example user@EnterpriseB.dom cannot be a member of the domain group support@company.dom



Each domain has a default group called "everyone". This group cannot be deleted and every user in the domain is a member of it. There is also a default system group called "allusers". This also cannot be deleted and every user on your system is a member of the "allusers" group.

Adding new groups

To add a new domain group select the domain you wish to work with from the Select Domain drop down and then select Groups. This will expand to list the groups and the right hand pane will also display a dialogue listing all the current groups in the selected domain. Clicking on the Add New button enables the area at the bottom of the screen where you can name the group and define who is allowed to send messages to it.

Group Name : @test.dom

Group May Receive Messages From

☐ No-one (Disabled)

☐ Any Group Member

☐ Anyone in this domain

☐ Anyone in this domain or System using password

☐ Any internal or External Account

☐ Any internal or External Account using password

☐ Include Forwarding in Email to this group

Update Settings

There are a number of options for limiting who can post to the group.

- **No-one** - means the group is disabled and cannot be emailed by anyone.
- **Any group member** - means only members of the group can post to it.
- **Anyone in this domain** - means any user who has an account in the domain that the group is in can post to the group members.
- **Anyone in the domain using the password** - If this is selected you can enter a password which must be provided on the first line of the message to the group. If this password is not present or the message is sent by a user outside the domain the message to the group will be rejected and a failure notification sent to the sender.
- **Any internal or external account** - If this is selected anyone from any domain is allowed to send a message to the group.
- **Any internal or external account using the password** - This option allows you to enter a password which must be provided on the first line of the message to the group. Anyone who provides the correct password will be able to post to the group whether they belong to the local domain or not.



If you limit post access to "Anyone with the password" anyone who wishes to post to the group must have

Password=group_password

on its own on the first line of the message they want to post. If the password is wrong or not present, group members won't receive anything and the sender will get a failure notification.

Include forwarding in email to this group

By default any forward account joined to a group will not receive a copy of any messages sent to the group. By forward account we mean any account that has at least one forward configured and which does not keep a copy of messages sent to it i.e. forward accounts which don't have a mailbox of their own. Checking this option will mean that forward accounts will receive copies of messages posted to the group.

Adding users to a group

To add users to the group select the group name from the list of groups in the menu on the left. This will display the settings for who can post to the group and allow you to move users into the group.

Highlight a user in the list of Users in Domain and click on > to add them to the group. Clicking on >> will add all of the users. To remove them highlight in the list of Users in Group and click on < or <<.

Click on the "Update" button when you have finished making changes. All new users in the group will be sent a welcome message informing them they have been added to the group and explaining to them how to post messages to the group.

Calendar Access

If your system has GMS WebOrganizer, each group has a calendar assigned to it. This calendar can be accessed by any accounts that

have been provided with access. This screen will allow you to enable specific users to access this groups calendar.

- **Add** - Clicking the **Add New** button will enable the options allowing you to specify the user or users who can access the calendar belonging to this group. The default access rights you can assign are:.

Read public - This right gives others the ability to see any events that you create with public access. They will not be able to see any private events or make any changes to your calendar.

Read private - This right gives others the ability to see any events that you create with public or private access. They will not be able to make any changes to your calendar.

Manage - This right gives others full control over your calendar. They will be able to see all your public and private events and are also able to edit the events to change times, details, alarms etc.

Custom - Once more familiar with access rights you may wish to use the Custom options to specify them more granularly.

- **Remove** - To remove a user from accessing this calendar you should highlight the specific account or accounts and click the **Remove** button.
- **Details** - To amend the access rights for a user or users, highlight the specific accounts and click the **Details** button. This will open a new screen enabling the current access rights to be amended.

Address Book Access

The steps undertaken here are identical to that of Calendar Access above.

Folder Access

The steps undertaken here are identical to that of Calendar Access above. The folder Inbox will be created automatically under the group account, and members of the group will be able to copy messages in to the folder. The Inbox will however be unable to accept incoming messages via SMTP.

Journal Access

The steps undertaken here are identical to that of Calendar Access above.

Notes Access

The steps undertaken here are identical to that of Calendar Access above.

Tasks Access

The steps undertaken here are identical to that of Calendar Access above.

Tasks Access

The steps undertaken here are identical to that of Calendar Access above.

Editing a group

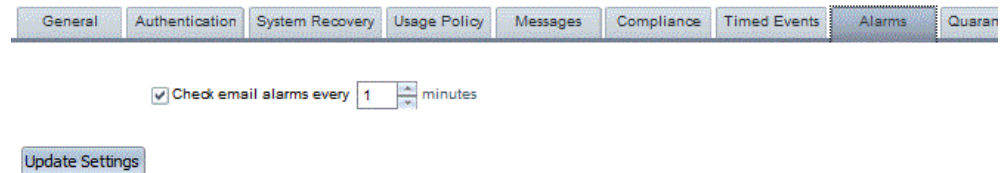
Editing a group is very similar to adding the group. Just click on the name of the group under "Groups" in the menu. A dialog similar to the one for adding groups will appear. You can then configure access and members in the same way as when you first added the group (see above). New members added in this way will receive a welcome message to let them know they have been added and explaining how to post to the group.

Deleting a group

Display the list of current groups by clicking on Groups in the menu then click on the group to be deleted in the list on the right. Next click on the "Delete" button and the group will be removed.

7.8 Manage Calendars

You may want to amend the frequency calendar events are checked for alarms. To do so go to System Administration, Settings, Alarms. This feature is available if GMS WebOrganizer has been installed. (See the *GMS User Guide* for more information on this feature)



General Authentication System Recovery Usage Policy Messages Compliance Timed Events **Alarms** Quarantine

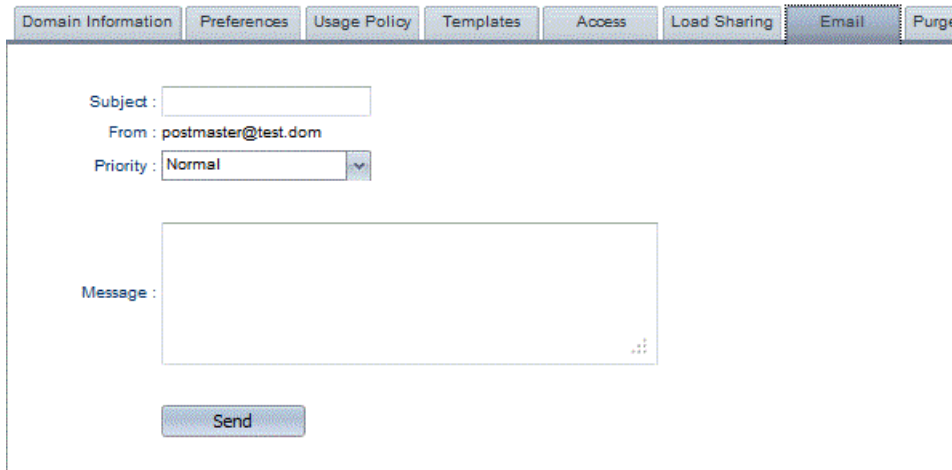
☒ Check email alarms every minutes

Update Settings

7.9 Mailing All Users in a Domain

You may want to send a message to everyone in a domain.

1. Choose Domains & Users, Domain and select the Email tab to display this page:



2. Select a priority, type in the message and subject then press Send.

If you wish to send a message to the bulk account from a traditional mail client simply send a message to everyone@<domain>. If access to the everyone group is restricted with a password you will need to type the password in the first line of the message. For example:

password=<grouppassword>
This is a message to everyone in a domain.

- There is a similar option under the System>Email tab that emails all users system wide.



If the right permissions are not set for the "everyone" group this tab will not be displayed.

7.10 Managing Logs

At a general level, GMS has two types of log:

- Message log — holds the contents of messages as a text file. These can automate recording of all communications, which you may need to comply with government and/or legal requirements.
- Transaction log — can be used to prove that e-mail has been received or delivered. Use transaction logs to fault find and to trace e-mail which is reported as lost.

At configurable intervals, logs can be compressed (zipped) and e-mailed offsite for backup archiving, then deleted. This prevents them filling the disk. GMS Archiver can automatically do this for you. GMS Archiver also allows you to search the offsite logs and retrieve any messages that match your search criteria. See "GMS Archiver" on page 307.

A separate log file is created for each service each day. The files are generally small (for example, a delivery log may take up only one MB a day for 1000 users).

Logs cover three separate areas:

- Domain — logs messages from or to users in this domain. These logs record email, instant messages and SMS messages. By default these logs are stored in the <\$path>\<Domain_name>\meslog directory.
- Transaction — SMTP, POST, POP3, IMAP, WWW, WebMail, Dialup, LIST, Manager, Messenger, Collaboration, SNMP and Dialup. By default these logs are stored in the <\$path>\log directory.
- Relay — logs messages from other servers relayed by this GMS server. By default these logs are stored in the <\$path>\meslog directory.

The transaction log for each service can log:

- Start/Stop — a time-stamped entry is made each time the service is started or stopped.
- All Failures — for example, the time when a remote connection dropped.
- Progress — general messages showing actions which happen.
- Statistics — details of all messages passing through the mail server.
- Protocol Logs — displays each action sent and received. This is useful for finding problems with mail clients.



Enabling full logging considerably increases the size of the log files but may be necessary to track properly what is happening to e-mail passing through the server.

In addition:

- POST can maintain logs of DNS Requests, showing the messages sent and received.
- SMTP can maintain logs of Redirection, showing when messages have been redirected by the entries in the redirect file.
- WWW and WebMail can produce parser logging. This is rarely used due to the large logs that it creates. It is usually only required if requested by Gordano Support personnel for debugging specific problems.

Specifying log levels

For each service, you can set the level of logging that is used. We recommend that for normal use you log Statistics and Failures only. If you experience problems with any of the services, turn on all the logging options for that service to get more information on what is happening.

To configure any logging option:

1. Choose System Administration, Logging, Transaction Logging to display this dialog:

	Progress	Statistics	Returns	Protocol	Anti-spam	DNS	Failures	Parser
SMTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	
POST	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	
POP3	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	
IMAP4	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	
LIST	<input type="checkbox"/>	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>	
WWW	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input type="checkbox"/>
Webmail	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	<input type="checkbox"/>
Dialup	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	
Manager	<input type="checkbox"/>	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>	
Messenger	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	
Collaboration	<input type="checkbox"/>	<input checked="" type="checkbox"/>		<input type="checkbox"/>			<input checked="" type="checkbox"/>	
SNMP	<input type="checkbox"/>	<input checked="" type="checkbox"/>					<input checked="" type="checkbox"/>	

☒ ZIP logs after days
☐ Email logs to after days
☒ Delete logs after days
 Maximum log directory in KBytes (Warn administrator)
 Minimum disk space in KBytes (Delete log files)

2. Click on the appropriate check boxes then press the Update button.

Configuring log handling

You can specify the frequency in days between zipping, e-mailing and deletion of a log on the above page too. To set the frequency of log deletion, compression and e-mailing:

1. If you want to keep logs on your system but zip the files to save space, select the "Zip Logs After" check box and specify the number of days after which they are to be zipped. Log files

- older than this are automatically placed in a zip file, but are not removed from your system.
2. If you want to e-mail logs off-site for safety, select "Email Logs to" and type the destination and the number of days after which they are to be sent.
 3. If you want to delete logs after a set time, select "Delete logs after" and type the number of days after which they are to be deleted. All logs older than this period will be deleted.
 4. Press the Update button.
 5. For a transaction log, choose the Transaction level page and for each service type specify what you want to log (see above).

Relay logs are configured under Relay Logging and to configure domain logs you need to go to Domain Administration, Logging after selecting the domain to work with from the drop down.

Disabling Domain and Relay logs.

To disable the domain message logs select the Domain from the drop down then Domain Administration, Logging. Select the Message Logging tab and un-check the "Log all messages through this domain" option for the required domain.

To disable the Relay Log navigate to the Support, System Variables page in the interface. Select the "LogAllMessages" variable from the "Select variable" box. Double click it to open it for editing then enter 0 as the "Variable Value" box then click on "Save". To enable the log again change the value back to 1.

Deleting, compressing or e-mailing a log

To delete, compress or e-mail a log immediately:

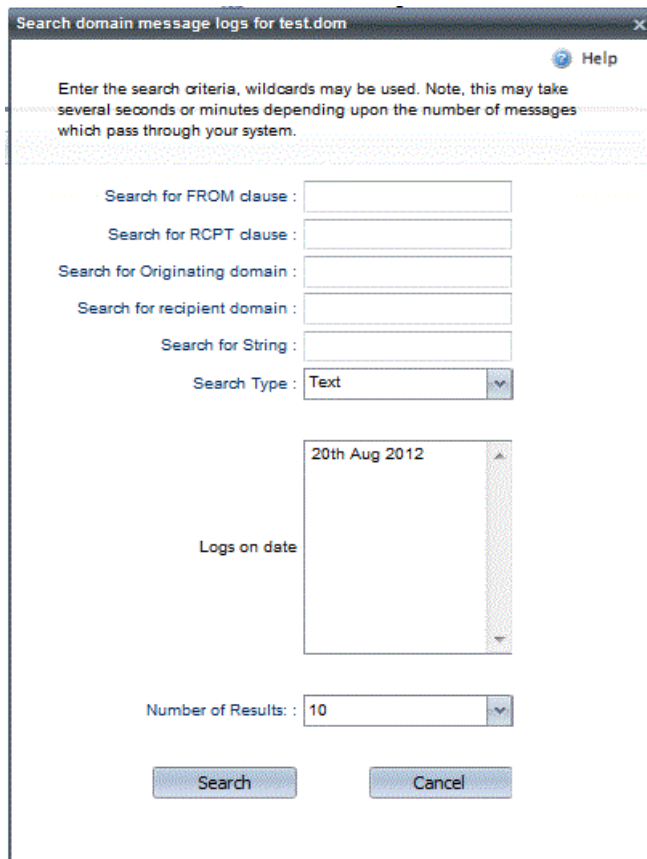
1. Choose the Logs you wish to work with from either the System or Domain Logs pages.
2. From the list of logs available, select the log you want to act on.
3. Choose Compress, Delete or E-mail to. If you're e-mailing the log, type the account to send it to.

Searching logs

The options are different for each log type, as described below.

To search a message log for an item:

1. Choose System Administration, Logging then Search Relay Logs from the secondary toolbar or to search the domain log Domain Administration, Logging then Search Domain Logs from the secondary toolbar. If there are no logs to search the button will be disabled. The page looks like this:



2. Specify as many search criteria from the following list as you need. You can use the wildcards "?" (one character) and "*" (any number of characters).
 - FROM clause — type the e-mail address of the message sender you are looking for.
 - RCPT clause — type the e-mail address of the message recipient you are looking for.
 - Originating domain — type the name of the domain messages originate from.
 - Recipient domain — type the name of the domain messages are sent to.
 - String — type a string which appears in a message.
3. Under "Logs on date", select the log files you want to search. Use CTRL+click if you want to select more than one log file to search, or SHIFT+click to select a group of log files.

4. If required, use the Number of Results value to restrict the number of results that are displayed.
5. Press the Search button.

To search a transaction log for a string:

1. Choose System Administration, Logging then Transaction Search from the secondary toolbar.
2. Specify whether to search incoming or outgoing messages for the string.
3. In the "Search for" text box, type in the string you are looking for. You can use the wildcards "?" (one character) and "*" (any number of characters).
4. Under "Logs on date", select the log files you want to search. Use CTRL+click if you want to select more than one log file to search, or SHIFT+click to select a group of log files.
5. If required, use the "Number of results" value to restrict the number of results that are displayed.
6. Press the Search Button.



Searching and retrieving messages from a message archive can be greatly simplified by using the GMS Archiver robot available from Gordano. Contact sales@gordano.com for further details.

7.11 Regular Expressions

There are many areas of this software where you will need to use IP addresses rather than domain names for entering information. Here, is an explanation the various ways in which IP addresses may be entered.

a.b.c.d	Specific IP address
a.b.c.*	All IP addresses beginning a.b.c
a.b.c.d-e	A range of IP addresses from d to e
a.b.c.d/n	Use first n bits

Note that a '!' may be placed at the beginning of the address to indicate NOT.

Examples

!194.194.194.194	NOT IP Address 194.194.194.194
194.194.194.*	Addresses in the range 194.194.194.0 -> 194.194.194.255
194.194.194.194/ 22	Addresses in the range 194.194.192.0 -> 194.194.195.255

194.194.192-195	As above
194.194.194.194/ 16	Addresses in the B Class range 194.194.0.0 -> 194.194.255.255

8 Authentication Options

GMS supports several authentication sources allowing you to store user data in the way that best suits your organisation. The options available are:

Windows:

- **GMS proprietary account database.**
GMS stores account information in the system Registry under the key HKEY_LOCAL_MACHINE\Software\InternetShopper. There is also an option to store the information in dat files under the <\$Path>Data directory.
- **Windows NT SAM (Systems Access Management) database.**
If an account is not in GMS' own user database, it can query Windows NT SAM database. GMS can read account information including user, password and home directory from the database. When you add an account to the NT SAM database, the user is automatically given an e-mail account and can use their NT password to collect e-mail.
You do not need to create these users within GMS itself. They can be placed in any mail domain, with the same account options as all other users. An NT SAM database user's mailbox is placed in their home directory (if user profiles are enabled).



NT SAM database users cannot use APOP logon.

Other sources (SQL, LDAP, ADSI)

GMS includes options to use SQL databases, LDAP and Microsoft Active Directory (ADSI). Full details are included in this chapter.

A custom database

- If an account is not in GMS' database, it queries the custom DLL, if this is configured. If the DLL reports that the account is valid, GMS uses the account. Custom DLLs are not supported by Gordano Ltd. — for information on writing these DLLs, see the *GMS Reference Guide*.
- Examples of custom DLLs include the Emerald authentication DLL that is developed by a third party for use with the Emerald ISP Management Suite.



If an account is not found, GMS delivers e-mail according to the “unknown user action” which is described in “Setting up an Unknown User Action” on page 93.

Linux, Solaris and AIX

- **GMS' account database.**
GMS stores account information in its own Configuration Database. This consists of a set of hidden files with the .reg file extension and which are stored in the same directory structure as the software and user's files (by default the /opt/gordano/mail directory and its sub-directories).
- **The Unix Database.**
This uses the UNIX database on the GMS machine for authenticating users.
- **A custom database.**
If an account is not in GMS' database, it queries the custom shared library, if this is present. If the shared library reports that the account is valid, GMS uses the account. Custom shared libraries are not supported by Gordano Ltd.

Other sources (SQL, LDAP)

- GMS includes options to use SQL databases and query LDAP servers including Active Directory.



If an account is not found, GMS delivers e-mail according to the "unknown user action" which is described in "Setting up an Unknown User Action" on page 93.

8.1 Authentication methods

As explained above GMS can authenticate users against a number of sources. These can be configured as follows:

1. Log on to GMS and select System Administration, Settings then select the Authentication tab on the right to display the following dialog.

General Authentication System Recovery Usage Policy Messages Compliance Timed Events

☒ Use Gordano's proprietary database current efficiency : 100 %

Please allow several minutes for the compact operation to work.
Your system will continue to be available for email services while this operation is carried out.

☐ Use NT SAM database

☐ Use external authentication database

Update Settings



On Linux, Solaris and AIX platforms "Use NT Sam database" is replaced with "Use UNIX account database".

2. If you want to enable the use of the NT SAM check the box next to that option and click on "Update". You will then need

- to configure each domain's settings separately. See "Using Windows ADSI for Authentication" on page 81 and "Using UNIX database accounts" on page 83.
3. If you want to use an external authentication database check that option and click on "Update" which will update the dialog to request some extra details
 4. You will be asked to choose an authentication method from the drop down. The options are:
 - MS ADSI authentication (*Windows only*) - Select this option and click on "Update". You will then need to configure each domain's settings separately. See "Using Windows ADSI for Authentication" on page 81.
 - LDAP authentication (also preferred for Active Directory) - Select this option and click on "Update". This displays the configuration options for LDAP. Enter any required details then click on "Update" again. See below for more information on the configuration parameters for LDAPAuth.
 - SQL authentication. - Select this option and click on "Update". This displays the configuration options for SQL. Enter any required changes then click on "Update" again. See below for more information on the configuration parameters for SQLAuth.
 - User defined authentication - If you select this option you also need to specify the location of the custom dll for windows or the custom authentication library for Unix that you intend to use. Use the full path name or if the dll or library is in the <\$path>bin directory you can just type the file name.

Once you have configured an authentication method you will need to stop and start all the Gordano services before the changes will take effect.

8.2 LDAP authentication configuration

Before LDAP can be used to authenticate usernames and passwords it must be set up on the GMS server. The first step in doing this is to enable the use of LDAP itself, once this is done the individual LDAP servers can be configured.



We recommend that LDAP authentication is also used when authenticating against an Active Directory server.

To enable the use of LDAP log onto the Administration interface and select System Administration, Settings then the Authentication tab on the right. On the right hand pane select the option "Use external authentication database" and click on **Update**. Next from the "Authentication method" drop down menu select the "LDAP Authentication" option then click on **Update**. Click **OK** to the

Popup warning you will need to restart the services, but do not restart them for now.



Note that on multi domain installations you can set up LDAP authentication details independently for each domain. If set at the system level the same authentication options will be used for all domains.

You will see a new dialogue appear on the same page that allows you to set up any number of LDAP servers against which to authenticate users. the process of adding LDAP servers at both the system and domain levels is identical so will only be explained once.

The option "Enable full user list mode" is selected by default. This allows caching of the user list on the GMS server and cuts down traffic between it and the LDAP server.

To add in a new LDAP server click on the **Add New** button. This will present you with a new dialogue allowing you to select the type of LDAP server you will use for authentication. There are a number of standard LDAP server types available by default, including GMS, Microsoft Exchange, Active Directory and Other. The latter of these provides the option to configure against any LDAP server including Lotus Notes/Domino and Novell Groupwise.

For the supported LDAP server types the only configuration required is the address of the LDAP server and the administrative password required for access to that server. Simply select the LDAP Serve type you wish to configure and click on the **Next** button. Selecting the option "Show advanced settings" allows LDAP authentication to be configured for more complex networks, this is explained immediately after the known server types.

Standard Parameters:

- **LDAP server** - Enter the address of the LDAP Server against which you want to authenticate.
- **Account name** - This is preconfigured to the default name of the administrator for your selected server type. If you are using a non default administrator replace the name with the appropriate one for your setup.
- **Account password** - The password for the Account name given above.

Advanced Parameters:

- **LDAP server** - Enter the address of the LDAP Server against which you want to authenticate.
- **LDAP port.** Default 389. - This is the port where LDAP responds on the LDAP server.
- **Use SSL** - If the LDAP server supports SSL and you wish to use it enable this option.

- **Account name** - This is preconfigured to the default name of the administrator for your selected server type. If you are using a non default administrator replace the name with the appropriate one for your setup.
- **Account password** - The password for the Account name given above.
- **LDAP Domain** - This is normally the same as the domain you use for email but may be different on complex networks.
- **LDAP timeout.** Default 20. - The max time the Gordano server will wait for a response (secs).
- **Reset connection count.** Default 100. The number of statements to be executed before resetting the connection to the LDAP server
- **SearchBase** - The searchbase specifies the base object for the search operation. The base object is the point in the LDAP tree at which you want to start searching. Its value is a Distinguished Name (DN). For example "ou=people, o=company.dom".
- **Filter.** Default is "(mail=%user@%domain)" - The filter is the criteria to be used during the search to determine which entries to return. This tells the LDAP server to check all records that occur in or below the searchbase that contain a parameter called "mail". The %user and %domain are dynamically substituted by the LDAPAuth.dll. So for example if user1@company.dom attempts to log on to a POP session then a search will be run to find a record that has a "mail" attribute that equals "user1@company.dom". Using the default requires your users to have an attribute called "mail" in their record in the format of user@domain. An alternative would be for your users to have two attributes, one called user and another called domain then have a filter of:
(&(user=%user) (domain=%domain))
- **Alias Filter** - Similar to the Filter setting above this is intended to allow access to users aliases or secondary email addresses. These will be displayed in the Aliases tab for the user within GMS but will not be editable from there. The configuration of this option is often more complicated than the Filter option above, as an example for Active Directory users you would use
(!(mail=%user@%domain)(proxyAddresses=SMTP:%user@%domain))
- **Email Attribute Name** Default "mail" - Each record that is to be authenticated against needs to have an attribute containing an email address.
- **Alias Attribute Name** No default as it depends on the LDAP server. Each record that is to be authenticated may have an attribute containing a list of additional email addresses associated with a primary email address. The name of the LDAP containing these should be provided here.
- **Password attribute name.** Default "password". - Each record that is to be authenticated against needs to have an attribute

containing a password. You could specify the "userpassword" attribute from the "person" object class. If you use the default "password" you may need to create a new object class and add an attribute called password to that object class. You will then need to add the new object class to all the records that you want to authenticate against and then add the "password" attribute to the records also.

- **Mailbox attribute name.** Default "mailbox". - As with the password attribute name each record needs to have an attribute containing the name of the user's mailbox (this is usually "inbox.mbx"). Gordano's default name for this attribute is "mailbox". Since none of Netscape's default object classes have an attribute called "mailbox" you will have to use another attribute such as "mailMessageStore" from the "mailRecipient" object class or create a new attribute called "mailbox". You will need to make sure each of the users that you want to authenticate has the attribute included in their record and that it has a value defined (default = "inbox.mbx").



Whenever you make any changes to these settings you will need to stop and start all of the Gordano services before they are applied.

Examples:

- AuthUser= " "
- AuthPassword= " "
- SearchBase= "ou=people, o=company.dom "
- Filter= "(mail=%user@%domain) "

Directory structure: company.dom\people. (Where the organisation(o) is company.dom, people is an organisational unit (ou) and your users have the organisational unit "people" in their record).

Values:

The values for each LDAP server you set up are held in a file called LDAP servers.txt within the root of the Gordano directory structure.

Implementation

The LDAP Authentication DLL implements:

- VerifyUser
- VerifyPassword
- GetMailboxName
- ChangePassword
- GetErrorMessage
- ListUser
- ListUserFree

Please see the Gordano Reference Guide for more information on the structure of authentication DLLs.



Note that if the user already exists in the Gordano's proprietary database then authentication will be made against the entry in the Gordano database and not the LDAP directory.

8.3 SQL authentication parameters

The configuration dialog shows a number of fields - the fields all have defaults except for "DSN name" which must be correctly set. This specifies the Data Source Name (DSN) that will link to the database containing the Gordano user account information.

Parameters:

- **DSN name.** - This is the Data Source Name to be connected to and must be specified. For Windows, DSNs are set up via the ODBC32 application in the Windows control panel.
- **User Name.** - This is the username associated with the DSN that may be required for authenticated access to the DSN.
- **Password.** - This is the password associated with the DSN that may be required for authenticated access to the DSN.
- **Verify an account exists.** - This is the SQL statement for verifying that a user exists. The default is:
`SELECT Address FROM Users WHERE Address = '%s@%s'`
The %s parts of the query signify items that are dynamically substituted. In this case the substitution of the first %s is the username and the second %s is the domain name of the user to be verified.
- **Authentication.** - This is the SQL statement for checking passwords. The default is:
`SELECT Password FROM Users WHERE Address = '%s@%s'`
As before the %s substitutions are for username and domain name respectively.
- **Obtaining mailbox name.** - This SQL statement retrieves the value of the Mailbox field from the database so the Gordano server knows what the user's mailbox is called. The default is:
`SELECT Mailbox FROM Users WHERE Address = '%s@%s'`
Once again the %s substitutions are for username and domain name respectively.
- **Change a user's password.** - This is the SQL statement to be used when changing a user's password. The default is:
`UPDATE Users SET Password = %s WHERE Address = %s@%s`
On this occasion the first %s is the dynamic substitution of the new password the table is to be updated with. The other two %s are for the username and domain name as before.

- **Listing users in a domain.** - This is the SQL statement that is used to display the users on the "Users" page in the Gordano interface. The default is:
`SELECT Address FROM Users WHERE Address LIKE '%%@%s'`
The %% in this query makes use of the % syntax in Structured Query Language. So if you were listing the users for the domain "company.dom" in the "Users" page of the interface, the query after substitution would actually be:
`SELECT Address FROM Users WHERE Address LIKE '%@CompanyA.dom'`
This would return a list of all users with an address that ends with "@company.dom"



Note: The Address field in the default statements above should contain full email addresses in the format user@domain.dom. The mailbox field should contain the name of the mailbox file for each user the default is "inbox.mbx"

Registry Values - Windows only:

Under /InternetShopper/Mail/SQLAuth

- AuthDSN
- AuthUser
- AuthPassword
- SQLVerifyUser
- SQLVerifyPassword
- SQLGetMailboxName
- SQLSetPassword
- SQLUserDomain

Implementation

The SQL Authentication DLL implements:

- VerifyUser
- VerifyPassword
- GetMailboxName
- ChangePassword
- GetErrorMessage



Note that if the user already exists in the Gordano's proprietary database then authentication will be made against the entry in the Gordano database and not the SQL database.

8.4 Using Windows ADSI for Authentication



With the release of Version 14 (Build 3509) of the Gordano Messaging Suite we now recommend that you use LDAP authentication in preference to ADSI Authentication.

To authenticate your users against Microsoft's Active Directory you first have to enable it at the system level by clicking on System Administration, Settings, Authentication in the GMS administration interface and selecting "MS ADSI Authentication" as the authentication method. You will then need to restart the GMS services for the change to take effect.

ADSI authentication can then be configured separately for each GMS domain. To set up ADSI for a domain select the domain from drop down then select Domain Administration, Settings and then click on the Authentication tab on the right.

This displays a dialog on the right of the screen allowing you to set up ADSI authentication.

Authorized user name

A user with access to the AD.

Authorized user password

Password for the above user.

Domains

A comma separated list of AD domains to authenticate against.

Security

There are four optional security options.

- **Secure authentication** - Requests secure authentication. When this option is checked Active Directory will use Kerberos, and possibly NTLM, to authenticate. When the user name and

password are NULL, ADSI binds to the object using the security context of the calling thread, which is either the security context of the user account under which GMS is running or of the client user account that the calling thread represents.

- **Use SSL** - The connection is encrypted using Secure Sockets Layer (SSL). Active Directory requires that the Certificate Server be installed on the machine that is being authenticated against to support SSL.
- **Use signing** - Verifies data integrity. The secure authentication option must also be checked to use signing.
- **Use sealing** - Encrypts data using Kerberos. The secure authentication option must also be checked to use sealing.

Once you have finished adding your settings click on Update to apply them. If you have entered valid details you will then be able to view a list of the AD users from the Domains & Users, Domain, Users branch of the administration menu. AD users can be recognised by the modified icon displayed next to their account name. In the following example the Administrator account is a user in the AD and the postmaster account is stored in the GMS proprietary database. If a user already has an entry in the GMS proprietary database this will take precedence over any AD entry for that user and authentication will be against the information in the GMS database.



Although the AD user is listed under the domain, an address book entry is not added to the webmail local addresses address book until the user has logged on for the first time.

8.5 Using Windows NT SAM database accounts

To use Windows NT SAM database accounts:

1. Create a User Group in the NT SAM database with the same name as the domain.
2. Add to the group all the users you want to have access to e-mail.



Do not add a user to more than one e-mail group.

3. In GMS go to System Administration, Settings then choose the Authentication tab on the right and select the option "Use NT Sam database". Click "Update". Now select your domain from the drop down and go to Domain Administration, Settings again choosing the Authentication tab.

4. The NT SAM authentication dialog will be displayed.



If a message is displayed saying that NT SAM authentication hasn't been set up you will need to select the system level authentication branch of the tree and check the "Use NT SAM database" option and click on update. Returning to the domain level Authentication will allow you to configure NT SAM usage for that domain.

5. Check the box "Use Windows NT SAM Database" and specify which of these three to use:
- Default domain on local machine in local or global group.
 - Default domain on machine — type the machine name.
 - Lookup in NT domains — enter a list of the domains. For example, if you were running GMS on a member server and authentication on several Primary Domain Controllers (PDCs), you would type here the list of domains handled by the PDCs.



If one machine runs GMS and another handles domains, the GMS machine must have read/write access to the disk on the other. To set this up you must enable null shares; see your Windows documentation for details or the Knowledge Base article on the Gordano website (<http://www.gordano.com/kb.htm?q=61>). Alternatively disable the "Allow NT Database Account Info" under System Administration, Security, Control in the interface

8.6 Using UNIX database accounts

To use UNIX database accounts:

1. Create a Group in the UNIX database with the same name as the domain.
2. Add to the group all the users you want to have access to e-mail.



Do not add a user to more than one e-mail group.

3. In GMS choose System Administration, Settings, Authentication and select the option "Use UNIX database". Click "Update". Select your domain from the drop down then Domain Administration, Domain Settings.

4. Select the Authentication tab on the right and the UNIX Database authentication dialog will appear.



If a message is displayed saying that no domain level authentication has been set up you will need to select the system level authentication again and check the "Use UNIX account database" option and click on update. Returning to the domain level Authentication to configure UNIX usage for that domain.

5. Check the box "Use UNIX User/Group Database" and specify which of these two to use:
 - Use default domain as group name.
 - Use specific group name — type the group name.

8.7 Authenticating against GMS from external sources

It is possible to configure external sources such as third party anti-virus and anti-spam software and devices to authenticate accounts against a GMS server. GMS provides an LDAP interface for this purpose. Please see the specific instructions for your software solution to configure this. The information you are likely to require from a GMS perspective is as follows.

- **GMS Server** - The address of the GMS server.
- **Account name** - An address with administrative rights within the GMS server. This is normally the postmaster account running on your primary domain. It is also necessary to specify the address book to query for the list of addresses. An example is
mail=postmaster@gordano.com,ou=gmsaddressbook
- **Account password** - the password for the account given above.
Search Base - the Search Base to use as the basis of your LDAP query. This would normally be as follows
mail=everyone@%domain,ou=gmsaddressbook
- **Filter** - The filter to apply to the results of the LDAP query to ensure only valid accounts are returned. This is normally as follows
(mail=%user@%domain)
- **Alias Filter** - You may also wish your query to return Alias accounts set up on the GMS server. For example the postmaster account also has aliases of hostmaster and root. In order to do this you need to also provide an alias filter which takes a different format to the standard Filter as follows
(!(mail=%user@%domain)(amp(mail=%*@%domain)(gmsAlias=%user)))

9 Domain Management

This section is for administrators who want to use the full capabilities of GMS domains. It describes:

- Types of domain — full, virtual, POP, robot and alias domains. The advantages and disadvantages of using each type are given.
- Adding domains — setting up MX records, domain parameters, aliases and the Unknown User action.
- Domain maintenance — listing, checking and deleting domains, limiting message sizes, archiving and customising the user interface for a domain.

You can give responsibility for managing a domain to a domain administrator; see “Delegating Domain administration” on page 110.



If you use more than one domain, you must set up MX records in your DNS individually for each.

9.1 Types of Domain

Full domains

A full domain has an IP address. It is a complete domain with accounts, list servers, auto responders etc. that are self-contained and independent of any other supported domain.

As far as the mail users in the domain are concerned, they are using their own mail server — they will not be able to find out the name of any other domains on the mail server. Where two companies share the same machine for all their e-mail, as far as the rest of the world is aware they use different machines.

Multiple domains affect the SMTP server and POP3 server differently:

- POP3 was not designed to support multiple domains on one mail server so GMS provides multiple domains by using a separate IP address for each. To support four domains you need four IP addresses. GMS can then work out which domain a POP user belongs to.
- SMTP divides out the e-mail based upon the domain name in the e-mail message - not the IP address the e-mail arrived on.

Setting up a full domain involves these steps:

1. Adding a new IP address to your machine.
2. Updating your DNS for the new domain.
3. Creating the domain in GMS.
4. Adding users to the domain.

The advantages of full domains are:

- Each is a completely separate domain (on disk, in the Registry or Unix Configuration file, etc.). The outside world need never know there is actually one machine supporting more than one e-mail domain.
- Each domain name can have lists and list servers.
- Message logs are separate and separately controllable.
- Individual members of a domain can collect mail independently.
- All user accounts in the NT User Database or Unix Database may be split across multiple domains.
- Administration of the domain — adding users, lists, forwarding etc. — can be delegated.

Full domains have one disadvantage — IP Addresses must be statically allocated to domains, so one IP address is required for each domain.

Virtual domains

A virtual domain *piggy backs* on a full domain. GMS creates users under the full domain but appends a postfix to the username so that identical user accounts in two different domains will not exist. This postfix is defined when you create the virtual domain.

The postfix can also be used when connecting to the POP3 server to download messages. For example, if you have an account joe in a virtual domain called "company.dom", with a postfix of "company", created under the full domain "isp.dom":

- email can be sent to joe@company.dom.
- but email must be collected from joe.company@isp.dom or joe@company.dom. This means that when you set up your account details in your POP3 or IMAP client you should specify the username as one of the following
 - joe.company
 - joe@company.dom
 - joe.company@isp.dom

The advantages of using virtual domains are:

- It reduces the number of IP addresses used.
- You can delegate domain administration.
- You can distinguish between addresses like the following, whereas with domain aliases these two appear to be the same:

user@company1.dom
user@company2.dom

The disadvantages are:

- Messages are logged in the host domain's message log.

- A virtual domain is only one domain with aliases so there is only one "Unknown User" account option. This could mean that one company's postmaster sees e-mail intended for the other company.
- Users must remember to log into the POP account using the extended account name (sales.company1), even though their user name is sales.

POP domains

A POP domain is an account where all the mail for all users in that domain is placed into a single POP3 mailbox. All the mail is mixed together for later separation using a utility such as Autodial or GMS. Each message placed in the POP domain account will have two additional clauses added to the header:

- X-Originally-To: — this contains the destination e-mail address and should be used to deliver the e-mail to the correct destination. Note that the e-mail address specified may not necessarily be in the "To:" or "Cc:" clauses (e.g. List mail, Bcc'ed e-mail).
- X-Originally-From: — this contains the e-mail address that the message is from. Again, this may not be the same as the "From:" clause (for example, List mail).



You must use the "X-Originally-To" clause to separate your e-mail. If you use the "To:" clause, you will see several effects:

- mail delivered to the wrong person
- people getting two copies of messages
- messages posted back into mailing lists.

GMS on a remote site can log into an ISP's GMS and collect mail from a POP domain account. This gives that site complete e-mail access, as if they were permanently connected to the Internet - they can use executables, lists, autoresponders, POP accounts, etc.

The advantages of POP domains are:

- An extra IP address is not required for each domain.
- Administration of mail is easier since new accounts only need to be added at the server downloading the POP domain's e-mail.
- GMS on a remote system allows the provider to use DHCP for all customers so fixed IP addresses can be avoided.
- All the mail for a given domain can be downloaded in one transaction from any of the server's IP addresses.
- Mail logging can be carried out by the destination rather than the source machine.
- The NT user or Unix databases are not used.

The disadvantages of POP domains are:

- Individual users cannot download their mail, leaving other mail for download later.
- You have no control over the number of users in the domain.

Robot domains

A robot domain is a domain where an application program is started by an e-mail message arriving for any address in the domain. A program which operates in this way is called a domain robot (as opposed to a user robot). This is extremely useful if you want to trigger a program remotely by sending e-mail to the appropriate domain. When the message is received the specified program starts.

This can be used for a "fake domain" where an executable needs the account name for further processing of the incoming e-mail (for example an e-mail to news gateway). A typical use of a domain robot is to take all mail arriving for users in the domain and forward it to the same users in a different domain.

You can give the executable access to the e-mail contents via the standard input and output streams if the 'Send message to Robot' and/or 'Accept message from Robot' check boxes are selected (see below).

For example code for an executable program, see "Robots" in the *GMS Reference Guide*.

Alias domains

GMS lets you have many aliases for any other domain already on the system.

For example, if you are using the full domain abcd.myisp.net and then purchase the domain abcd.dom, you can simply tell GMS that abcd.dom is an alias of abcd.myisp.net. This means that sales@abcd.myisp.net and sales@abcd.dom are the same account.

You can set up any number of aliases in this way.

9.2 Adding a Domain

There are four steps to setting up a domain, as follows.

Setting up MX records

Mail Exchange information is held by the DNS as MX records in this form:

```
company1.dom.  IN MX 10 smtp.company1.dom.  
               IN MX 20 mx.isp.dom.
```

Providing setup information for all the varieties of DNS software is beyond the scope of this guide, but for more information, see the book *DNS and Bind* by Paul Albitz & Cricket Li, published by O'Reilly & Associates, Inc. (For purchase information see www.ora.com.)

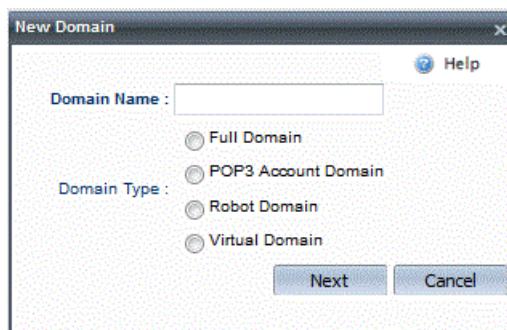
Setting up domain parameters

Follow the instructions below for the type of domain you want to set up.

Full Domain

To add a full domain:

1. Choose Domains & Users then click on New Domain in the secondary toolbar to display this page:



2. Type in the domain name and select the type Full domain. Press the Next button.
3. Specify the postmaster's password for the new domain.
4. Select the domain's IP address in the list.
5. Enter the company details and press the Save button.



To create sub domains of your primary domain. For example

Primary domain - CompanyA.dom

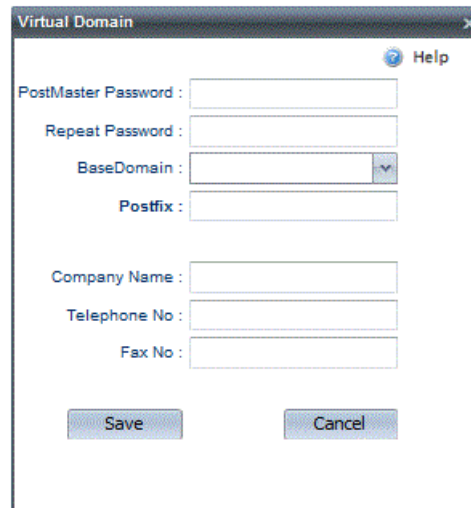
Sub domain - Sales.CompanyA.dom

*You must first remove the domain alias *.CompanyA.dom created by default when the primary domain was created.*

Virtual Domain

To set up a virtual domain:

1. Choose Domains & Users then New Domain in the secondary toolbar (this displays the page shown above).
2. Type in the domain name and select the type Virtual domain. Press the Next button to display this page:

A screenshot of a software window titled "Virtual Domain". The window contains several input fields: "PostMaster Password" and "Repeat Password" (both text boxes), "BaseDomain" (a text box with a dropdown arrow), "Postfix" (a text box), "Company Name" (a text box), "Telephone No" (a text box), and "Fax No" (a text box). At the bottom of the window are two buttons: "Save" and "Cancel". A "Help" icon is located in the top right corner of the window.

3. Specify the postmaster's password for the new domain.
4. Select the base domain name in the list, then the postfix to use (see above).
5. Enter the company details and press the Save button.

For details of how to set up POP clients for users, see "E-mail Clients" on page 215.

POP Domain

To set up a POP domain:

1. Choose Domains & Users then New Domain in the secondary toolbar.
2. Type in the domain name and select the type POP3 account domain. Press the Next button.
3. Specify the postmaster's password for the new domain.
4. Enter the company details and press the Save button.



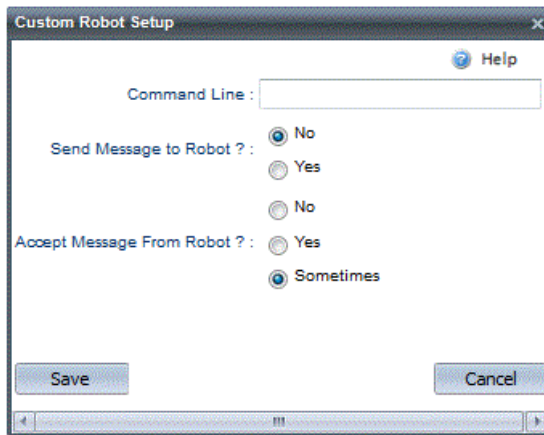
To collect mail, the system collecting mail can log on to any IP address of your mail server, with a username the same as the domain name. The password will be that which you defined when you set up the domain.

Robot Domain

To set up a robot domain:

1. Choose Domains & Users then New Domain in the secondary toolbar.

2. Type in the domain name and select Robot, then press the Next button. From the following page either select an existing robot from the drop down list or select Custom and press the Configure button to display this page:



3. Type in the command line to run and specify whether to send/accept messages to/from the robot. You have three choices:
 - Send message to robot — only select Yes here if the robot is going to use the message header in some way.
 - Accept message from robot — the robot passes the message back after processing it. For example, it might post a response.
 - Sometimes — the server expects a message back from the robot, but does not post an error if it does not receive one.
4. Click the Save button.

Setting up domain aliases

Use domain aliases when you want a domain to accept mail for more than one domain. When you set up a domain, domain aliases are added to the list of local domain names.

Domains can have unlimited aliases and wild cards are supported. To set up an alias:

1. Choose Domains & Users, Domain then select the Domain Information tab and scroll down until you see Domain Aliases. Any existing aliases will be displayed in the box.
2. To add a new Alias click on Add New and type the new alias into the text area then press Enter. Press the Save button once you have completed adding new aliases.
3. To remove an alias, select it and press the Remove button to remove it from the list. To remove all the aliases, press the Remove All button.

Setting up an Unknown User Action

The Unknown User Action is a very powerful feature of GMS. You can use it to:

- *Chain* mail servers together (perhaps across sites).
- Catch mail delivered to an incorrect address.
- Inform users of the correct address to e-mail.
- Let mail servers share management of the same domain. That is, run poweruser accounts on GMS and others on MS Exchange.

See "GMS on Complex Networks" on page 189 for examples of how this feature can be used.

To set up the Unknown User Action:

1. Choose Domains & Users, Domain then the Preferences tab on the right. The relevant part of the page looks like this:

Domain Information Preferences Usage Policy Templates Access Load Sh

☐ Delete undeliverable mail after days

Insert X-info into each message with text

SMTP forward mode

☒ Use sender envelope

☐ Use recipient envelope

Unknown User Action

☐ Fail to account

☐ Redirect to server

☒ Reject the mail

☐ Transfer to account

☐ Accept and return failure message

☐ Accept and quarantine message

☐ Accept and discard message

No such mail drop defined

2. Under Unknown User Action, select one of the following:
 - Fail to Account — The message is accepted by the server, a fault report is generated and the e-mail message is added as a MIME attachment. This is then sent to the named account.
 - Redirect to server — Send the message on to the specified server. You may use this if you use GMS as a firewall passing all mail on to an internal server.
 - Reject the mail — The mail message is rejected and the sending server must return it to the originator of the message.

- Transfer to user account — The message is accepted by the server and transferred to the specified account without making any changes to it.
- Accept and return failure message — The message is accepted and the sender receives a message indicating delivery has failed.
- Accept and quarantine message — The message is accepted but placed in the domain level quarantine folder. No error is returned.
- Accept and discard message — The message is accepted and silently thrown away. No error is returned.

9.3 Maintaining Domains

The tasks in this section apply to all domain types. For guidance on adding a domain of each type, see the relevant section above.

Listing domains

All of the domains are listed under Domains & Users in the menu for you.

Checking domains

You can check a domain's MX records and IP address.

To check a domain:

1. Choose Domains & Users, Domain then Check Domain in the secondary toolbar.
2. Select the check box(es) for the type of check you want to run.
3. Press the Check button

Deleting domains

If you remove a domain from GMS, any users in it will no longer receive any mail. To remove a domain, choose Domains & Users then click on the Delete Domain button next to the domain you wish to delete, press the Next button, then confirm the deletion by pressing the Delete button.

Configuring account size limits and archiving

The account size limits control the size of incoming messages, account size, number of folders and inbox size. By default these are set to 0, which means there are no limits. If you have limited disk space or bandwidth, you may want to impose limits for the domain.

To impose an account size limit:

1. Select the domain from the drop down and select the Profiles option.
2. Select the "Domain Base Profile" and click on the Account Settings tab on the right.
3. Type the values you want for each limit.
4. Press the Update button.



System Administrators can set these limits to any figure. Domain administrators cannot set any limits that exceed the limits set in the system base profile.

Purging domain e-mail

You can automatically clear out old e-mail, making the best use of your disk space. This is useful if many users either never read their e-mail or leave it on the server.

To purge old messages for the domain:

1. Choose Domains & Users, Domain then select the Purge Settings tab on the right.
2. If you would like the purge to run automatically at regular intervals enter the period in days at which the purge should be run. If you don't want it to run automatically enter 0 (zero).
3. In the "Delete messages older than" box, specify the age of messages to be deleted.
4. Select the folders that you would like the purge to operate on.
5. If you only want to delete messages which users have actually read, select the "Only read messages" check box.
6. Press the Update button to remove messages matching the above criteria according to the defined schedule.
7. If you would like to purge the messages immediately use the Purge Now option in the secondary toolbar.

Advertising/customising the user interface

You can change the user interface in several ways:

- Adding a footer to all messages in a domain. You can use this to advertise services, as a disclaimer, etc.
- Replacing with new HTML text the default support page which appears when a user chooses Support. You can do this for a single domain or for the whole system. See "Customising the User Interface" in the *GMS Reference Guide*.

To add your own messages to footers:

1. Choose Domains & Users, Domain and then select the Templates tab on the right.

2. Select the "Add footer to bottom of each message" check box, type the message in the Footer area in plain text. You may also add an HTML Footer for use with HTML formatted messages.
3. Select whether the footer should be applied to external mail, internal mail or all mail and press the Update button.

Domain welcome message

When new user accounts are added using the Domains & Users, Domain, New User option you are given the option to send a welcome message to each of the accounts. You can either type a unique message for each user when adding them or you can define a message for all users added to a particular domain. The welcome message used for each domain is set from the Domains & Users, Domain, Templates page. Simply type your message in the space provided. Once you have completed your changes click on the Update button to apply them.

Access

Access to both the administration and WebMail interfaces can be restricted by IP address, if you prefer you can simply use whatever is set at the system level under System Administration, Security, Access Control, or you can enter specific settings for each individual domain on the system under Domains & Users, Domain, Access. By default, all IP addresses are allowed to access the interfaces.

If you do decide to restrict access to either of the interfaces please ensure that you add your own IP address to the list prior to clicking on the **Update** button, otherwise you will be immediately thrown out of the system.

Usage Policy

Each domain on the system may have its own Acceptable Usage Policy set under Domains & Users, Domain, Usage Policy. This will be displayed to users when they first connect to the mail server and should outline the companies policy on email usage.

It is good practice for every company to develop an acceptable use policy for email in the event that abuse of the email system takes place. Any legal argument ensuing from this abuse is much easier to defend if such a policy exists.

Interfaces

This option allows you to specify the default interface that is presented to your users, as well as which interface options are available to them for selection from the drop down menu on the

logon page. The interfaces are configured under Domains & Users, Domain, Preferences.

Email

An Email can be sent to all of the users within your domain from the Domains & Users, Domain, Email page. This makes use of the underlying "allusers" group which is created during a standard installation, or when each new domain is created.

If this tab is unavailable (or greyed out) it will be due to the fact that you have not yet enabled this group to accept posts. See "Groups" on page 60 for further information.

10 Profile Management

This section is for all administrators. It describes the main tasks you'll carry out when configuring Profiles.

GMS allows you to create different user profiles. For example you may want a group of your users to have special privileges such as a larger mailbox size and access to their account via GMS WebMail. To do this you would set up a new profile with those attributes enabled and assign that profile to your privileged users. In a similar way you can reduce limits and access rights for other groups of users.



Each Domain has a default profile called the "Domain Base Profile". This can be edited to suit your requirements or you can clone new profiles

10.1 Domain and System Profiles Overview

You can have both system and domain profiles. System profiles can be applied to any user in any domain by a system administrator. Domain profiles however are unique to users in the domain for which that profile has been created. This allows administrators of individual domains to choose their own profile policies. Domain administrators who do not have system rights can only create users with a domain profile belonging to the domain they are an administrator for.

You can view the profiles that are currently set up by selecting Profiles from the menu on the left. You will see a display similar to the one below.

Profiles

Profile Name	Allow All Domain Access	Default		
Administrator Profile	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
System Base Profile	<input type="checkbox"/>	<input type="checkbox"/>		

Applied to:

postmaster@test.dom

This is the view as seen by a system administrator. If you log on with only Domain administration rights you would not have the option for "Allow all domain Access" and of course the profile names themselves would be different.

10.2 Making a new profile

The above picture shows the list of Profiles available by default at the system level. At present there just two profiles, note that one has been selected as the default profile. There can only ever be one default at each of the System and Domain levels.

It is not possible to create a new profile from nothing so you need to select which profile you want to "Clone" (Copy). Click on the profile name in the list then click on the Clone icon on the far left of the grid. This will open up a new dialogue where you should type a name for the new profile in the box and then click on OK. You will now have a new profile that is an exact copy of the one you originally selected. The next thing you will want to do is to edit your new profile. This is explained below.

10.3 Editing Profiles

To edit a profile first select Profiles in the menu and then the new profile you just created. This will display the following, each of the options are described fully below.

The screenshot displays the 'Profile Management' interface with several tabs at the top: Account Settings, Access Rights, Configuration Rights, Privileges, Preferences, and Users. The 'Account Settings' tab is active, showing the following configuration options:

- Maximum message size:** Radio buttons for 'Use maximum' (selected) and 'Set to' (with a text input field). The value '(No limit) KB' is displayed next to the 'Use maximum' option.
- Maximum folder size:** Radio buttons for 'Use maximum' (selected) and 'Set to' (with a text input field). The value '(No limit) KB' is displayed next to the 'Use maximum' option.
- Maximum size of account:** Radio buttons for 'Use maximum' (selected) and 'Set to' (with a text input field). The value '(No limit) KB' is displayed next to the 'Use maximum' option.
- Maximum number of folders:** Radio buttons for 'Use maximum' (selected) and 'Set to' (with a text input field). The value '(No limit)' is displayed next to the 'Use maximum' option.
- Starting language:** A dropdown menu currently set to 'English(United States)'.

At the bottom, there are two list boxes for group management:

- Non-member Groups:** Contains the entry 'testgroup'.
- Member group(s):** Displays 'No items to show.'

Navigation buttons (>, >>, <, <<) are located between the two list boxes. An 'Update Settings' button is positioned at the bottom left of the form.

Account Settings

Clicking on the Account Settings tab for a profile allows you to set one or more of the following account parameters:

- Maximum Message size — the size of a single message arriving at the account.
- Maximum Folder size — the maximum size that any one user folder is allowed to grow to.
- Maximum size of account — the maximum disk space for all the user's mailboxes/folders (IMAP and GMS WebMail lets users create multiple mailboxes/folders)
- Maximum number of folders — the maximum number of IMAP/Webmail folders the user is allowed to have in their account.
- Minimum mail refresh interval "x" minutes - This setting controls the minimum frequency a GMS WebMail mailbox can be refreshed, hence reduces the resources used by users who check their mail too frequently.
- Starting Language — this is the language a new user will start with when they access their GMS WebMail account for the first time.
- Groups — you can select the groups that new users with this profile will be a member of. This option is not available in system profiles since you can not add groups at the system level.

If the folder size exceeds 90% of the allowed size the user will receive a warning email suggesting that they free up some space within the folder.



A domain administrator cannot apply any maximums that exceed the system settings in the System Base Profile.

Access Rights - setting user access rights

Clicking on the Access Rights tab for a profile allows you to define what access rights are given to users that have that profile. The options are as follows:

- Allow this account to access Email — having this option checked allows the user to access their mailbox.
- Allow this account to access Email using POP3 — having this option checked allows the user to download their messages using a POP3 client.
- Allow this account to access Email using IMAP4 — having this option checked allows the user to download their messages using an IMAP4 client.

- Allow this account to access Email using WWW — having this option checked allows the user to view their messages in WebMail.
- May configure software from anywhere — having this option checked allows the user to access the configuration server from any IP address.
- GMS WebMail access from anywhere — having this option checked allows the user to access the GMS WebMail client from any IP address.
- Password Control — the password control options allow you to define how often passwords should expire.



GMS WebMail as a stand alone server does not contain POP3 or IMAP services. To enable POP3 and IMAP mail collection GMS Mail must also be installed.

Configuration Rights - Setting configuration access

Clicking on the Configuration Rights tab for a profile allows you to define how much access users with this profile will have to the GMS configuration pages.

- Domain Access — by checking the “User may administer his own domain” option you can allow users with the selected profile to administer their own domain. Domain administrators can add users to the domain, and can set up domain profiles. Any profiles set up by a domain administrator cannot exceed any limits set up in the profile that the domain administrator belongs to. If you don’t want the domain administrators to have full domain access you can un-check any of the individual privileges such as “manage GMS Anti-Spam and GMS Anti-Virus”. If you wish to allow the user or users assigned to this profile to manage other domains you can select the option “User may administer domains” and enter a space separated list of the domains this is applied to.
- System Access — by checking the “Manage complete system” option you will allow the users with the selected profile to access any part of the Configuration interface.
- Logs Access — by checking the “Manage system logs” option you will allow the users access to the transaction, relay and message logs for all domains on the system.
- GMS Anti-Spam and GMS Anti-Virus access — by checking the “Manage GMS Anti-Spam and GMS Anti-Virus for all domains” option you will allow the users to access and configure the GMS Anti-Spam and Virus modules that can be installed with GMS.

Privileges - setting user privileges

Clicking on the Privileges tab for a profile allows you to define what privileges users with that profile should have. There are six sections:

General

- Change password — if this option is checked users with this profile will be able to change their own password whenever they wish. If you have set an expiry period under the "Access" menu (see above) this will still apply.
- Alter their forwards — checking this option allows users to add and change their forwards.
- Set a vacation or automatic response — setting this allows the users to set up an autoresponder which is often useful for letting people know that a user will not be viewing his mail for a time.
- Set their plan — a user's plan is a section of text which is returned in response to the finger command or a search with the "Find" option. By checking this option you allow the users to edit their plans. A default plan is blank.
- Change their personal details — Each account can store a number of details about the user such as full name position etc. If you enable this option users will be allowed to edit or add to their personal details.
- Add aliases — aliases are very useful if you want to have two personas but only want to check one mailbox for mail. Checking this option allows users to add their own aliases.
- Rebuild their mailbox — occasionally it may be necessary to rebuild a mailbox, perhaps if it has become corrupted somehow. Checking this option allows the users to do this themselves. Note that rebuilding a mailbox sets all your messages to the un-read state.
- Search users - if enabled this allows all users belonging to this profile to search for other users using the **Find** option.
- Send email externally - enabled by default allows users to send external email through the server, if disabled users will only be able to send email to local users.
- Send email externally if in personal address books - only allow the users to send external email if the recipient of the email exists in the users personal address books.
- Send external email if in shared address books - only allow the users to send external email if the recipient of the email exists in any address book the sender has access to.
- Receive external email - allows the user to receive email from an external sender, if unchecked users will only be able to receive email from local senders.

- Receive external email if in personal address books - only allow the users to receive external email if the sender of the email exists in the users personal address books.
- Receive external email if in shared address books - only allow the users to receive external email if the sender of the email exists in any address book the recipient has access to.

Sharing

- May use sharing — If this is unchecked the user will not have access to any of the GMS Collaboration sharing features including the ability to share Contacts, Calendars, Journals Notes and Tasks. If it is checked the user will have access to these facilities which are fully described in the GMS User Guide.
- Show domain address book — if this is checked users in this profile will see domain address books. Checking this option does not allow them to add entries to domain address books or to add new domain address books. Domain address books can only be viewed by users in the domain that the address book was created in.
- Show system address book — if this is checked users in this profile will be able to see system address books. Checking this option does not allow them to add entries to system address books or to add new system address books. System address books can be viewed by any user on the system that has the show system address book privilege.
- Show local address book — this option displays a special address book that contains a list of all the accounts set up under the user's domain. The user can only edit their own account details and not that of any other accounts.
- May share with everyone — this option relates to the Access Rights for entries in System and Domain level address books. This particular option allows the user creating an entry in one of those address books to share that entry with the everyone group. The everyone group contains all users that exist under the user's particular domain.
- May share with allusers — this option relates to the Access Rights for entries in System and Domain level address books. This particular option allows the user creating an entry in one of those address books to share that entry with the allusers group. The allusers group contains all users that exist on that particular server.
- May change freebusy settings - enabling this option controls whether the user is able to change their own freebusy settings under the My Account area.

WebMail

- May use GMS WebMail — this gives the user the right to access GMS WebMail.

- May use the address book — enabled by default, this option gives users the right to use the GMS Address Books including their personal address book. The options below can be used to increase the granularity of the users access rights.
 - Manage Domain Address Books — this gives the user the right to Add, Remove and Rename address books at the Domain level. It does not give the user the right to edit entries within these address books.
 - Manage Domain Address Book Entries — this option gives the user the right to Add, Edit or Remove entries from the Domain level address books. It does not give the user the right to manage the address books themselves.
 - Manage System Address Books — this gives the user the right to Add, Remove and Rename address books at the System level. It does not give the user the right to edit entries within these address books.
 - Manage System Address Book Entries — this option gives the user the right to Add, Edit or Remove entries from the System level address books. It does not give the user the right to manage the address books themselves.
 - Attach vCards to messages - this option determines if a user has the right to attach vCards to their outgoing messages.
- Add disposable addresses — disposable addresses are temporary addresses created with a specific life span or time to live. These are ideal if users wish to correspond with discussion lists for a short period of time but do not want to receive spam that this correspondence may generate.
- Filter incoming email — enabling this allows users of GMS WebMail to set up active filters. Filters can be used to carry out actions on messages that meet certain defined criteria. For example you could have a filter to copy all messages arriving at a mailbox from Boss@test.dom to a folder called Important.
- Add their own personalities — GMS WebMail allows the addition of different personalities, for example you can send some emails from a business personality and others from personal personality. Checking this option allows users to add their own personalities. See the *GMS User Guide* for more information on personalities.
- Allow local personalities only — this option limits users to personalities for their own domain only.
- Collect email from POP3/IMAP4 servers — this is another feature related to GMS WebMail. Using the WebMail client you can set it to download mail from external POP or IMAP mailboxes. This is ideal if you have accounts with more than one ISP and only want to check one mailbox. Checking this option allows users to set up this facility. The *GMS User Guide* explains more about this option.

- Send HTML email from GMS WebMail — enabling this allows users to create and send messages in HTML format.
- May CC email - allows the user to CC (Carbon Copy) other users on email that is sent.
- May BCC email - allows the user to BCC (Blind Carbon Copy) other users on email that is sent.
- Use calendars, tasks and notes - If this is checked the user will have access to the personal and shared calendaring available in GMS WebOrganizer which is fully integrated into GMS WebMail.
- May use Gizmos - If this option is enabled then WebMail users will have access to all Gizmos made available to them by the system administrator. Gizmos are a JavaScript based mashup technology.

Mobile Gateway (requires GMS SMS/Pager Gateway)

- May use SMS Gateway - This option enables the user to send SMS messages via the mobile gateway to mobile phones.
- May use Pager Gateway - This option enables the user to send messages to a pager.

Instant Messaging (requires GMS Instant Messenger)

These settings define what instant messaging privileges users with this profile should have.

- May use GMS Instant Messenger
Selected by default, this option allows the user to use Instant Messaging if a valid license key is installed.
- Launch GMS Instant Messenger on logon
If instant messaging is enabled for your account when you log in to GMS WebMail by default an instant messaging window will be launched and you will automatically be logged in to instant messaging. If users with this profile prefer not to automatically log in to instant messaging you should un-check this option. You can log on to instant messaging at any time by clicking on the Compose instant message button in the top menu bar of GMS WebMail or logging in to GMS Messenger through the default login page.
- Include the following image
If selected, you can enter a default image which can be included in outbound emails. This image will be placed in the top right corner of messages sent from GMS WebMail Professional. This could be your company logo or other promotional image and can be combined with the users presence images, detailed later in this section.
 - Image URL - enter the URL to the image you wish to be included in your users email.

- Alt Text - enter the alternative text you wish to be shown when the mouse cursor is placed over the image, once it has been displayed in a message.
- Link to URL - enter the URL you wish the message recipient to be redirected to, should they click upon the image displayed in their message.

Note: For a user to include this image in their email, they must select "Include user image" from the Options section, available in the GMS WebMail Professional message compose window. See "Composing an Email Message" on page 20 of the *GMS User Guide*.

- Allow user selected image
If selected, this option will allow the user to specify the URL to an image that will be used instead of the system configuration. This image will be included in their email when sent from the GMS WebMail Professional interface.
- Allow user presence indication
If selected you can enter the URL to specific images showing an online and offline statement. When a user sends a message from GMS WebMail Professional they can include their GMS Instant Messenger presence information, this will include either the online or offline specified image depending upon whether the user is logged on to GMS Instant Messenger.
 - Offline Image URL - enter the URL to the image you have chosen to use to indicates a users offline presence.
 - Online Image URL - enter the URL to the image you have chosen to use to indicates a users online presence.

Collaboration (Requires GMS Collaboration key)

These settings define users rights to access and set information regarding GMS Collaboration usage.

- May use GMS Collaboration
Enabled by default, this option allows users access to the GMS Collaboration server from MS Outlook (providing they have first installed the GMS Collaboration client on their desktop machine). Roaming profiles are supported, so the client can be used in a hotdesking situation.

Documents (Requires a GMS WebMail key)

The documents section of a profile allows you to control whether or not a user may use the Documents facility within WebMail.

- May use Documents
Enabled by default, this option allows users to maintain a variety of documents within the WebMail interface and to share those documents with other users of the system.
- Document Store Capacity

Allows the administrator to set a maximum size for the users document store. Note that as users can maintain a number of revisions of each document that stores may grow quite quickly.

- Maximum Revisions

Dictates the maximum number of revisions to be supported for each document. Once this number has been reached any further revisions to the document will cause the oldest revision to be deleted.

Preferences - setting configuration appearance

You can either use the default GUI settings or you can configure each of the following to your preference.

- Background colour
- Title colour
- Tab font face
- Tab font size

Preferences - configuring Anti-Spam settings

- Report mail as junk mail - allows users to report mail as Junk mail. If using GMS WebMail the users will see an icon in their status bar allowing them to report spam to the system administrator. Normal mail users can forward the message to spam@theirdomain.
 - Automatically add Junk Mail to Bayesian Filter - If you have users on your system whom you trust not to report good mail as spam or junk then enabling this option will allow them to add messages directly to the Bayesian filter without any administrator input.
 - Automatically report Zero Hour false negatives - Again for trusted users this option allows them to report Zero Hour false negatives, i.e. mail that has not been caught by the Zero Hour filter but should have been.
- May use the junk mail filter - allows users access to the Junk Mail filter in the administration interface under Administration > Mail > Account > Settings.
 - Enable the junk mail filter - will enable the junk mail filter for all accounts under this profile using the default settings.

AV Preferences - configuring Anti-Virus settings

This configuration requires GMS Anti-Virus. Prior to configuring the Anti Virus settings for the profile you must set the GMS Anti Virus configuration to "Allow user settings via profiles". This is configured by selecting the domain from the drop down then Anti Virus in the menu and the Actions tab on the right. The Virus scanner must also be enabled under System, Anti Virus, Actions.

You are now able to apply specific Anti Virus settings to the profiles in the domain you have set these options for.

Actions

There are three options that control the operation of the Virus Scanner.

- **Use Domain Virus Scanner Actions**

The settings in place for the domain will be applied to all users in this profile.

- **Enable Specific Virus Scanner Actions**

The settings in place further down this page will apply to all users in this profile.

- **Disable Virus Scanner**

If this option is selected none of the users in this profile will be protected from viruses.

The rest of the options on this page affect what happens when the Virus Scanner detects an infected mail message.

- **Reject Message**

If a virus is found any mail can be rejected with a "550 This message contained a virus" SMTP reply code.

- **Redirect To**

Any files found to contain a virus will be redirected to the given account.

- **Deliver Message as Usual**

This is the default action. The message is delivered to the intended recipient in the normal manner.

- **Deliver to User Quarantine folder**

The message is copied to the quarantine folder. The message can be accepted, forwarded or deleted from the quarantine folder.

- **When a Scan fails for any other reason**

You have the option to select Reject mail and notify postmaster as a safeguard against errors on your system. This option would protect the server from viruses should the messages not be scanned if, for example, the definition files have been deleted from the disk. Note: This setting will reject all inbound mail until the issue is resolved.

Alerts

It is possible to alert a number of people to the fact that there was an attempt to send a virus through the system. Exactly which alert options are available will depend on the action you have configured to occur when a virus is discovered. Either the default domain level alerts may be used, or specific alerts set that will affect only users in this profile.

- **Alert Postmaster**

To send an alert to the administrator of the system select this check box. If you would like the alert to go to someone other than the postmaster please enter their email address in the box provided, otherwise the default of postmaster@domain.name is used.

- **Alert User**

Check this box if you would like the intended recipient of a virus to be informed that someone has attempted to send him an infected file.

- **Alert Sender**

Selecting this option will send a message to sender of the file alerting them to the fact that they attempted to send an infected file through the system.

10.4 Changing a User's Profile

Once you have created a new profile you may want to change some of your existing users to use that profile. This can either be done under the Users tab within the profile by clicking on Add Members, or from the individual user configuration page. For the latter go to Domains & Users, Domain, User and on the Account Information tab select the new profile from the Account Profile drop down and click on the "Update" button to apply the change.

10.5 Profile Examples

Delegating Domain administration

As a system administrator you may want to grant a user the privilege to administer a domain. To do this you need to have a profile that grants domain administration rights for the domain. You should clone the system base profile to a new profile, perhaps called "test.dom Admin". Next you would select that profile and display the "Configuration" tab for the new profile. This allows you to select the "User may administer his own domain" option. Now any user who is assigned to this profile will have the right to administer their own domain. If the user is in the "test.dom" domain then they will be able to administer that domain.

Service Levels

Some service providers like to provide different levels of service for instance platinum, gold and silver levels. Profiles makes this extremely easy as you can set up a profile for each level of service. For example the platinum level might allow the users to have full rights to set their own aliases and autoresponders etc. and give them access to GMS WebMail from anywhere. A gold level might allow users to access GMS WebMail but with no options to set

filters, personalities etc. and a silver level might deny the user access to GMS WebMail but still allow them to download their mail using POP.

11 Advanced Management

This section is for administrators who want to use the full capabilities of GMS. If you are running a system with more than one mail server, please also refer to “GMS on Complex Networks” on page 189.

This section starts by describing how you can tune system performance, as follows:

- Using Watch to monitor GMS.
- Incoming e-mail — tuning threads, extensions and connections.
- Outgoing e-mail — tuning bandwidth, extensions and threads.
- E-mail collection (POP3) — tuning the number of connections, extensions, bandwidth and threads, also the immediate deletion of messages.
- Inbound delivery rules (*smart routing*).
- Outbound delivery rules (*smart delivery*).
- SMTP DLLs.

It then describes a number of other areas:

- Reducing use of IP resources.
- Changing the ports used by services.
- Using ESMTP extensions.
- RFC compliance.
- Generating server messages.
- Configuring an SMTP logon message.
- Changing POST and POP timing settings.
- Listing and starting outgoing mail queues.
- Setting up DNS servers and the DNS cache.
- Editing global, domain and user variables.
- Threads.
- Porting accounts from other servers using AutoPort.
- Allow LDAP directory services access to addressbooks

11.1 Tuning System Performance

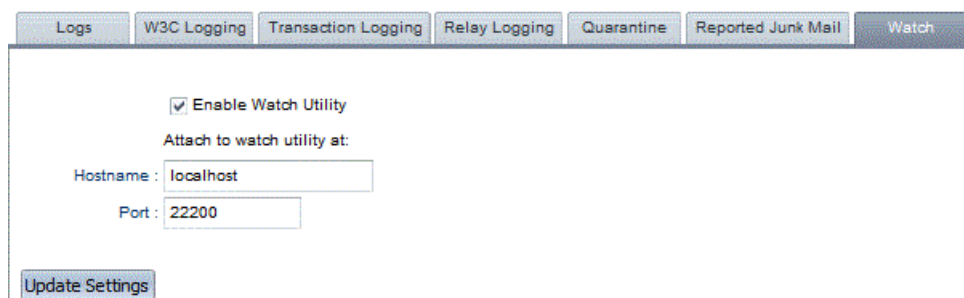
GMS' default values will suit all but the most demanding establishments, but if you wish to tune your system's performance, you can change the settings described in this section.

Using the Watch utility to monitor performance

The GMS Watch application lets you monitor the threads being used by the server and the transaction logs in live mode as messages are processed by the server. GMS sends the required information to the machine specified. This machine should be running the GMS Watch program.

To run Watch:

1. Choose System Administration, Logging then the Watch tab on the right to display this page:



2. Select the Enable Watch Utility check box.
3. In the Hostname box, type the hostname of the machine running the GMS Watch program in the form "machine.domain.dom".
4. In the Port box, specify the port that the information should be sent on. The default setting is port 22200 — do not change this unless it has also been changed in the GMS Watch program.
5. Press the Update button.

Incoming e-mail

There are three areas where you can tune incoming e-mail performance, extensions, threads and connection times, as described below.

Extensions

Use the relevant ESMTP extensions from the set described in "Using ESMTP features" on page 130.

To enable/disable ESMTP features:

1. Choose System Administration, Performance and then the ESMTP tab on the right to display this page:

General Ports Connections Access Control Redirect ESMTP Deliv

Incoming

☒ Enable Enhanced SMTP

VRFY Command:

☐ Disabled

☒ Enabled (no wildcard)

☐ Enabled (wildcard allowed)

☒ Allow HELP Command

☒ Allow NOOP Command

☒ Allow Delivery Status Notification

☒ Allow Enhanced Status Codes

☒ Enable ETRN

☒ No password - deliver to MX

☐ Plaintext password - deliver to MX and static IP

☐ MD5 Password - deliver to MX and any IP

☒ Allow size KB

☐ Allow XTND

☒ Allow 8bitMIME

Allow AUTH Logon:

☐ LOGIN

☐ MD5

☐ CRAM-MD5

☐ PLAIN

Allow Pipelining And Restart:

2. Select or deselect the relevant check boxes and radio buttons.
3. Press the Update button.

Threads

You can set the number of threads used by SMTP for incoming mail (the range is 1 to 255). This controls how many simultaneous transactions SMTP can handle. Each thread requires memory, so increasing the number of connections increases the memory requirements of your mail server.

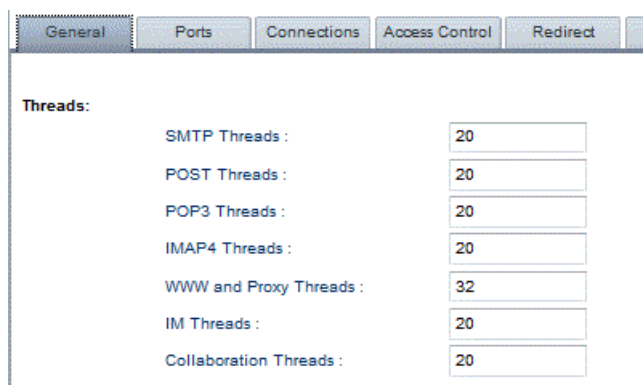
The main reason for increasing the number of threads is that your server is especially busy, for example if you are an ISP with a large

number of dial-up customers. You might reduce the value if you have limited memory available.

If you have limited memory you may also want to restrict the amount of memory by limiting the maximum number of threads available to the services. This setting can only be made directly to the system variables, see the MaxThreads setting in the *GMS Reference Guide* for more information.

To change the number of threads used by SMTP for incoming mail:

1. Choose System Administration, Performance then the General tab on the right to display this page:



The screenshot shows the 'General' tab of the GMS Administrator interface. At the top, there are tabs for 'General', 'Ports', 'Connections', 'Access Control', and 'Redirect'. Below the tabs, the 'Threads:' section contains a list of services with their corresponding thread counts in text boxes:

Service	Threads
SMTP Threads :	20
POST Threads :	20
POP3 Threads :	20
IMAP4 Threads :	20
WWW and Proxy Threads :	32
IM Threads :	20
Collaboration Threads :	20

2. In the SMTP Threads text box, type the number of threads you want to use and press the Update button.

The Set to Default button returns all the values to their defaults.

Service Connection times

You can change the timeout for each service. You might increase this for the POP service, for example, if users downloading large messages using POP experience problems and the POP log shows that the connections are timing out.

To change the connection times:

1. Choose System Administration, Security and then the Connections tab on the right.
2. Type in the number of seconds before timeout for the service and press the Update button.

Outgoing e-mail

There are three areas where you can tune outgoing e-mail performance.

POST outbound bandwidth

Limiting bandwidth helps to stop GMS saturating the link to the Internet. This is especially useful if you need to preserve a percentage of bandwidth for other services, such as browsing the Web.

To limit the outbound bandwidth that POST uses:

1. Choose System Administration, Performance then the General tab on the right to display this page:

The screenshot shows the 'General' tab of the GMS Administrator's Guide. The 'Threads' section includes the following settings:

Threads:	Value
SMTP Threads :	20
POST Threads :	20
POP3 Threads :	20
IMAP4 Threads :	20
WWW and Proxy Threads :	32
IM Threads :	20
Collaboration Threads :	20

The 'Bandwidth' section includes the following settings:

Bandwidth:	Value	Unit
<input type="checkbox"/> Limit SMTP bandwidth		KBytes/sec
<input type="checkbox"/> Limit POST bandwidth		KBytes/sec
<input type="checkbox"/> Limit POP bandwidth		KBytes/sec

2. Under Maximum POST Bandwidth, select the "Limit to" check box and type in a figure in KBytes/sec. This is the maximum bandwidth that POST can use.
3. Press the Update button.

Extensions

Use the relevant ESMTP extensions described in "Using ESMTP features" on page 130. To enable/disable ESMTP features, choose System Administration, Performance then the ESMTP tab on the right and (de)select the relevant check boxes. Press the Update button.

Threads

You can set the number of threads available for use by POST (from 1 to 255). This controls how many simultaneous transactions POST can handle. The memory overhead for POST threads is much lower than for SMTP threads. Each thread delivers a mail queue in the Out directory.

You might increase the POST threads if you have a lot of mail in the Out directory waiting to be posted.

To change the number of POST threads:

1. Choose System Administration, Performance then the General tab on the right.
2. In the Post Threads field, type the number of threads and press the Update button.

E-mail collection (POP3)

You can change parameters in any of the areas described below to alter the performance of POP3 collection.

Number of connections

This specifies the number of simultaneous connections from a single machine to your mail server. Typically, a value of one prevents people using a large number of POP accounts from the same machine.

Extensions

The following are all POP server commands, which can be issued in a POP session to carry out the described actions. APOP is the only one which you need to configure from within GMS:

- APOP — authenticated POP login. This encrypts passwords, making it more difficult to hack into the system by "sniffing" passwords from TCP packets transferred to/from your server. APOP passwords cannot be used with NT User Database accounts.

You have three choices:

- Disable APOP login.
- Let the POP3 server announce that it can accept APOP encrypted passwords.
- Make APOP login mandatory. If you set this, ensure that all your subscribing POP clients support APOP.

To set APOP up, choose System Administration, Security, Connections and select the check boxes you want, then press the Update button.

- LAST — lets users display the id of the last message in their mailbox.
- UIDL (Unique ID Listing) — lets users display a unique id for each message.
- TOP — a mail client can request the first n lines of a message.
- XTND — this supports two elements, XMIT and XLIST.
XMIT is used to send mail via POP servers rather than SMTP.
XLIST is used to list message headers. It can operate in several modes: Get all headers, Get headers matching the given clause (Received, To, etc.) or Get the header for a specific message ID. For full details, see the *GMS Reference Guide*.
- VERS — lets users display the POP version number.

POP download bandwidth

Limiting bandwidth helps to stop GMS saturating the link to the Internet. This is especially useful if you need to preserve a percentage of bandwidth for other services, such as browsing the Web.

To limit POP download bandwidth:

1. Choose System Administration, Performance and then the General tab on the right.
2. Under Limit POP Bandwidth, enter a figure in KBytes/sec. Press the Update button.

Immediate deletion (POP3 DELE)

Normally POP3 does not remove deleted messages from a user's mailbox until they quit their session. This ensures users do not lose mail on a poor connection. You can configure it to delete messages immediately the user has requested they be deleted, although this contradicts RFC1939.

The advantages of this are:

- Users only download messages once on a dial-up.
- It reduces the chance of messages being left on the server accidentally (the user may not realise that messages are not being deleted).

To delete messages immediately they have been read by users:

1. Choose System Administration, Settings then the Compliance tab to display this page:

General Authentication System Recovery Usage Policy Messages Compliance Timed Events Alarms

☐ Enforce RFC 822 header

Enforce CRLF :

☐ No Action

☒ Enforce CRLF end of line

☐ Reject message mismatched CRLFs

☐ Enforce RFC 2822 line length

☒ Enforce RFC 2821 transparency

☐ Enforce RFC 1984 DSN

☒ Allow RFC 1123 return

☐ Match SMTP and header "From:" clause

☐ Require domain in MAIL and RCPT commands

☒ Insert missing "From:" clause as per RFC 822

☒ Insert missing "To:" clause as per RFC 822

☐ Always insert missing "To:" clause

☐ Insert "Return-Path:" clause

☐ MSMail address fix

☐ Restore SMTP headers

☒ POP3 DELE works immediately *Note that this contradicts RFC 1939

☐ POP3 RETR marks messages for deletion *Note that this contradicts RFC 1939

☐ Show real host in SMTP "Received:" clause

☒ Show real host in POST EHLO/HELO command

☐ SMTP resolve hostname

Maximum hop count : 17

Maximum length of "Received" line : 78

☐ Always send

Bad recipient notifications : ☐ Never send

2. Select the "POP3 DELE works immediately" check box and press the Update button.

Threads

You can set the number of threads available for use by POP (from 1 to 256). This controls how many simultaneous transactions it can handle, so changes the performance of the mail server.

You might increase the POP threads if you have many users and little bandwidth between the clients and the server. You might reduce the value if you do not have a lot of memory available.

To change the number of POP3 threads:

1. Choose System Administration, Performance, General.
2. In the POP3 Threads field, type the number of threads. Press the Update button.

Configuring Smart Routing

Smart routing is the redirection of messages to/from specified locations before they are delivered. You could use this, for example, to send mail from all known Spammers to a null account (the

equivalent of deleting it), or to redirect all mail for Sales to another account.

The accounts to be redirected are listed in a Redirect file using a notation that allows entire domains to be included using wildcards. For details, see "The Redirect File" in the *GMS Reference Guide*.

To set up smart routing:

1. Choose System Administration, Performance then the Redirect tab on the right. Any existing redirect commands are displayed in the table.
2. Press the Add New button to enter a new redirect rule:

3. If you want to just add a comment to the file, select the Comment radio button and type the text. Press Update and skip the other steps. The comment could give details about a rule, for example.
4. To create a rule, select Rule. For any of the following two steps, you can use a "*" wildcard.
5. Specify the mail source, either as a name (in the MAIL Clause text box), or an IP address (in the Remote IP Address text box).
6. Specify the mail destination, either as a name (in the RCPT Clause text box), or an IP address (in the Local IP Address text box).
7. In the Action drop-down list, specify what to do when a matching message is found.
 - Protocol refuse with — returns the specified message (type it in the Parameter text box) to the sender. The message must take the form 5xx, for example "503 Bad sequence of commands".
 - Protocol retry later — returns the specified message to the sender. The message must begin with a number 4xx; see "Error Messages" in the *GMS Reference Guide*.
 - Redirect to — sends the message to the address you specify in the Parameter text box.
 - Run following script — allows a mml script to be specified to act upon connections matching this redirect rule. Enter the name of the script in the dialog box below. Note the script must be placed in the <\$path> directory.

- Don't take action on match — ignores the rule.
8. When you finish, press the Update button. The rule will be displayed like this:

Mail	From IP	To	To IP	Action
# This is a comment				
spam@*	*	*	*	Refuse

Move Up Move Down Add New Remove All

9. If you want to change the position of the command in the file (commands at the bottom of the list override entries which are above them), use the appropriate buttons to move the entry up or down as required.
10. To edit an entry simply highlight it in the list and edit the entries in the Redirect Rule box below as for creating a rule above.
11. To remove an entry highlight it and click on Delete.

Configuring outbound delivery rules (Smart Delivery)

When POST sends outgoing mail, it works through the list of servers defined in the `postservers.txt` file (known as the *Sending rules*). For details of the file, see "Postservers.txt" in the *GMS Reference Guide*.

Rules lower in the list override those at the top. For example, with the two rules shown below, mail to all domains is resolved by MX records through DNS, except for mail to `domain.dom`, which is always sent to `server.domain.dom`:

```
* * 25 12
domain.dom server.domain.dom 25 12
```

Set up rules depending on the type of connection, as described below.

Permanent or dial-up connections

To set up a rule for either of these connection types, do the following:

1. Choose System Administration, Performance and then the Delivery Rules tab on the right to display the page:

2. In the Target Address box, type "*", meaning mail for all domains.
3. In the Post Server box, type the name of your ISP's server.
4. In the Port box, type "25".
5. In the Retry box, type 12 for a permanent connection or 0 for dial-up. This is the delay in minutes between consecutive attempts at sending e-mail messages to a server that cannot be reached first time. The retry value of 0 for dial-up means do not retry.



With a permanent connection, if all your mail is urgent you can reduce this value to ensure that any mail that fails to be delivered is retried again fairly quickly. We do not recommend setting a value lower than five minutes. Be careful if you have a busy server as this can increase server activity dramatically.

6. Press the Add New button to add a new rule. The added rules are shown like this. To remove a rule highlight it and Delete it,

or to edit highlight and edit the Delivery Rule Details. The order of rules can be changed by highlighting the rule you would like to move and using the appropriate buttons.

General	Ports	Connections	Access Control	Redirect	ESMTP	Delivery Rules	MX	Miscellaneous
Target address	Post server	Port	Retry	Account	Password			
All	Resolve MX	25	12					
other.dom	mail.other.dom	25	12					

If you find that mail is not being posted out from your server correctly and you see lots of "gethostbyname" failures in the post log check that the entry in DNS for the mail server and the hostname and domain given in your tcp/ip configuration match up.

The reason for this is that the local post server must do a lookup to determine who it is first before attempting to lookup MX records for the recipient domain in order that it can remove itself from the MX records returned (if it appears there, i.e. in the case where it is acting as a lower priority MX record).

Local domains

For a local domain you need an entry, like the following:

```
domain 127.0.0.1 25 12
*.domain 127.0.0.1 25 12
```

The second rule covers any subdomains

To set up the first of these sending rules (This entry is only required if you are using a dialup):

1. Choose System Administration, Performance, Delivery Rules to display this page:

Delivery Rule Details

Target Address :	<input type="text" value="All"/>
Deliver to :	<input type="text" value="Resolve MX"/>
Port Number :	<input type="text" value="25"/>
Retry Every :	<input type="text" value="12"/> minutes
Account :	<input type="text"/>
	<input type="checkbox"/> Change Password
Password :	<input type="password"/>

2. In the Target Address field, type the domain name.
3. In the Post Server field, type 127.0.0.1. This is the server's loopback address.
4. In the Port field, type "25".

5. In the Retry field, type 12. This is the delay in minutes between consecutive attempts at sending e-mail messages if there's a problem the first time.
6. Press the Update button.

To set up the second rule

1. Choose System Administration, Performance, Delivery Rules
2. In the Target Address field, type *.domain
3. In the Post Server field, type 127.0.0.1
4. In the Post Server field, type 25
5. In the Retry field, type 10
6. Press the Update button.

SMTP DLLs (*Windows only*)

DLLs let you extend the functionality of GMS to suit your own requirements. SMTP DLLs act on all e-mail entering the system during the course of a normal mail transaction. The DLLs can act on any stage of the SMTP protocol.

For more details, see "SMTP DLLs" in the *GMS Reference Guide*.

SMTP Shared Libraries (*Unix*)

Shared Libraries let you extend the functionality of GMS Mail to suit your own requirements. SMTP Shared Libraries act on all e-mail entering the system during the course of a normal mail transaction. The Shared Libraries can act on any stage of the SMTP protocol.

11.2 Other Advanced Areas

This section describes those areas which do not directly affect the performance of the system.

Reducing use of IP resources

There is currently a shortage of IP addresses on the Internet in general, so GMS provides two methods of reducing your IP address requirements:

- Using multiple domains on one IP address. This is called *multihoming* and involves using virtual domains. Full domains require an IP address for each domain, but virtual domains "piggy back" on one full domain, sharing the same IP Address. For details, see "Virtual domains" on page 86.
- Using domain aliases - for details, see "Setting up domain aliases" on page 92.

Using virtual domains is better because you can distinguish between addresses like the following, whereas with domain aliases these two appear to be the same:

user@company1.dom
user@company2.dom

Changing the ports used by services

If you change any service's port from its default value:

- This prevents other services accessing the port.
- You may not be able to post mail to any other mail server.

Because of this, you must take care when changing a value. Only make changes if you are connecting to a machine internally, for example to a proxy.

You can specify which port to use for each of the following services:

- SMTP incoming — the port the SMTP server uses to accept e-mail. The Internet Standard is to use port 25, but you may wish to run another mail server on the same machine and make it direct mail to GMS at a different port.
- SMTP outgoing — the port GMS uses to send all mail to destination servers. In general, you would only change this definition if you knew all mail was going to a specific port on a machine defined by the parameter PostServers.
- POP3 — the port the POP server listens on for the POP3 Protocol.
- IMAP4 — the port the IMAP server listens on for the IMAP protocol.
- Finger — the port allocated for the finger server.

- Password server — the port the password server listens on for password request changes.
- DNS — the port GMS uses for DNS when resolving MX records. Note that changing this entry causes all MX lookups to fail unless you have a DNS server which supports the new port number.
- Web Proxy — the port used by Proxy server.
- Web Configuration (MML) — the port used by the Web Configuration server.
- MML Port.

To change the port used by a service:

1. Choose System Administration, Performance then the Ports tab on the right to display this page:

	Non Secure	Secure
SMTP incoming port :	25	465
SMTP submission incoming port :	587	
SMTP outgoing port :	25	
POP3 port :	110	995
IMAP4 port :	143	993
Finger port :	79	
Password server port :	106	
DNS port :	53	
WWW administration GUI port :	8001	
WWW Webmail GUI port :	9000	
WWW User GUI port :	8888	
IM port :	8367	8368
Collaboration port :	8376	8377
SNMP port :	161	
LDAP port :	389	

2. Type the new number of the port you want to change. This can be any available port on the server.
3. Press the Update button.
4. Stop and restart the relevant service to bring the change into effect. The easiest way to do this if you have the interface open is to choose System Administration, move your cursor over the particular service and press the Stop button for the service, then restart it.

GMS Messenger Port

The messenger port must be configured directly via the Support, System Variables section. See "Editing Global, Domain and User variables" on page 141.



To return all the values to their defaults, press the Set to Default button.



There are some advanced port and IP address configuration options available see "IP address and Port Flexibility" on page 163.

Using ESMTP features

The Enhanced SMTP (ESMTP) features are defined in a series of RFCs extending the SMTP protocol. These enhancements have emerged over time and each adds extra features to SMTP.

The ESMTP features supported by GMS are 8BitMIME, AUTH, Delivery Status Notification, Enhanced Status Codes, ETRN, Pipelining and Restart, Size, VRFY and XTND.

This section describes these briefly; for full details, see “Services” in the *GMS Reference Guide*.

Disabling/enabling ESMTP features

To enable/disable ESMTP features, choose System Administration, Performance then the ESMTP tab on the right and (de)select the relevant check boxes. Press the Update button.

ESMTP features

The features available are as follows:

- 8BitMIME — the sender uses this command to announce that it supports higher bit ASCII transmission.
- Auth — use Auth to set up authenticated SMTP transactions. GMS supports three types of authenticated SMTP — LOGON, MD5 and CRAM-MD5. MD5 uses encrypted passwords and is the equivalent of APOP, LOGON does not and is the equivalent of normal POP. For full details, see the *GMS Reference Guide*.
- Delivery Status Notification (DSN) — this option requests that the GMS server confirms that a transaction was completed as desired.
- Enhanced Status Codes — these give precise error codes relating to the delivery of mail. They are only delivered to servers issuing the EHLO command to indicate that they understand ESMTP; all other servers receive the standard response codes.
- ETRN — also known as QSND, this is specifically designed to allow integration with dial-up mail servers. A dial-up mail server can connect to the GMS server and issue the ETRN command to force all the e-mail for it server to be posted out. The keyword associated with this ESMTP extension is ETRN.
- Pipelining — reduces the time it takes to send multiple messages. A sending server uses Pipelining to send all the messages it has to a receiver in one burst, without sending a Reset command after each message. It fires all the commands down the pipe without waiting for a response from the remote

server — once all the commands have been issued, the remote server issues all its responses at once.



Pipelining and Restart are alternatives.

With Pipelining, if a user on a remote server sends a message to multiple users on your server, this uses only a single SMTP connection with one MAIL FROM clause and multiple RCPT clauses. This means the message body is only transmitted once.

- Restart — after a connection is lost while a message is being sent, on reconnection the Restart command from the sender gives the receiver the option of continuing from the point it had reached, rather than starting again at the beginning.
- Size — this is used by the sending server to state that it has a message of the specified size for the receiving server. The receiver replies, either accepting or rejecting the message. The main difference between this approach and the message size limits described in “Account Settings” on page 101 is that it acts at the protocol level so the message is never actually transmitted — this preserves bandwidth.

To specify the ESMTP Size, choose System Administration, Performance, ESMTP, select the Size check box and type in the value in KB.

- VRFY — this command verifies a user name. It lets external servers check that an e-mail account actually exists on your server. The response may include the full name of the user and must include their mailbox.
- XTND — this supports two elements, XMIT and XLIST. XMIT is used to send mail via POP servers rather than SMTP. XLIST is used to list message headers. It operates in three modes: Get all headers, Get headers matching the given clause (Received, To, etc.) or Get the header for a specific message ID. For full details, see the *GMS Reference Guide*.

Generating server messages

You can choose from a number of useful server-generated messages from the list below. The first four options in this list are enabled by default:

- Delivery Receipts when requested — determines whether GMS should respond when a remote host requests a confirmation of the delivery of an e-mail to the recipients inbox. This is not an indication that e-mail has been read — the receiving mail client handles this — only confirmation that the e-mail has reached its destination mail server.

- Read Receipts when requested from local users — determines whether GMS should respond automatically when a remote host requests a confirmation that a received e-mail has been read.
- Read Receipts when requested from external users — determines whether GMS should respond automatically when a remote host requests a confirmation that a received e-mail has been read.
- Return undelivered messages — specifies that any e-mail rejected by a mail server because the recipient is unknown must be returned as an attachment to an error message giving the reason for the non-delivery. If you prefer to return the e-mail in the error message body, instead of as an attachment, disable this option.
- Statistics Message to Postmaster — if this is checked, at midnight GMS sends the Postmaster an e-mail summarising the number of e-mail messages received and sent by the mail server during the preceding 24 hour period.
- Statistics Message (to Gordano Ltd.) — if this is checked, at midnight GMS sends Gordano Ltd. an e-mail summarising the number of e-mail messages received and sent by the mail server during the preceding 24 hour period.
- TRAP to Support (at Gordano Ltd.) — automatically e-mails any occurrences of traps to Gordano Support. A trap occurs when the server automatically catches a problem that could cause it to stop responding — the thread the trap occurs on is recovered and the server continues to function normally. Enabling this option assists the Support department to see any problems that may be affecting use of the server.
- MML errors to Support (at Gordano Ltd) — Automatically emails any occurrences of MML errors to support. This allows our engineers to see problems as soon as they occur and frequently a problem can be fixed before it has even been reported to support.
- Service start Message to Postmaster — Automatically emails a message to the postmaster when a service is started.

To change settings from the default:

1. Choose System Administration, Settings and the Messages tab on the right to display this page:

The screenshot shows a web interface with a top navigation bar containing tabs: General, Authentication, System Recovery, Usage Policy, Messages, and Co. The Messages tab is selected. Below the tabs is a list of settings, each with a checkbox and a label. The settings are: Delivery receipts when requested (checked), Read receipts when requested from local users (checked), Read Receipts when requested from external users (checked), Return undelivered messages (checked), Statistics message to Postmaster (unchecked), Statistics Message (to Gordano Ltd) (unchecked), TRAP to Support (at Gordano Ltd) (checked), MML Error to Support (at Gordano Ltd) (checked), and Service start Message to Postmaster (unchecked). At the bottom of the settings list are two buttons: Update Settings and Set to Default.

Setting	Checked
Delivery receipts when requested	Yes
Read receipts when requested from local users	Yes
Read Receipts when requested from external users	Yes
Return undelivered messages	Yes
Statistics message to Postmaster	No
Statistics Message (to Gordano Ltd)	No
TRAP to Support (at Gordano Ltd)	Yes
MML Error to Support (at Gordano Ltd)	Yes
Service start Message to Postmaster	No

Update Settings Set to Default

2. Select/deselect check boxes as required.
3. Choose the Update button to effect your changes.

Changing RFC compliance

GMS follows the RFC standards for e-mail closely, but you may need it to deviate from the strict interpretation of the RFC standards so it can work with other non-standard mail clients and servers. The options available are listed below:

- **Enforce RFC822 Header** — If this box is checked, an e-mail message header must include a minimum of a To and From clause. These are normally inserted by the mail client, a process which is entirely transparent to the user. However, during a Telnet session these clauses must be input manually after the DATA statement and before the message body in order to comply with RFC822.
- **Enforce CRLF end of line** — according to RFC standards, all lines must end with a Carriage Return, Line Feed pair <CRLF>. Unfortunately, some mail servers (especially old versions of Sendmail) only terminate with a carriage return. If you cannot persuade the administrator of the non-standard mail server to update it, you can modify GMS to accept this shortcoming.
- **Enforce RFC2822 Line length** — According to RFC standards there are two limits placed on characters in a line. Each line of characters must be no more than 998 characters, and should be no more than 78 characters, excluding the CRLF. Select this option to enforce character line length.
- **Enforce RFC1894 DSN** — enforces the use of Delivery Status Notification (DSN) messages during the delivery of mail messages.
- **Allow RFC1123 return** — specifies that any e-mail rejected by a mail server because the recipient is unknown should be returned as an attachment to an error message giving the reason for the non-delivery. If you prefer to have the e-mail in the error message body, instead of an attachment, disable this option.
- **Correct SMTP "From:" Clauses** — if this option is checked, GMS will try to correct badly formed e-mail From clauses. Errors such as unbalanced angle brackets, quotes and illegal spaces can be handled. Note that some From addresses are so badly formed that it is impossible to guess the intended address.
- **Correct SMTP "To:" Clauses** — if this option is checked, GMS will try to correct badly formed e-mail To clauses. Errors such as unbalanced angle brackets, quotes and illegal spaces can be handled. Note that some To addresses are so badly formed that it is impossible to guess the intended address.
- **MS Mail Address Fix** — the Microsoft mail client, MS Mail, does not always enter the correct From or To clauses in an e-mail message envelope. This option forces GMS to check for the account "NULL" or an empty e-mail address in the protocol and

replace it with the "From" or "To" clause from the message itself.



While the above option gives MS Mail users the warm feeling that they know where the message was sent to, it is potentially dangerous because the To clause may not contain the real destination address of the e-mail.

- POP3 DELE works immediately — enabling this option allows the removal of mail from a user's mailbox immediately the DELE command is issued, instead of the recommended method of updating the mailbox contents when the client issues a QUIT command. This option contradicts RFC 1939.
- Show real host in SMTP "Received:" clause — enforces the entry of the real host name in the Received header rather the host name passed to GMS in the HELO clause
- Show real host in POST EHLO/HELO clause — Enforces the entry of the real host name as configured in TCP/IP settings in the EHLO/HELO clause
- SMTP resolve host name — forces GMS to perform a DNS lookup on the host name given in the HELO clause and rejects connections from any hosts that are not resolved correctly.
- Maximum Hop Count — GMS keeps a record of how many times an e-mail message passes through the mail server so that it can detect when e-mail is caught in a loop. Loops are usually caused by an incorrect mail server and/or DNS setting.
When the value entered here is reached, GMS breaks the loop and warns the postmaster of the problem. The default value is 17.
- Maximum length of "Received" line — Very long Received lines can cause problems for some mail servers. You can restrict the length of the Received line to a set number of characters.



















To change a compliance parameter:

1. Choose System Administration, Settings then the Compliance tab on the right.
2. Select or deselect check boxes for any of the on/off parameters you want to change.
3. If required, type in the values for the last two parameters. Press the Update button.

Controlling Services (*Windows*)

To stop or start the GMS services from the user interface:

1. Choose System Administration to display this page:

System		Timed Events			
Service	Status	Event Name	Type	Next Due	
WWW	Started	CalendarAlarms	System	2012-08-21 11:29:01	 
SMTP	Started	CheckGMSUpdates	System	2012-08-22 02:00:01	 
POST	Started	DialupWeekdays	System	2012-08-21 11:38:37	 
POP	Started	DialupWeekends	System	2012-08-25 09:00:01	 
IMAP	Started	DynamicASUpdate	System	2012-08-23 01:00:01	 
GMS Instant Messenger	Started	LogRules	System	2012-08-22 03:00:01	 
GMS Collaboration	Started	MesLogtest.dom	System	2012-08-22 03:10:01	 
LIST	Started	QuarantineReminder	System	2012-08-22 01:00:01	 
Manager	Started	VirusUpdate	System	2012-08-23 01:00:01	 
GMSLDAP	Started				
GMSSQL	Started				
GMSSNMP	Stopped				

Scripts				
Type	Session ID	Page	User	Duration (secs)
USER	4988	\restdispatcher.mml	postmaster@test.dom	0

2. The status column shows the state of each service. In the above example the GMSSNMP service is stopped. To start it you would highlight it with the cursor and click on Start.
3. Highlight the service then Press the button for the service you want to start or stop. This effects the change immediately.
4. The Restart button has the same effect as stopping and then starting a service.

Controlling Services (*Unix*)

All the GMS services can be stopped by typing the following from a command line:

```
<$basedir>/mail/bin/glmail stop
```

GMS services can be started by typing the following from a command line:

```
<$basedir>/mail/bin/glmail start
```

Services can also be shut down on an individual basis using the kill command

To start just one service type:

```
<$basedir>/mail/bin/<servicename>
```

For Example:

```
opt/gordano/mail/bin/pop
```


Setting up an SMTP logon message

You can include a message as part of the SMTP logon banner. Each line of the message will automatically be preceded by "220-" for you so please do not enter this, simply enter the text you wish displayed. An example might be:

Unsolicited commercial e-mail will be rejected
Contact postmaster@domain.dom if rejected in error

When displayed by SMTP this would become

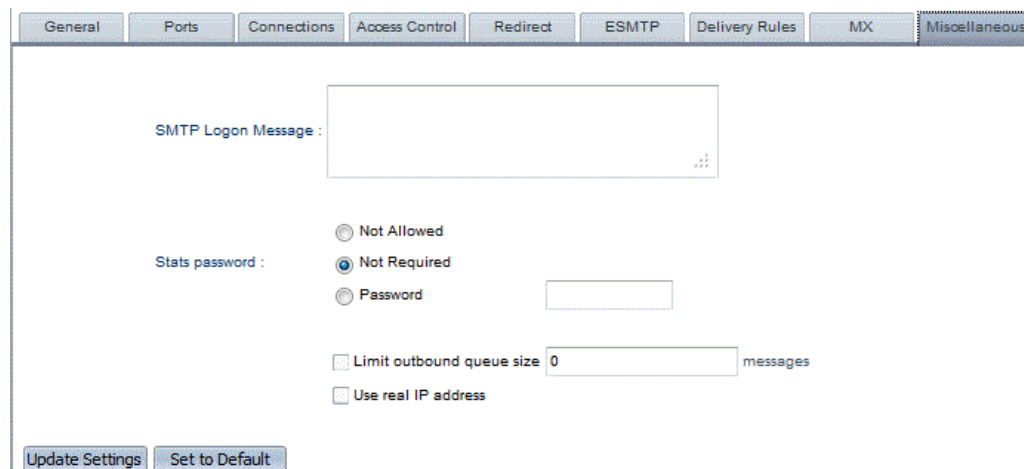
220-Unsolicited commercial e-mail will be rejected
220-Contact postmaster@domain.dom if rejected in error



Microsoft Outlook is known to experience problems when SMTP logon banners are defined.

To add a message to the logon banner:

1. Choose System Administration, Performance and then the Miscellaneous tab on the right to display this page:



The screenshot shows the 'Miscellaneous' tab in the GMS Administrator's Guide. The 'SMTP Logon Message' field is a large text box. Below it, the 'Stats password' section has three radio buttons: 'Not Allowed', 'Not Required' (selected), and 'Password'. To the right of the 'Password' radio button is a small text box. Below these are two checkboxes: 'Limit outbound queue size' (checked) with a value of '0' and 'messages', and 'Use real IP address' (unchecked). At the bottom are two buttons: 'Update Settings' and 'Set to Default'.

2. Type the message you want into the text box, following the rules described above.
3. Press the Update button.

Changing POST and POP timing settings

You can configure a number of parameters which control the way messages are handled after an initial failure in delivery. These are:

- Send immediately — if this is enabled, GMS' POST service sends e-mail messages as soon as they are received from a mail client or mail server.



Do not select the Send Immediately check box if you use a dial-up connection.

-
- Default retry time — The delay in minutes between attempts to send e-mail messages to servers that could not be reached on a previous attempt. The previous failure might be because of a DNS or mail server failure, for example.

If this value is set to zero, POST never checks to see if there is mail waiting to be sent and you must either use SMTP to tell POST about new mail or use 'MAIL -k'. The upper limit, 10080 minutes, is seven days.



Do not set this if you use a dial-up connection.

If all your mail is urgent you can reduce this value to make sure that any mail that fails to be delivered is retried again fairly quickly. We do not recommend setting a value lower than five minutes. Be careful if you have a busy server as this can increase server activity dramatically.

You can set different values for different domains by using Smart Delivery rules; see "Configuring outbound delivery rules (Smart Delivery)" on page 124.

- Sending warning if mail not sent — The time in hours after which a warning is generated and sent to the original sender of an e-mail if it has not been delivered during this period.

Reduce this if you want to be warned quickly if mail is not sent out. We do not recommend a setting of less than four hours as it is not unusual for mail to take at least this long to be delivered.

- Return mail if not deliverable — The time in hours after which mail is returned to a user if it cannot be delivered.

Reduce this from 72 if all your mail is urgent and you would like to know as soon as possible if it fails. Do not make this interval too short or e-mail will be returned to a sender before a temporary DNS or mail server fault can be rectified. We do not recommend values under 24 hours as it can take at least this time for mail to be delivered over the Internet — if the message is very urgent e-mail is not the best way to send it!

- POP Logon Delay — Sets a delay in seconds before GMS sends an OK response to POP clients which might be too slow to accept it without a pause in the protocol. The default value, 0, disables the delay.

To change a timing parameter:

1. Choose System Administration, Performance and then the General tab on the right to display this page:

Message delivery timing:

☒ Send message immediately

Default retry time : minutes

Sending warning if mail not sent for : hours

Return mail if not deliverable for : hours

2. If you want mail to be sent immediately, select the Send Message Immediately check box.
3. If you want to change any of the numeric parameter values, type in the new value. (Read the description of the parameter above carefully before you change anything.)
4. Press the Update button.

Listing and starting outgoing mail queues

You can list all the POST queues to show for each queue the domains that outgoing mail is destined for, the number of messages and their size in KB.

To view the queues:

1. Choose Reports, Mail Queue Size.
2. The queues are listed in this format:

Mail Queues

Update Every : ☒ seconds ☐ minutes

To start queues:

1. Press Display to show all current mail queues
 - Refresh - Clicking Refresh will refresh the queue data displayed.
 - Reschedule - Highlighting a queue and clicking on the Reschedule button will force the post service to attempt to send that queue immediately.

- Reschedule All - Highlighting a queue and clicking on the Reschedule All button will force the post service to attempt to send all queues immediately.
- Details - Highlighting a queue and clicking on the Details button will display additional details of the message queue including the next scheduled retry time and details of any potential problems associated with the specific mail queue.
- Delete - Highlighting a queue and clicking on the Delete button will immediately remove that queue from the server. Mail in the queue will simply be deleted.

Setting up DNS servers and the DNS cache

You can specify which DNS servers GMS uses to resolve e-mail addresses. You can also set up a DNS Cache that will greatly speed up DNS requests for frequently requested domains.

To set these up:

1. Choose System Administration, Performance and the MX tab on the right to display this page:

General Ports Connections Access Control Redirect ESMTP Delivery Rules **MX**

Expire cache : 4 hours

Flush cache : 5 minutes

Cache size : 1024 KBytes

DNS Servers :

☒ Use HOSTS file

Protocol : ☐ UDP Only ☒ UDP then TCP if data truncated ☐ TCP Only

Update Settings Purge Cache Set to Default

2. In the Expire Cache field, specify the time in hours after which the cached MX record information is considered to be out of date and will not be used. By default this cache is set to update after 24 hours.
3. In the Flush Cache field, specify how often in hours the cache should refresh its MX record data. If the DNS server needed for the MX lookup is not available, the previous MX record information can be stored until the cache expiry time is reached.



You can set the expiry and flush times to any value but be aware that DNS records are constantly changing. If the times are set too high, it is likely that the DNS records for a domain may have changed before the cache is refreshed and GMS will try to deliver e-mail to the wrong host.

4. In the Cache Size field, specify the size of the DNS Cache. This is set at 1MB by default and you should not normally have to

- change this. If GMS cannot service a DNS request from the cache, it will automatically contact the specified DNS Servers to do so.
5. In the DNS Servers text box, type a space-separated list of DNS Servers. If this box is empty, GMS will use those entered in the system TCP/IP configuration. If more than one server is defined, GMS sends queries to each server in turn to spread the load.
 6. Select the Use HOSTS file check box if you want GMS to try to use the local Hosts file to resolve names before trying to resolve them via DNS.
 7. Press the Update button to effect your changes.

Editing Global, Domain and User variables

Under certain circumstances you may need to edit directly the three sets of variables which control GMS:

- Global variables — elements which affect the overall operation of GMS, for example, the number of threads allocated a service, whether or not APOP login is enforced on the system, and the list of DNS servers to be used.
- Domain-specific variables — the values which can change on a per-domain basis, for example domain name, domain id and domain user count.
- User variables — elements like passwords, user-specific mailbox sizes and access rights.



These variables are changed transparently when you change configuration through the standard user interface, and that is the only way we recommend changing the setup in normal circumstances. Only change the variables if you are directed to do so by GMS Support staff.

If you are asked by Support to change a system value:

1. Choose Support, Variables.
2. Scroll down the list to find the variable they ask you to change.
3. Double click on the variable to open it for editing and type the new value into the Variable Value field and press Enter. Make sure you click on the Save button to apply and changes you have made.

The procedure is the same for the other two types of variables, Domain Variables are found under Domains & Users, Domain, Variables and User Variables under Domains & Users, Domain, Username, Variables.

Changing use of threads

You can set the number of threads available for use by each service (the range is from one to 256). The number of threads allocated

controls how many simultaneous transactions the service can handle, so affects the performance of the mail server. On the other hand more threads use more memory, so there's a trade-off between this and the benefits of allowing more connections.

The main reasons for changing from the defaults are:

- Your server is especially busy, for example if you are an ISP with a large number of dial-up customers.
- If you have many users and plenty of bandwidth between the clients and the server, you might increase the values for POP, POST or SMTP.
- If you have a large number of users accessing your server through the WWW interface, you might increase the WWW value.
- If you do not have a lot of memory available, you might reduce the values for POP, POST, SMTP or WWW.

To change the number of threads used by a service:

1. Choose System Administration, Performance and the General tab on the right.
2. Type the number of threads for the service and press the Update button.



To return all the values to their defaults, press the Set to Default button.

Using ETRN

Using ETRN with GMS as the server

Do not set up the domain within GMS

Ensure that GMS will accept mail for this domain by adding the domain to the "Allow Relay for..." section

Add an entry to your Sending Rules as follows

`"domain.com server.domain.com 25 0"`

This means send all mail for domain.com to server.domain.com on port 25 but only send when requested.

server.domain.com should have a valid A record in DNS

ETRN by itself is not a completely secure command so the supplied ETRN utility additionally provides the capability of password protecting mail queues. The password can be transmitted either in plain text or in encrypted form, this is controlled by the AllowEtrn registry entry.

To allow password protection of the queue an extra parameter should be added to the entry in your postservers.txt file for the domain in question, so the entry outlined in step 3 above would become

`"domain.com server.domain.com 25 0 password"`.

There is also a third option which allows mail to be dequeued to the IP address of the server issuing the ETRN command. For this to work the postserver entry must contain a password parameter as above. The machine issuing the ETRN command must indicate a destination machine of * in the ntmetrn.exe utility

The three options form a bit map for the AllowEtrn registry entry so all three options can be allowed if required. Refer to the *GMS reference Guide* for more details on AllowEtrn.

Using ETRN as a client

When retrieving mail via SMTP in a dialup situation you can use the utility NTMEtrn.exe provided as part of the GMS Option Pack available from <ftp://ftp.gordano.com>.

If you are using a static IP which requires that an A record is set up in DNS, the command line might look something like:

```
NTMEtrn -mserver.isp.dom -qclient.dom -sKeepOut  
-dserver.client.dom
```

If you are using a dynamically assigned IP address then an example of the command line required would be

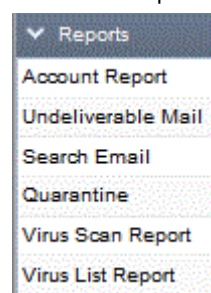
```
NTMEtrn -mserver.isp.dom -qclient.dom -sKeepOut -d*
```

Run "ntmetrn -h" for help on usage.

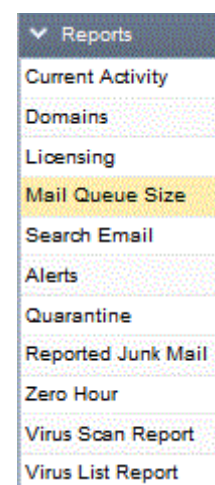
11.3 Reports

GMS provides administrators with a number of useful reports that allow you to monitor the performance of your system. There are two levels of report, Domain reports and System reports. To access system reports log on to GMS then select Reports in the menu. To access the reports for a particular domain you need to first select the Domain in the drop down then select Reports in the menu.

Domain Reports



System Reports



Account Report (domain)

The account report shows the last access date and time, profile and disk space usage for every mail user in the domain. You can sort the listing by selecting the title of the column you want to sort by. Click the title again to sort in reverse order.

Undeliverable Mail (domain and system)

This report shows any mail that is found to be undeliverable. Simply select the required entry from the list then click on the "View" button.

If there were any undeliverable messages the subsequent report displays the following information.

- Date and time of the messages.
- The QueueID (the name of the queue that contained the undeliverable message(s)).
- The destination the message was meant for.
- The From address.
- The To address.
- The size of the message.

You can sort the listing by selecting the title of the column you want to sort by. Click the title again to sort in reverse order.

If no undeliverable messages exist on the system then the report will be empty.

Quarantine (domain and system)

All messages found to contain banned content, for example restricted words or a virus, from or to a local user, can be redirected to the Domain Quarantine folder, others will go to the System Quarantine folder.

Quarantine Folder			
Date	Number Of Messages		
2012-08-21	2		

Refresh
Manage
Delete
False Positive

This report shows the date of each individual quarantine folder and the number of messages within that folder are displayed.

The following options are available:

- **Manage** - Highlighting an entry and clicking on **Manage** opens a management screen to allow you to accept, forward, delete, virus scan or report falsely quarantined messages.
- **Delete** - Deletes the highlighted entry including all the messages it contains.
- **Refresh** - Refreshes the display.
- **False Positive** - Reports the highlighted entry and all of the messages within it as a False Positive result. That is messages that should have been delivered to the user rather than placed in Quarantine.

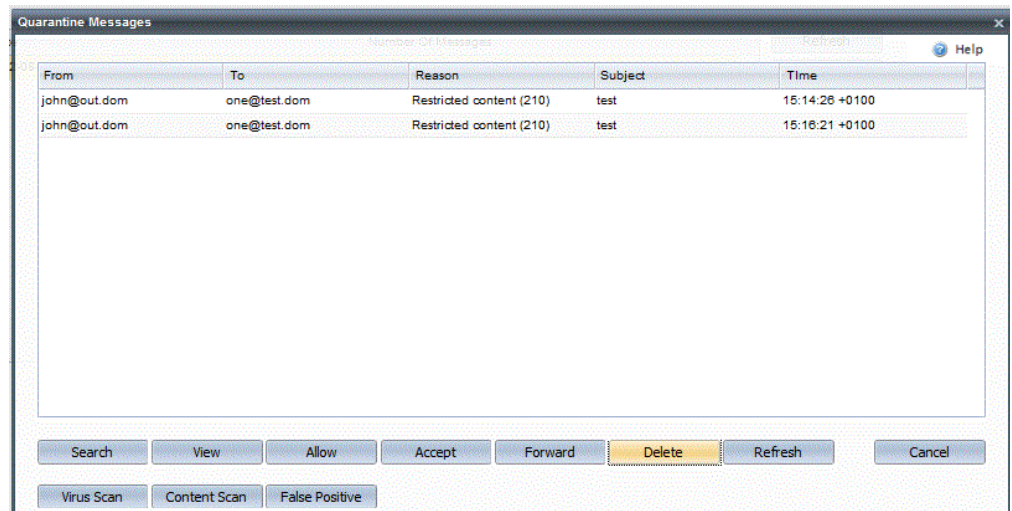
Access to this folder is controlled via user profiles.



In addition to copying messages to the Domain or System Quarantine folder they may also be delivered to the each users Quarantine folder. Users are able to perform their own management of this folder including reporting false positives, allowing through to their inbox, or blacklisting senders. See the User Guide for more information.

Quarantine Messages

This screen allows complete management of all of the individual messages within a particular days quarantine folder.



The Quarantine Messages list shows all off the messages quarantined on a particular day. It shows the sender, the recipient, the reason the message was placed in the quarantine folder, the subject of the message and the date and time it was sent. The following options are available:

- **View** - Highlighting a message and clicking on **View** will display that message in the lower panel on the screen.
- **Accept** - Accepts the highlighted message and delivers it to the intended recipient.

- **Forward** - Accepts the highlighted message and delivers it to the named recipient.
- **Delete** - Deletes the highlighted message.
- **Refresh** - Refreshes the screen to show the most up to date status.
- **Virus Scan** - If a message is placed in quarantine due to having failed a virus check it can be rescanned from here. If the message no longer fails the virus check you can elect to use one of the above options.
- **False Positive** - This option is used to report messages that have ended up in the quarantine folder due to failing the Zero Hour checks that should not have, i.e. genuine messages.
- **Cancel** -.Closes the dialog and returns to the previous screen.

The same options as above are available on the View screen for individual messages.

Virus Scan Report (domain and system)

This report shows messages that have passed through the virus scanner and whether or not they were found to contain a virus. The first step asks you what you would like included in the report. You can choose to display results for all messages that have been scanned and/or messages that were found to contain a virus. Simply check the options you require, select the days you would like the report to cover from the list of dates then click on the "Report" button. You can select multiple days from the list by holding down the "Control" key on your keyboard while selecting the dates with the mouse pointer.

If there were any matching messages on the selected day the report displays the following information.

- Date and time of the message.
- Who the message was from.
- Who the message was to.
- Whether a virus was found or not. If the name of the virus is known that will also be shown.
- Any action that has been taken as a result of a virus being detected.
- Whether or not any virus has been disinfected.

You can sort the listing by selecting the title of the column you want to sort by. Click the title again to sort in reverse order.

If you have no virus logs available on your system this report is not available and instead of the report an explanatory message is displayed.

Virus List Report (domain and system)

A list of Viruses the system is protected from, can be displayed when selecting this report.

Enter the name of the virus you wish to check the system is protected from and click **Report**

The wildcard "*" can be used in searches.

Search Email (domain and system)

The email search report is available to both system and domain administrators.

The email address is entered in the "Email Address" field. Wildcards can be used e.g. "*@test.dom".

Search for - enter the search criteria from the following options:

- All activity
- Custom
 - Received email
 - Sent email
 - Email collection
 - Web access
 - List server
 - Virus scans

Search - enter the period you wish to search

Number of results - specify the number of results to be returned.

The Search button will begin the search process along with a warning that it may take some time.

Note: Domain administrators are only able to search for emails sent to or received from the domain(s) which they have rights to manage.

Licensing (system)

The Licensing Report shows details of usage on each of the licensed GMS services including the total number of licensed seats, the number of those seats that have been used and also displays the percentage of the particular license that has been used.

Zero Hour (system)

The Zero Hour report will firstly show you the version of the Zero Hour detection engine you are running, and the status of that Zero Hour detection engine.

It also allows you to open a number of flash images directly on the Gordano Website showing real time views of live spam on the Internet. The options available here are:

- Daily Outbreak Report
- Daily Outbreak Monitor Report
- Top Outbreak Countries Report
- Top Outbreak Domains Report

Current Activity Report (system)

You can monitor service activity (IMAP4, LIST, POP3, POST or SMTP) in real time and, if necessary, start or stop a service. You would need to restart a service, for example, after changing its timeout value.

To monitor services from the user interface:

1. Choose Reports then select the "Current Activity" report from the reports branch of the tree
2. The information for each service is displayed, with these fields:
 - Action — the service name.
 - Id — the session number.
 - IP Address — the address of the remote connection, if any.
 - Mode — the status, as given in the tables which follow.
 - Time — the time this thread has been processing the transaction, in seconds.

The following tables list the possible values for each service type:

POST

Status	Meaning
IDLE	No action currently taking place.
CONN	Connecting to remote host.
HELO	Sent HELO, waiting for response.
EHLO	Sent EHLO, waiting for response.
MAIL	Sent MAIL from, waiting for response.
RCPT	Sent RCPT to, waiting for response.
DATA	Sent DATA, waiting for response.
RSET	Resetting connection for another transfer of e-mail.
QUIT	Closing down the connection.

POP

Status	Meaning
IDLE	No action currently taking place.
LOGN	User logging in.
USER	Sent response to USER command.
PASS	Sent response to PASS command. Logon successful.
QUIT	Closing down the connection.

IMAP

Status	Meaning
IDLE	No action currently taking place.
CONN	Just got a connection, now expecting authentication command.
AUTH	Authentication OK.
SELE	Successful select or examine — a folder has been selected for work.
LOGO	Connection closing down.

SMTP

Status	Meaning
IDLE	No action currently taking place.
CONN	Connected to remote host.
HELO	HELO clause received, waiting for MAIL clause.
MAIL	MAIL clause received, waiting for RCPT clause.
RCPT	RCPT clause received, waiting for DATA or RCPT clause
DATA	Receiving e-mail message from remote host.
QUIT	Closing down the connection.

Domains Report (system)

This report lists the domains on the system. The information given includes:

- IP address
- type of domain
- date created
- number of users
- disk space usage

You can sort the listing by selecting the title of the column you want to sort by. Click the title again to sort in reverse order.

If you select a domain from the report and then click on the "Display" button.

a further report is displayed providing more detailed information on that domain.

Mail Queue Size (system)

This report provides information on the mail queues existing on the system. The first step asks you to decide whether you want to display the queue length as Kbytes or number of messages in the queue. You are also asked to specify how often you want the information updated. Once you have made your selection click on the "Display" button to show the results.

The results screen lists the queues and their size. You can select a queue in the list and click on the "Details" button for more information on an individual queue.

You can sort the listing by selecting the title of the column you want to sort by. Click the title again to sort in reverse order.

Reported Junk Mail (system)

This report shows any mail that has been reported as spam by users on the system. The report will initially show the date and the number of messages reported on that date. At this stage you can highlight one of the rows in the report and **Delete** it. Alternatively you can click on the **Mark as Spam** button to add all of the messages reported that day to the system Bayesian filter, or click on **Manage** to obtain a full report for that day displaying the individual messages.

The secondary report displays the following information:

- The From address
- The To address
- The reason for the message being in the report
- The Subject of the message
- The Date

You can sort the listing by selecting the title of the column you want to sort by. Click the title again to sort in reverse order.

There are a range of options open to you in this secondary report to deal with the reported messages. If you wish to inspect the message further to ensure that it is actually spam then click on the **View** button which will display the source of the message in the bottom pane of the report. The **Delete** and **Mark as Spam** buttons allow the message to be deleted or added to the system Bayesian filter respectively.

Alerts (system)

This page provides a powerful diagnostic tool to assist you in diagnosing problems that may be occurring on your server. This page shows alerts from the server in realtime. When the page is first displayed, approximately 500 alerts (or the number of alerts saved since system restart) will populate it. Alerts will be updated each second and appended to the listing.

If you select one of the lines in the table and click Details, a new browser window will be displayed and a page containing a full explanation of the log entry will be displayed from Gordano's website. The log entry displayed may also contain real values from your server.

Click Manage Alerts to specify which type of alerts should be displayed.

11.4 Monitoring via SNMP

Simple Network Management Protocol (SNMP) provides a means to monitor network devices and to manage statistics collection, performance and security. GMS provides its own SNMP agent on

the server, while an SNMP client will be required in order to read the information provided.

SNMP monitoring is off by default, all configuration for it can be accessed from the System Administration, Monitoring option in the menu on the left hand side of the administration interface.

To enable publishing of SNMP information select the "Enable SNMP Monitoring" check box then select which of the services you wish to monitor. You can monitor either an individual service, some the services or all of the services.

Each of the GMS services publishes a row in the "applTable" table defined in RFC2788. Additionally SMTP and POST also publish a row in the "mtaTable" and "mtaGroupTable" tables defined in RFC2789.

To retrieve this information with your SNMP client you will need to load certain Management Information Base (MIB) files. The RFC2788 and RFC2789 information is published via the standard "Network Services" and "MTA" MIB files respectively. All of the additional information is published under Gordano's own MIB file which can be found in the root of the Gordano installation directory and will need to be installed on your SNMP client.

The Gordano MIB has been registered with IANA and a full list of registered enterprise numbers can be found on their web site.

Password

The default SNMP community/password is "public". For security reasons we would strongly recommended that this is changed before enabling SNMP, if you do not change it then anyone able to connect to your SNMP service will be able to monitor the status of your server.

Allowed IPs

The Allowed IPs option provides a further security measure to protect your SNMP information by allowing you to specify IP addresses that can connect to the SNMP service. You can use wildcards when specifying IP address ranges using the formats previously described.

11.5 Allowing Relay

Relay is the practice of using a mail server to send mail to users who are not local to that server. Servers that allow relay in this way are often used by Spammers (Bulk emailers) to distribute unsolicited commercial email (UCE). Servers that allow open relay in this way are often blacklisted by the internet community and may find they are denied connections to other mail servers because of this. By default GMS is configured not to allow relay at all.

However while it is generally scorned upon to allow your server to relay messages it is sometimes necessary to allow relay in special circumstances. For instance you might have roaming users or home workers who are not connecting from your local network. By default these sorts of users will be able to send mail to other users on your network but not to any external domains (i.e. they cannot relay).

To get around this GMS lets you permit relaying for these types of user whilst still denying relay to the rest of the internet. The options are:

- Allow Relay
- Adding addresses to the LocalIP range.
- Allow Relay for specified domains.
- Authenticated SMTP.
- POP/IMAP before SMTP (Requires GMS Anti-Spam).

Allow Relay

You can enable relay from the System Administration, Security, Relay page of the interface by clicking on the "Allow relay" option. This will make your server an open relay allowing anyone on the internet, particularly spammers to relay through your server. This option is not recommended under any circumstances.

Adding to LocalIP range

If the remote user is always connecting to your server using the same IP address you can tell GMS to treat that IP address as though it were local and allow relay for any connection from that IP address. You can add LocalIPs from the System Administration, Security, LocalIP page of the interface. This method is no good if the user's IP address is constantly changing.

Allow Relay for specified domains

If you want to allow all the users in a particular domain to relay through your server you can add the domain on the System Administration, Security, Relay page of the interface. This is useful if your mail server is acting as a backup or relay server for any non-local domains.

Authenticated SMTP

If you Enable "Allow AUTH" from the System Administration, Performance, ESMTP page your remote users will then have to authenticate to SMTP prior to sending external messages through your server. That means they have to provide a username and password before they can relay. The drawback is that this is only supported by some mail clients.

POP/IMAP before SMTP

Gordano's add on product GMS Anti-Spam enhances your options with POP/IMAP before SMTP. This requires the user to log on to POP or IMAP with their password and username before they can then relay. With some mail clients which try to send mail before they check POP and IMAP the user may need to try twice before messages can be sent. This is probably the best of the three solutions for roaming users. You can configure this option from the Anti Spam, Bypasses, Authenticated Clients page of the interface where GMS Anti-Spam is installed.

11.6 Shared and Public Folders

GMS supports Shared and Public folders within the IMAP server using the IMAP ACL extension covered by RFC 2086. Access Rights can be set by any ACL enabled mail client, such as Mulberry. Other clients such as MS Outlook can use ACLs but are not able to set them.

Shared and Public folders can be set up from the System Administration, Performance, Access Control page.

Enabling Access Control Lists

Selecting this option enables IMAP Access Control Lists (ACLs). If enabled then IMAP will advertise the fact by returning the keyword ACL to the IMAP Capability command. Any clients supporting ACLs will then query the server for further folders that they are allowed to access.

Shared Folder Prefix

All user level shared folders are shared under the prefix specified here. For instance if you use a prefix of "share" then users shared folders could be accessed using "share.username.mailbox".

Public Folder Prefix

Public folders are accessible both to the users logged in to the system and to anonymous users. Public level shared folders are shared under the prefix specified here. A specific account must be set up to hold public shared folders (see below). If you use a prefix of "pub" then public shared folders could be accessed using "pub.mailbox".

Public Folder Account Name

This is an account that would be specifically set up to hold public mailboxes. It is not advisable to use one of your standard mail accounts for this, rather you should set up a specific account. The account must already exist prior to being entered here.

Access control modes

Enforce full access for folder owner

This mode enforces the use of the default ACL rights of "lrswipcda" for a user's own folders. This is the default mode giving fast performance and minimising configuration issues.

Enforce admin access for folder owner

This mode enforces the use of administer access for a user's own folders. This minimises configuration issues.

Allow full access control

This mode allows full control for all folders. This can lead to problems should users delete all admin access for their folders.



At least one account should always have administration access to a folder. If this access right is not available then the rights for a mailbox can never be changed. We therefore recommend that you do not use option 3 above.

Access Control Rights

The following is a full list of the Access Rights that can be enabled/disabled for a mailbox.

l	lookup (mailbox is visible to LIST/LSUB commands)
r	read (SELECT the mailbox, perform CHECK, FETCH, PARTIAL, SEARCH, COPY from mailbox)
s	keep seen/unseen information across sessions (STORE SEEN flag)
w	write (STORE flags other than SEEN and DELETED)
i	insert (perform APPEND, COPY into mailbox)
p	post (send mail to submission address for mailbox, not enforced by IMAP4 itself)
c	create (CREATE new sub-mailboxes in any implementation-defined hierarchy)
d	delete (STORE DELETED flag, perform EXPUNGE)
a	administer (perform SETACL)

11.7 Porting Accounts from other Mail servers

AutoPort for Messaging Servers

GMS includes a utility to provide seamless porting from other mail servers.

This utility allows email accounts to be ported from one proprietary system to another without the need to make any changes to the existing server. The administrator does not need to contact users in order to change their passwords and the transfer of mail files takes place automatically. Furthermore, the email service is not disrupted

and users do not have to disclose or change their passwords or change the configuration of mail clients. The transfer process between the GMS server and the existing server will work with any Internet Standards-Compliant messaging server as the source server including those supporting POP3, IMAP4 or SMTP protocols.

The porting is completed in three stages:

1. **Preparation** - The GMS System is prepared (off the network) by installing the GMS software, setting it up for porting and giving it the same IP address as the existing server you will be replacing. To prepare the server to retrieve the accounts select the System Administration, Porting option in the menu on the left of the screen.

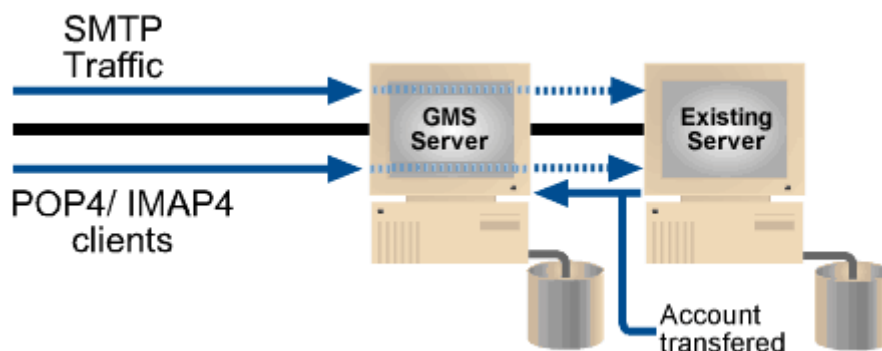
Set the details of the Host to be ported from, this is normally an IP address. Follow this by selecting the protocol to use, the Port on the remote host, whether or not you wish to use SSL, and the type of access that you wish to initiate the porting process for each user.



The SSL option requires that you have installed an SSL certificate on both the old and new servers.

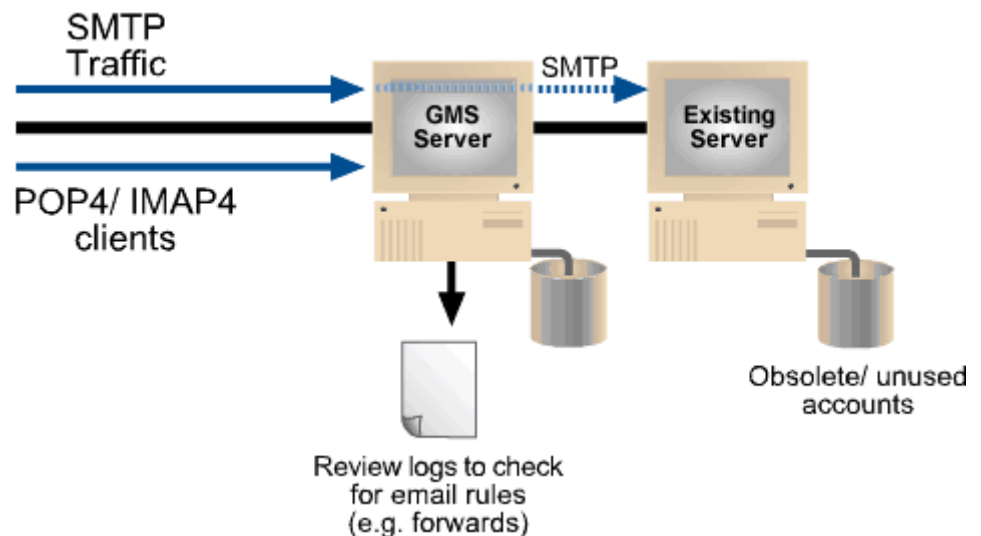
You should now set the Unknown user action for the GMS server to send mail, received for accounts that have not yet been created, to the source server. Go to Domains & Users, Domain and select the Preferences tab on the right. Select "Redirect to server" entering the IP address of the source server then click on Update.

2. **Account Transfer** - To begin the porting process, the existing server should be taken off line and given a new IP address (as defined above). The GMS server is connected to the network (preferably on the same LAN segment) and the existing server and the GMS server restarted. Users can continue to collect and send email in the usual way as illustrated in the diagram.



3. **Retiring the existing server** - After a period of time you may determine that it is time to retire the existing server. Some special mail routing rules (e.g. forwards, auto-responders etc.)

and accounts that have not been accessed will not be transferred automatically. By reviewing the message logs, See "Managing Logs" on page 67. you can identify these special rules or accounts and take the required action.



Porting Options

The porting process can be controlled with these options, dependant on which options you select the delay in a user logging on to the system and actually gaining access to their mailbox may be slightly delayed.

- **Include domain in logon** - will pass the domain name as well as the username to the system being ported from.
- **Port every logon** - provides a persistent porting mechanism, i.e. every time the user logs on an attempt will be made to fetch any fresh messages from the remote system. This is a useful option while testing porting behaviour
- **Archive ported messages** - enabling this option will place all ported messages into the days message log.
- **Content scan messages** - this option provides the option of checking the incoming messages for spam and viruses. Useful if the incumbent system did not provide protection, and as a double check on the validity of messages.



Autoport technology is patented in the United Kingdom under patent number GB2391649. A patent application has been filed in the United States and is pending approval.

11.8 Allow LDAP directory services access to Address Books

GMS provides a facility allowing user to access address books stored on the GMS server from their email client. This means your organization can have a shared address book containing the

addresses of everyone in the organization that they can access using their usual email client.

GMS allows two types of access - non-authenticated or authenticated which can be controlled by configuring a system variable.

By default GMS is configured to only allow authenticated access, however certain email clients do not provide the ability to authenticate, hence you may need to change this setting.

If you need to reconfigure the authentication settings go to Support, Variables and select the variable **LDAPAuth**. Double click on it to open it for editing, enter a value of 0 and press Enter. Click the Save button to apply the change. If you wish to reconfigure authenticated access the variable should be reset to the default value of 1.



Allowing unauthenticated access will allow anyone with a valid email address access to your address books therefore this option should be used with caution.

Please see the GMS Users Guide for full instructions on setting up LDAP directory access from the client perspective.

12 Customisation

GMS provides options allowing you to change the look of the various GMS interfaces. This section will explain the options available.

12.1 WebMail Customisation

WebMail Professional and Express can be customized by enabling the variable WebMailAllowCustomisation. The variable can be enabled at system, domain and user levels in the following way. To enable customisation for a single user select Domains & Users, Domain, Username and then the Variables tab on the right of the screen. To enable customisation for a domain select the Domains & Users, Domain and then the Variables tab on the right of the screen. To enable customisation for the entire system select the Support, Variables tab. On the selected tab click on Add New and enter WebMailAllowCustomisation in the Variable Name entry box, then enter the required value in the Variable Value entry box based on the bit map below and click on the Add button.



A user level variable overrides the domain setting and a domain setting will override the system setting. This way you can give separate users and domains different customization rights

Bit	Value	Meaning
0	1	Allow WebMail Professional users to set colors and backgrounds.
1	2	Allow WebMail Express users to set custom colors.
2	4	Allow WebMail Express to use Cascading Style Sheets to alter the look of the Express client.
3	8	Allow WebMail Express users to select a Cascading Style Sheet on a per user basis. (Implies that Bit 2 is also set.)

Example: To allow WebMail Professional users to set colours and backgrounds and WebMail Express users to set custom colours you would set WebMailAllowCustomisation to a value of 3 (i.e. 1 + 2).



The GMS User Guide contains full instructions for users who have been granted the permission to set colors and backgrounds.

12.2 Cascading Style Sheets

If you set WebMailAllowCustomisation so that cascading style sheets can be used, a default style sheet is loaded when the user logs in to WebMail Express. To change the colours and look of the client you can create your own style sheet which will be used in

place of the default one. Some example style sheets are included in the Gordano Accessory Pack which can be downloaded from the Gordano website <http://www.gordano.com>. If you extract the contents of the Accessory Pack you will have a `wxp.css` file and `mozwxp.css` file in the Gordano\MML directory. These are the default style sheets that will be used by Internet Explorer and Mozilla respectively. If you open these files in a text editor you will see that they contain a lot of items for which you can change styles, colours, sizes etc.

If you want to use more than one style sheet or a non-default style sheet you will need to set a user, domain or system variable called `WXPCSSLinks`. This variable defines a colon separated list of base stylesheet names for example:

```
wxp.css:domain_level.css
```

This means the styles in `wxp.css` will be used unless they are overridden by the contents of `domain_level.css`



Netscape 4 and earlier do not support Cascading Style Sheets. The default look will be seen when accessing WebMail Express using a browser that does not support style sheets.

Allowing User Selection of Style sheets

If you have enabled user selection of Style Sheets the user will be presented with a list of styles to select from, assuming that you have copied the style sheets from the Accessory Pack to the MML directory on the GMS Server.

You can add your own Style Sheets to provide even greater choice to the user. The name of the Style Sheet as displayed to the user within WebMail Express is determined by the name of the CSS file. For example if you name the CSS file to `wxpGordano.css` then "Gordano" will be displayed in the drop down selector.

12.3 Product Logo

WebMail Express

You can define whether or not a logo is displayed in the top left of the WebMail Express page by setting the user, domain or system variable `WXPSHOWPRODUCTLOGO`. By default this is set to 1 and the logo is displayed. To hide the logo set this variable to 0 using the User/Domain/System variables pages under the relevant pages of the Administration GUI. You can also define custom logos in the same way as for WebMail Professional (as explained below).

WebMail Professional

You can change the logo that is displayed in the top left of WebMail Professional pages for example to use your corporate

logo. This can be done from the domain and/or system levels allowing you to specify different logos for each domain on your system. The Domain level logo is defined on the Domains & Users, Domain, Domain Information page of the administration interface. The system level logo is defined on the System Administration, General page of the administration interface. You can also specify a URL that is launched in a new browser window when a user clicks on the logo.



If you log on to the administration interface the default GMS logos are used even if a custom logo has been defined.

12.4 Embedding WebMail Express into a website.

The WebMail Express client has been designed to allow you to embed it into your existing website using HTML frames.

12.5 Custom logon and logoff pages

The Gordano Accessory pack contains a number of custom pages which unpack into the `gordano/mml/usr` directory. These pages are accessed via port 8888 by default. For example:

`http://mail.companya.dom:8888`

This will display a custom log on page. You can change the look of this page by editing the following file:

`gordano\mml\usr\logonscreen.mml`

Or you can write your own page from scratch using MML. See the MML Programmer's Guide.

Additional variables

WebMailLogOffURL - This can be set at a user, domain or system level and specifies the URL the user will be taken to when they click on the Sign Off button in WebMail Express or Professional.

WebMailLogOnURL - This can be set at a user, domain or system level and specifies the URL the user will be taken to when they have been automatically logged off due to a session timeout.

13 IP address and Port Flexibility

IP address and Port Flexibility offers a great deal of control over the ports and IP addresses that the different services use. There are 3 types of connection handling methods available to you as described below. They are configured from the System Administration, Performance, Connections page of the interface. This section will explain:

- Using all IP addresses
- Using specified IP addresses
- Using the IP connection file

13.1 Use only IP address

This is the simplest option to use, each full domain that you set up will need to have an IP address available to it. All the GMS Services will respond using the default ports and the IP addresses defined on your network interface card and associated with the domain. There is no configuration option available for this selection.

13.2 Use specified IP addresses

This is somewhat of a halfway house allowing a degree of flexibility in the configuration of IP addresses and ports for services to respond on. Each full domain that you set up will require a free IP address on your system in order that the default options may be set up for it, however once set up you may amend these options on a per IP basis. Domains will only bind to the IP addresses that are configured against them. This option also allows you to define on an IP/Port basis what remote IP addresses are allowed to connect to each of the services.

Configuration options

Having selected the Update button for this option you will see a number of options displayed in a list box immediately below. If you select an item from the list and double click on it you will be able to alter Protocol, Port, IP address settings etc. for each service. The options are described below:

Protocol

Each service can have a number of protocols associated with it, for instance the POP service supports the protocols for POP3, PASSWORD and FINGER. If you select the **ANY** option from the dropdown you will not be able to run the protocols on non-standard ports.

IP Address

Enter the IP address or range that this service should respond on, if you want the service to respond on a non standard port you can indicate this by appending **:port-number** to the IP address, for example if you wanted the SMTP service running on IP 123.123.123.123 to respond on port 75 rather than the standard port 25 you would enter
123.123.123.123:75

Allow Local IP Addresses

Enabled by default, this option forces the use of the LocalIP setting under System Administration, Security, Local IP to determine a default set of IP addresses that are allowed to connect to the service. This setting is cumulative with **External IP**.

External IP

The default setting for this entry is ANY, i.e. any remote IP address may connect to the service. You can allow only certain IP addresses to connect to the service or allow everyone and ban certain addresses using the standard IP notations. If you want only a subset of your IP addresses to be able to connect to the service then this option should be changed and the IP range added using the usual wildcard options.

13.3 Use IP Connection file

This third and final option provides full flexibility over how your server is set up. You have complete control over which services responds on which IP address and what port it listens on. It is not necessary to have a free IP address on your system to add a second or subsequent domain as each could share the same IP but listen on different ports. Each time you set up a domain or enable an additional service you will need to visit here to enable the connections options for the domain. Services will only bind to the IP addresses that are configured against them. This option also allows you to define on an IP/Port basis what remote IP addresses are allowed to connect to each of the services.



This option is a one way process once it has been selected it is not possible to revert to the other options. If you add new domains you will need to visit the System Administration, Performance, Connections page to configure the connection options for that domain before the domain can be used.

Configuration options

Having selected the Update button for this option you will see a number of options displayed in a list box immediately below. If you select an item from the list and double click on it you will be able to

alter Protocol, Port, IP address settings etc. for each service. The options are described below:

Protocol

Each service can have a number of protocols associated with it, for instance the POP service supports the protocols for POP3, PASSWORD and FINGER. If you select the **ANY** option from the dropdown you will not be able to run the protocols on non-standard ports.

Domain

This option allows you to select the domain that you would like to be associated with the service option you are currently editing. You may select any domain from the drop down menu.

IP Address

Enter the IP address or range that this service should respond on, if you want the service to respond on a non standard port you can indicate this by appending **:port-number** to the IP address, for example if you wanted the SMTP service running on IP 123.123.123.123 to respond on port 75 rather than the standard port 25 you would enter
123.123.123.123:75

Allow Local IP Addresses

Enabled by default, this option forces the use of the LocalIP setting under System Administration, Security, Local IP to determine a default set of IP addresses that are allowed to connect to the service. This setting is cumulative with **External IP**.

External IP

The default setting for this entry is ANY, i.e. any remote IP address may connect to the service. You can allow only certain IP addresses to connect to the service or allow everyone and ban certain addresses using the standard IP notations. If you want only a subset of your IP addresses to be able to connect to the service then this option should be unchecked and the IP range added here using the usual wildcard options.

13.4 Sockets

Be aware that there are a finite number of sockets available for each service. The maximum number available for each service is 1000.

If you use the wildcard in the **IP address** field for a protocol this means that the service will bind to all IP addresses on your network

interface card on the standard port for that protocol, but the advantage is that only one socket will be used to do so.

If you specify IP addresses individually for each protocol a socket will be used for each. for example, if you have 10 IP addresses on your network interface card and enable the 3 protocols under the POP service for each of the IP addresses this will use a total of 30 sockets. if you enable only POP3 and FINGER protocols under the POP service for each of the 10 IP addresses then this will use 20 sockets.

13.5 Adding and deleting a service

This option is not available with the Use only IP address option. From the page which lists the current IP/Port settings there are a number of buttons, including Add New and Delete.

The Add New button will allow you to select a service to be added and go on to configure IP and Port options for that service. You would typically need to do this if you had just added a new domain or wanted to enable a new service under an existing domain.

The Delete button will permanently remove the selected service from your machine. You can also click on Remove All to remove all the entries, please use with great caution, or use Add Comment to enter text reminding you what various settings are for.

Finally when you have completed working with the options on this page you must click Save to commit you changes.

13.6 Adding a comment

This option allows you to insert comments into the list of current settings to remind you what the settings are for. The comments are marked with a # symbol. To add a comment in the middle of a list select the line you would like the comment added above and then click on the Add Comment button.

13.7 Default Ports used by GMS

The following ports are used by GMS.

Service	Port
WatchPort	22200
WWWPort	80
WWWProxyPort	8080
WWWAdminMMLPort	9000
WWWWebMailMMLPort	8888
WWWScriptMMLPort	8025
WWWSSLProxyPorts	443
PasswordPort	106
FingerPort	79

Service	Port
IMAPPort	143
POPPort	110
SMTPPort	25
DNSPort	53
SSLPOPPort	995
SSLIMAPPort	993
IMPort	8367
MySQLPort	8306
CollaborationPort	8376
LDAPPort	389
SNMPPort	161

14 Security

This section is for all administrators. It describes:

- Some background information explaining why security is important.
- The legal implications of poor security practices.
- Standard security precautions you can take. These include setting passwords, using APOP logon, disabling relay and using a Local IP list, imposing limits on RCPT clauses, bad commands etc., and
- Imposing various timeouts.
- The GMS Firewall product.
- Details of the GMS Anti-Spam and GMS Anti-Virus options.

14.1 Introduction

GMS is secure against attack by hackers, viruses, etc. It has full logging (transaction and message logs) and configuration-saving options to ensure against system failures.

GMS can use lookup to verify that the sending server is genuine. It can also perform lookups on the To and From clauses to verify that the sending server has valid MX records.

You can:

- Set the maximum number of sessions from one remote host to prevent denial of service attacks.
- Set the maximum number of RCPT clauses an incoming message can have.
- Make APOP logon mandatory.
- Disable mail relay (and specify the IP addresses of machines allowed to claim they are from local domains).

14.2 E-mail and Security

This section explains why security is important in e-mail systems.

Everything on the Internet is plain text

The very nature of the Internet, where large volumes of electronic mail messages are routed through any number of SMTP servers en route to their destinations, means that mail messages may be:

- Read
- Modified (including their source/destination information).
- Destroyed
- Duplicated

If you use encryption software, for which only you and the recipient have keys, you can do something about the first two security risks. However, there is little you can do about the last two except request that the destination mail server sends a message to acknowledge receipt of your message.

Also, it is possible to fake completely the From, To, Date and Subject clauses. In fact the existence of e-mail is no proof that the named person sent it. For example, e-mail from god@universe could easily be sent by anyone with a fair knowledge of e-mail systems. It has yet to be seen whether the existence of an e-mail message can be considered acceptable evidence of an agreement in a court of law.

The Troubleshooting section shows just how easy it is to fake a message; see "Troubleshooting" on page 317.

GMS storage files

GMS stores all information in unencrypted files on the mail server computer. This means that anyone with access to the server can read (and perhaps modify) mail messages on it. This approach has been taken because of the overheads associated with encryption and decryption.

User mailboxes

Individual user mailboxes are ASCII text files that contain currently undeleted mail messages.

Logging all throughput

When GMS has been requested to log all messages passing through the server, all these messages are stored in plain text files.

14.3 Legal Implications

This section explains why it is important to take security precautions.

Spam

If another company receives large amounts of Unsolicited Commercial E-mail (UCE) which is relayed from your server, this will at the very least reflect badly on your reputation. It will probably cause you to be added to various DNSBL (DNS based Black Lists) lists etc. — for details, see “GMS Anti-Spam” on page 233.

Spam will also use a lot of your resources — network costs, disk space, administration time, etc.

Viruses

An employee may receive a virus in an e-mail attachment and unwittingly release it onto your network. It takes time and costs money to eradicate this and, if it's a *Trojan Horse* virus, it may transmit company data to an external third party.

If another company receives e-mail relayed from your server which contains a virus, this could put you in danger of legal action to recover the costs of removing the virus from their systems.

Using footers as disclaimers

You can customise footers on all messages on a per-domain basis. Such a footer could be a disclaimer, something like this: “The contents of this e-mail do not reflect the opinions of Company X”. Whether this would protect your company in court is debatable.

Acceptable use policies

The contents of employees' e-mail messages can cause your company legal problems. We recommend that you give all employees a statement similar to the following to make their obligations clear.



Gordano Ltd. accepts no responsibility for problems resulting from use of this policy. Allow for your company's specific circumstances and take legal advice.

- All messages composed, sent or received on the internal or external electronic mail system are and remain the property of Company. They are not the private or confidential property of any employee, contractor or agent.
- Company retains the right to review, audit, intercept, access and disclose any information created, received or sent via its e-mail systems at any time without prior notice for any business

purpose. E-mails, like other hard copy or computer files, may be exposed to disclosure and can be used as evidence in legal proceedings.

- Notwithstanding the company's right to retrieve and read any e-mail messages, such messages must be treated as confidential and accessed only by the intended recipient. No one is authorized to retrieve or read any e-mail messages that are not sent to them. Any exception to this policy must receive prior approval from company management.
- The e-mail system is not to be used to create or transmit any offensive or disruptive messages. Among those that are considered offensive are any messages which contain sexual implications, racial slurs, or any other comment that offensively addresses someone's age, race, gender, sexual orientation, physical attributes, religious or political beliefs, national origin or disability.
- The e-mail system must not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
- The e-mail system shall not be used in violation of any or another person's rights. Disparaging or libellous comments must not be made nor may any copyrighted material be used without proper authorization. Violations could result in liability for the individual as well as the company.

14.4 Standard Security Precautions

This section describes ways to improve the security of your system.

Password policy

Passwords are encrypted in GMS's database, but to improve general security, try to force your users to follow these rules:

- Passwords must include a mix of letters and numbers. (GMS passwords must be at least five characters long.)
- Passwords must not be common words, names, places etc.

A good technique for choosing passwords is to use two three letter words separated by a number or symbol. For example, "cat8dog" or "the4ton".

It's up to you to decide whether you let users change their passwords. If not, you can obviously implement the above rules more easily.

If you add many users at once and allocate them simple passwords initially, ask them to change these as soon as possible.



GMS stores passwords in the Registry in an encrypted form (by default), or in plain text (if you enter them manually). To comply with certain countries' export controls, GMS uses a weak password encryption algorithm to store passwords, so passwords can be encrypted and decrypted easily. Ensure that your Registry and any copies of the passwords are not accessible by third parties.

To prevent dictionary attacks against user passwords, GMS increases the time delay after each failed logon attempt in a sequence. Initially this is for one second, but the period doubles after each failed logon attempt. Users should not try to log on during this denial period. If a user tries to log on during it they will fail, even if they supply the correct password. This protection applies to POP and IMAP and WWW logins.



*Passwords cannot contain **

Password Expiry

GMS allows you to specify an expiry interval so that passwords have to be changed on a regular basis. This is configured under Profiles on the Access Rights page by entering a number in the "Passwords expire every [x] days" area. You also have to specify and confirm a password that the user's password will default to when it expires. This password should not be widely known and is designed to allow an administrator to change the password for a user who can no longer access their account because their password has expired.



Two advisory messages are sent to users as the password expiry date approaches giving them the opportunity to change their password.

Restricting access to the Web server

GMS can be configured using a supported Web browser from anywhere in the world. You will only want to give permission to do this to selected administrators.

To give a user permission to do this:

1. Select the user's profile in the new administration pages. See "Profile Management" on page 99.



If you only want to grant one or two users this privilege you might want to create a new profile just for them.

2. Select the Access Rights tab for the Profile.
3. Select the "May configure software from anywhere" check box.
4. Press the Update button.

By default the Web Configuration Server can be accessed by one of the above users from any IP address. You can restrict access to it further by specifying a single IP address, or a range of addresses, as the only addresses from which it can be accessed.

To control access to Web Configuration Server:

1. Choose System Administration, Security, Access Control.
2. Click on Add New and type the IP address you want to add to the permitted access list in the text area that appears and press Enter then click on Save. Press the Update button to confirm your changes.

Checking who is logged on

If you want to know who is logged on to GMS at any time, choose System Administration, Security, Who. Press the Refresh button to update the list. Highlight an entry and click Logoff to end that user session.

Enabling or enforcing APOP logon

APOP encrypts passwords, making it more difficult for a hacker to gain access to the system. You can enforce APOP logon but, if you do, you must ensure that your users' mail clients support this protocol and that the users understand that they must use APOP. Because of this, you may want to let your users choose whether or not to use APOP.



*Some mail clients do not support APOP.
APOP passwords cannot be used with NT SAM User Database accounts.*

To configure use of APOP:

1. Choose System Administration, Security, Connections.
2. To enforce APOP, select the "Require all POP clients to use APOP" check box.
3. To enable APOP but not enforce it, select the "Enable APOP authentication" check box.

Disabling the Finger server and Password server

For security, you might want to disable the finger and/or password servers.

To configure use of either server:

1. Choose System Administration, Security, Protocols.

2. To disable the finger server, deselect the Allow Finger Server check box. To enable it, select the box.
3. To disable the password server, deselect the Allow Password Server check box. To enable it, select the box.
4. Press the Update button. Your changes will only take effect after a system reboot.

Authenticated SMTP

If your server is secured from relay but you have roaming users who must, for whatever reason, use your server to send mail via SMTP you can enable authenticated SMTP by checking the "Allow AUTH" option on the System Administration, Performance, ESMTP page.

This will allow any user who successfully authenticates against SMTP using their pop username and password to relay mail through your server.

This option is only supported by a limited number of mail clients.

Adding addresses to the Local IP list

The LocalIP setting is used in conjunction with the Anti Relay options (see above) to determine which IP addresses are able to send non-local mail through the mail server.

On installation GMS automatically attempts to recognise a Class C IP address block based on the IP addresses attached to the network card of the machine acting as the mail server. You may want to amend this if, for example, you only have a partial Class C address block or have more than one Class C address block.

For more information on address blocks, see "How do I enter IP addresses?" in "Frequently-asked Questions" on page 333.

To add a local IP address:

1. Choose System Administration, Security, Local IP.
2. Click on Add New and type the IP address in the text area that appears then press Enter. Once you have finished entering IP addresses click on Save to commit your changes.



To remove an IP address, select it in the list and click on the Delete button. To remove all IP addresses at once, click on the Remove All button.

Authenticated POP3/IMAP users

You can set up GMS Anti-Spam (if installed) so that successful POP/IMAP logon from a non-local client adds that client to the list of IP addresses who are allowed to relay mail through your server. This is particularly useful if you have a number of roaming users but still

want to maintain a strict anti-relay policy on your server. See "Authenticate" on page 271.

Post Authentication

It is possible to have the post service authenticate to a remote SMTP service (assuming that service supports the AUTH command). To allow this to happen there are two things that you must do.

1. Enable the "Allow AUTH" option under System Administration, Performance, ESMTP, Outgoing
2. Add an account and password that exists on the remote SMTP server to the relevant entry on the System Administration, Performance, Delivery Rules page.

This is really useful where mail is being sent through a remote server that is on a different network.

Imposing limits

Setting limits on three parameters improves security:

- The number of RCPT clauses that will be accepted for any message arriving at the SMTP server. If you have GMS Anti-Spam installed this setting can be overridden on a per-domain basis. The default setting is 100.
- The number of responses to a single command POST will accept. When the POST service issues a command to a remote host, this setting controls the maximum number of responses to the command that the remote host can send. The default setting is 100.
- The number of bad commands the server accepts over a connection before it disconnects. This option affects all the services except POST. It defines the maximum number of unacceptable commands that can be sent from a remote host before the service is automatically disconnected. The default setting is 100.

To change any of these, choose System Administration, Security, Commands, select the Limit option for the parameter and type the new maximum. Press the Update button.

Imposing a WWW session timeout

WWW sessions are set to time out after a specific delay. The default is 10 minutes and you should not extend this. If you do, this increases the chance of an unauthorised user gaining access to an administrator's computer and accessing restricted areas while the administrator is absent.

To reduce the timeout, choose System Administration, Security, Connections and specify the WWW Session Timeout value in minutes up to a maximum of 240. Press the Update button.

Limiting sessions from a single host

You can limit the number of simultaneous SMTP, POP3, IMAP4 and WWW sessions from one remote host (IP address) to prevent a *Denial of Service* attack. To view the current settings, choose System Administration, Security, Sessions to display this page:

Maximum SMTP sessions :

Maximum POP3 sessions :

Maximum IMAP4 sessions :

Maximum WWW sessions :

The reasons for changing any of the parameters are as follows:

- Maximum SMTP Sessions from one remote host — specifies the maximum number of simultaneous SMTP connections from a remote host. Its default setting is to allow an unlimited number of connections.

If you have problems with a single host taking up all the available SMTP threads for a period of time, reduce the value. Many servers will open a new thread for each message they are sending, so if a remote host is sending 200 messages to your server this could conceivably use up 200 threads for the period that the messages are being transferred.

If you have many SMTP connections to your server from the same IP address, increase the value. This happens if the connections come through a proxy or firewall.

- Maximum POP3 Sessions from one remote host — specifies the maximum number of simultaneous POP connections from a remote host. The default setting is one, which helps prevent denial of service attacks on POP, as normally you would only expect a single connection from any one IP address.

If you have many users accessing your server from the same IP address, increase the number. This happens if users connect through a proxy or firewall.

- Maximum IMAP4 Sessions from one remote host — specifies the maximum number of simultaneous IMAP connections from a remote host. The default setting for this is 20.

Increase the figure if you have heavy users of IMAP and need more than 20 simultaneous connections. Reduce the value from 20 if you suspect that denial of service attacks are eating up the available IMAP threads.

- **Maximum WWW Sessions** — Specifies the number of simultaneous sessions available. This limit is implemented to stop systems using too much memory. The value can be set from 1 to 9999. Default is 1000. Each session requires that memory is allocated for it, therefore the greater number of sessions the greater amount of memory is required.

Make any required changes to the parameters, then press the Update button.

Using service timeouts to stop denial of service attacks

Three types of service have a timeout period in seconds, after which the connection is dropped if there is no activity. These are the following:

- **IMAP clients** — the IMAP client inactivity timer value in seconds. Reduce this if you experience problems with IMAP threads being used.
- **POP clients** — the time in seconds the POP server gives POP clients before automatically logging them off the system due to inactivity.

Increase this if your users experience timeouts downloading their mail (these are more likely if they get a lot of large mail messages). If this is the case, your users should also increase the timeouts in their client software.

Reducing the value helps prevent POP threads being used up for long periods of time, so prevents denial of service attacks.

- **SMTP** — the time in seconds the SMTP server waits before dropping a connection due to inactivity. You can increase this if you get a lot of connections from really slow servers or clients, but note that this does leave you open to denial of service attacks.

To change a timeout from the default:

1. Choose System Administration, Security, Connections.
2. Type in the number of seconds for the parameter(s) you want and press the Update button.



Changes will not take effect until the services have been stopped and then restarted.

Disabling other functions

There are several other options you might want to disable for security reasons. To change these:

1. Choose System Administration, Security, Control and disable any of the following:

- Stop executing scripts — this stops users executing MML scripts. By default this is selected — only change it if you have a good reason to do so.
 - Show Support menus — you can stop users from using the Support options if you have a reason to do this.
 - Allow direct editing of system variables — this enables the System, Domains and User Variables pages. By default these are unavailable and only enable them if you have a good reason to do so.
 - Allow Find — the Find button which lets users lookup other users by name.
2. Press the Update button.

Protecting the SMTP STAT command

The SMTP STAT command shows statistics on the SMTP server usage. To use it, log on to port 25 using telnet then type STAT. Data shown includes the number of accounts on the system, server up time, etc.

For security you should set a password to stop unauthorised use of the command. A user then has to type **STAT <password>** to obtain the statistics.

To set a password on STAT:

1. Choose System Information, Performance, Miscellaneous.
2. Under Stats password, select Password and type the password into the text box.
3. Press the Update button.

Setting up Configuration Server session control

You can specify how sessions are to be recognised and maintained in the Configuration Server, that is, whether to use cookies and/or IP addresses.

To set up session control:

1. Choose System Administration, Security, Session Control.
2. Specify which of the following to use
 - Use both Cookies and IP addresses — this is the default setting. It looks at the IP address connecting to the server to maintain session information, but also maintains a cookie for the duration of the session so a second connection from the same IP address will have no effect on the first user's session.
 - Only use Cookies — this should also work well to maintain session information provided of course that the user has not disabled the use of cookies in their browser. If they have, the logon will be refused.

- Only use IP addresses — take care when selecting this option as a second connection from the same IP address will override the settings of the first connection. This could occur for example if your users connect through a proxy server.
3. Press the Update button.

14.5 MX Backup

GMS Firewall server is a single user version of GMS. It can be configured to act as an MX Backup server to ensure that you can still accept mail if your main mail server is unavailable for any reason. The mail is queued on the backup server until the main server becomes available again, at which point it is automatically forwarded to it. It delivers messages only to a server with a higher priority MX record; the backup server itself must have a lower priority MX record. For details, see "How is the Mail Server Found?" on page 8.

14.6 Firewalls

GMS Firewall is a standalone product that can be used in conjunction with another mail server to protect your network from unauthorised access. It sits on a gateway machine and its main function is to pass mail arriving from the Internet onto your internal mail server and pass outbound mail out to the Internet. It also provides a WWW proxy service so that your users can browse the Web safely.

For details of how to set up a firewall, see "Configuring GMS as a Firewall" on page 193.

14.7 Network Address Translation (NAT)

You may wish to use GMS with a firewall that employs Network Address Translation (NAT). This allows you to hide internal IP addresses from the outside world and means a larger number of IP addresses are available to the internal network. There are a couple of things to bear in mind when using NAT with a mail server however. If an external ip address is translated to an internal IP address or the IP of the firewall that is doing the translation, GMS will see the connection as local and therefore allow relay for that connection. To prevent this you will need to either

- Configure your NAT software not to translate incoming addresses.
- Configure GMS to disallow relay for the address(es) that the external addresses are translated to. This can be done from the System Administration, Security, Local IP page by adding the address to exclude in the format !123.123.123.123 where !

means "not" and 123.123.123.123 is the address to be excluded from the local IP range.

15 Secure Sockets Layer (SSL)

GMS supports the use of Secure Sockets Layer for the transmission of messages. SSL is a system which uses a private key on the server to encrypt any data transmitted over the connection. To set up GMS to use SSL requires you to have two things.

- an SSL key (available from sales@gordano.com)
- a separate encryption certificate for each domain that is to use SSL. This can be a self generated certificate or a certificate obtained from an external certificate authority such as VeriSign.

15.1 Entering the SSL activation key

Once you have received your SSL activation key from sales@gordano.com enter it on the Licensing page following the instructions sent with the key.

15.2 Assigning a certificate

There is a utility in the Gordano\bin directory called Keycert.exe which should be run. This gives you three key options.

- Use existing certificate
- Generate CSR for submission to CA
- Generate Self-Signed Certificate for testing



CSR = Certificate Signing Request

CA = Certificate Authority

The following section explains how to use keycert.exe to set up a certificate.

SSL Key Certificate Generator (keycert.exe)

This utility will allow you to apply existing SSL Certificates that you may have obtained from external certificate authorities. You will need to know the names of the key and certificate files and the password associated with these files.

You may also generate a CSR for submission to an external Certification Authority. If you are generating a certificate request please take careful note of the filenames and password used as you may need these at a later date.

If generating a Self Signed Certificate please set an encryption strength by selecting the required number of bits to be used for the key from the drop down menu. The higher the number of bits, the more secure the key is. Also set a period in days that this certificate should be valid for. This can range from 1 day through to a maximum of 365 days.

While there is nothing wrong with self signed certificates users will receive a warning the first time they visit your server, they can then add this certificate to the list of trusted certificates in their browser.

Certificate File Location

By default all certificate/key pairs are stored in the `gordano\bin` directory, however you may if you wish specify a separate location either by using the Browse buttons or simply typing in the path to the files. By convention a key file has the extension `.pem` signifying the type of encryption used in the file and a certificate request file has the extension `.csr`

The names chosen for the key and certificate do not matter but both should be given the same name, only the extension being different, so that they are easily matched up if necessary in the future.

Common Name

Every certificate has a common name associated with it. This is normally the fully qualified name of the machine that the certificate will be used on. i.e. `host.domain.com`

If you wish to use a single certificate to cover a number of sub domains select the Use Default Certificate option. You may replace the hostname portion with a wildcard of `*`, i.e. `*.domain.com`

Company Information

Your Company Information is a required part of any certificate as they are required to accurately reflect the holder of the certificate. Anyone connecting to your server will be able to see these details so please make sure they are accurate.

Company Details

Again please fill out these details as accurately as possible, users connecting to your server will use these details to contact you regarding any queries they may have. For example, they want to email or call you to verify the authenticity of the certificate prior to accepting it. It is preferable that you also provide a contact name and telephone number although these details may be omitted if you so wish.

This information will be combined with the Common Name and Company Information provided earlier to give your server a unique identity. This unique identity is often referred to as the Distinguished Name of a certificate.

Pass Phrase

If you are using an existing certificate the pass phrase entered must match that already associated with the certificate.

If you are creating a request to send to a Certifying Authority please keep a careful note of the Pass Phrase entered, as once you receive your certificate you will need to refer to it when applying the certificate.

If you are creating a self signed certificate you may use whatever Pass Phrase you wish.

Enter the Pass Phrase a second time into the Confirm box to ensure that you have entered it correctly.

Press the Finish button to complete.

Make sure that you have entered your SSL key into GMS, stop and restart the services and you should now have an SSL enabled server.

15.3 Configuring GMS to use SSL

Once the certificate has been set up correctly and the GMS services restarted the next step is to tell GMS to start using SSL. The following is required.

ESMTP settings

Go to System Administration, Performance, ESMTP and check the "allow STARTTLS" option under both the Incoming and Outgoing sections.

Setting the secure ports

Next you will need to go to the System Administration, Performance, Ports page and check the ports that are used for secure connections. The IMAP and POP ports are set to the recognised ports for these services and should not be changed. The other ports on this page can be set to any available port that you wish. for instance you might set the WWW administration GUI SSL port to 8001. This means you can then access the GMS administration pages over a secure HTTPS connection for example <https://127.0.0.1:8001>.

The WWW WebMail GUI SSL Port refers to the GMS WebMail client. If set to 9001 connecting to <https://127.0.0.1:9001> from the server would display the WebMail login screen over a secure connection.

The WWW User GUI SSL port refers to the custom GUI that can be created in the `Gordano\MML\usr` directory.



All the port numbers you assign must be different and must not already be in use by another application or service. For example you can't set the WWW User GUI SSL port to the same value as the WWW WebMail GUI SSL port.



You will need to stop and start the GMS services before any port changes will come into effect.

Setting the POST SSL mode

If you want SSL to be used when messages are posted to the local or remote servers you will need to configure the SSL mode on the System Administration, Performance Delivery Rules page of the interface. There are three settings:

- 0 - Don't use SSL for this connection.
- 1 - SSL may be used for this connection if the remote server supports it.
- 2 - SSL must be used for this connection.

You can specify different rules for different receiving servers. For example if you only want SSL to be used for non- local mail you can add a rule that sets an SSL mode of 0 for all local mail and set all other rules to have an SSL mode of 2. This way all local mail would be delivered over an SSL connection and any mail to other servers would not be posted unless a secure connection to the remote server is available.

Configuring clients

Once you have finished configuring the above all you need to do is to configure your email clients to use SSL (if they support it). You will need to consult your client documentation to determine how this is done.



If you use GMS WebMail as your client no client configuration is necessary. Just make sure the SSL mode is enabled on the Ports page above.

Restricting Weak Connections

GMS provides two methods of restricting connections that do not support a sufficiently high enough cipher strength. Generally speaking there will be no need to amend these settings at all but certain industries have compliance requirements that must be met.

Standard Method

The standard RFC compliant method of restricting weak connections is to initially accept all connections and then politely decline to process any further requests if the negotiated connection is not of a high enough strength. This can be set by selecting the appropriate cipher strength from the drop down menu on the System Administration, Security, Connections page. Any connection not meeting the required strength will receive an error in response to any requests made after SSL negotiation.

Strict Method

For especially strict compliance regimes we also provide a method of simply not accepting any SSL connections which do not match your criteria at all. This requires the setting of a variable in the registry containing a list of the particular ciphers you wish to support. You will need to paste the appropriate string from those provided below into the variable and then stop and restart the GMS services.

Open regedt32 on the GMS server and navigate to HKEY_LOCAL_MACHINE\Software\InternetShopper\Mail\SSL\ and create a new string value called Ciphers. Paste the appropriate string from below into it depending on the minimum strength you wish to use. We would recommend the string supporting 128 bit and above as there are a lot of servers that still use 128 bit connections.

HKEY_LOCAL_MACHINE\Software\InternetShopper\SSL
Type: Reg_SZ
Key name: Ciphers

String for medium and high support (128bit or above):

ADH-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:ADH-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:AES128-SHA:ADH-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DES-CBC3-SHA:DES-CBC3-MD5:ADH-RC4-MD5:IDEA-CBC-SHA:RC4-SHA:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5

For high only (256bit or above):

ADH-AES256-SHA:DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:ADH-AES128-SHA:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA:AES128-SHA:ADH-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:DES-CBC3-SHA:DES-CBC3-MD5

Finally, you can produce your own list of SSL ciphers to use if you wish by running the OpenSSL client on the GMS server. You can get a list of high security cipher algorithms using the "OpenSSL ciphers HIGH" command, medium ciphers using the "OpenSSL ciphers MEDIUM" command etc. The strings provided above should work on all GMS installations, but if you have any issues with unsupported ciphers then the first step is to generate your own list and replace the above string with your own list. If you want to use both HIGH and MEDIUM you will need to concatenate the two lists provided by the OpenSSL client.

16 GMS on Complex Networks

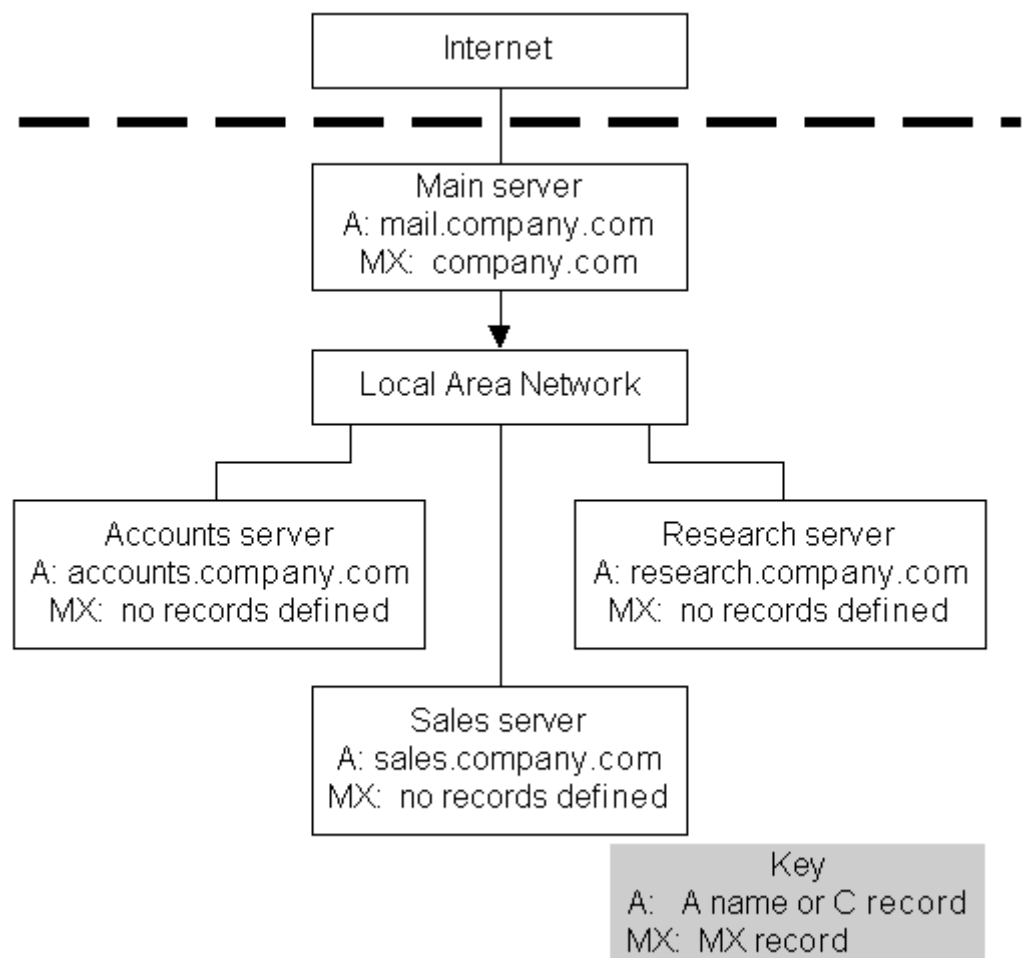
There are many situations in which you may have to set up GMS within a complex network of other mail servers. This section gives an overview of setting up GMS on such a network. It describes:

- Configuring multiple SMTP hosts.
- Configuring GMS as an MX backup server.
- Installing GMS on a bastion host.
- Configuring GMS as a firewall.
- Configuring multiple servers sharing a domain — normal forwarding and “round-robin”.
- Using multiple MX records.

16.1 Multiple SMTP Hosts

Where you have several mail servers networked together, GMS can be set up to act as a distributor for all SMTP mail.

Imagine a company with three departments, Accounts, Sales and Research, each with its own mail server. Although each department wants its own mail server, all users in the company must have an address of the form user@company.dom. Here is the setup:



The three departmental servers are connected to a main server which, in turn, is connected to the Internet.

This system can be configured in several ways but the best of these:

1. Stores all the user information on the main server, so there is only one user database to maintain.
2. Sets up the Accounts, Sales and Research servers to forward all mail to the main server. This is done by entering `main.company.dom` in the Unknown User action box under Domains & Users, Domain, Preferences.
3. Sets up a list of forwarding accounts on the main server so that it knows which server to forward mail messages to.

Potential problems and their solution

This setup has two potential problems:

- If a user called Joe in Accounts sends mail to Harry in Sales, the Accounts server has no user records and so forwards it to the main server. The main server accepts the mail and finds that Harry has a forward account to `harry@sales.company.dom`, so sends it to him there.
- A user may give their extended e-mail address (for example, `harry@sales.company.dom`), which could be incorrect for three reasons:
 - There is no MX record for `sales.company.dom`.
 - The company does not want external organisations to know their internal machine names.
 - There is a firewall in place which only allows incoming SMTP connections to the mail machine (that is, the main server).

To resolve these problems, MX records should be set for `accounts.company.dom`, `sales.company.dom` and `research.company.dom` as `mail.company.dom`. If this is done:

1. Any incoming mail for `harry@sales.company.dom` is delivered to `mail.company.dom`.
2. The main server forwards it to `harry@sales.company.dom`.

However, there is a problem since the MX record now points back to the machine it just came from. To overcome this, you would have to add entries for each to the Sending Rules. The rule for `sales.company.dom` would look like this, for example:

`SALES.COMPANY.DOM SALES.COMPANY.DOM 25 12`

For more details, see "Configuring outbound delivery rules (Smart Delivery)" on page 124.

Multiple site setup

It is possible to set up a system where the research department is actually at another site and its IP address is on the Internet. In this case the forward account would send the mail back out of the company, onto the Internet and to its final destination.

To do this:

1. Set up the research mail server to accept mail for company.dom even though the IP address (and/or real domain name) is not in the same domain as company.dom.
2. In the Sending Rules, enter the real domain name (for example, research_co.dom), this being the domain to which mail will actually be forwarded.

When users in the Research department send mail, it will be sent out directly or, if it is internal mail to mail.company.dom, using the Sending Rules. Here it will be forwarded to Sales or Accounts, as before. All mail for the Research department would be delivered via the main mail server, mail.company.dom.

16.2 Configuring GMS as an MX Backup Server

Configuring GMS as an MX Backup server is very straightforward. Do the following:

1. Install GMS on the backup server.
2. During installation, enter the fully qualified name of the machine as the domain that GMS should use. That is, enter backup.domain.dom.
3. Make sure that backup.domain.dom is listed as a lower priority MX record in your DNS configuration, which it would look something like this:

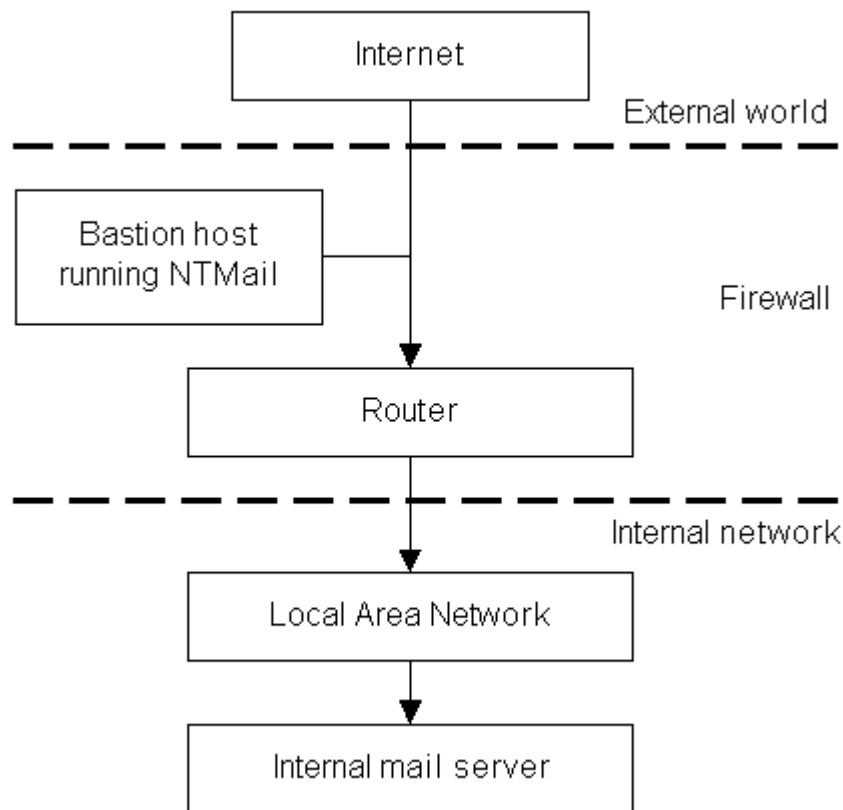
```
domain.dom. MX 10 mail.domain.dom.  
domain.dom. MX 20 backup.domain.dom.
```

Note the following:

- If mail.domain.dom is unreachable for whatever reason, all your mail is sent to backup.domain.dom where it is held until mail.domain.dom becomes available again. When this happens all mail held on the backup server is automatically forwarded to the main mail server.
- The GMS Firewall key only allows a single user to be added. This is the postmaster account created at installation time, which is necessary for configuration purposes.
- You can get a Firewall licence from sales@gordano.com. Simply install the same version as you are running on your main server on the backup server, obtain the key from sales and install it.

16.3 Installing GMS on a Bastion Host

Installing GMS on a bastion host is very simple. A typical setup is shown below:



In this example:

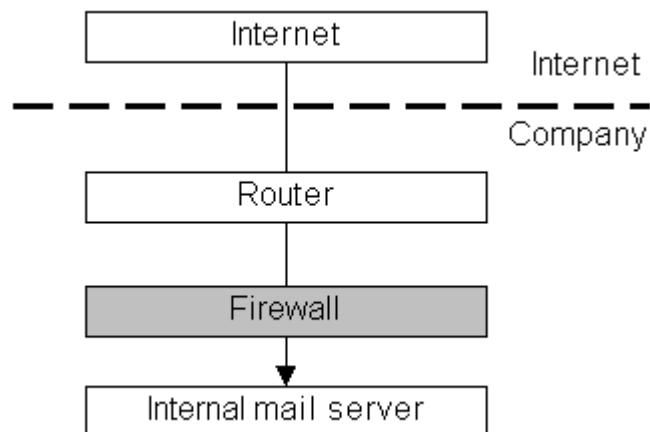
1. Configure the router only to allow SMTP connection from the bastion host to the Internal mail server, and vice versa. No other SMTP connections are allowed.
2. Give GMS your domain name (for example, company.dom) and set it to send all mail for unknown users to the Internal mail server.
3. Configure the internal mail server to send all outbound mail to GMS on the bastion host, which will, in turn, deliver it through the Internet.

The advantage of this configuration is that, if the Bastion host is compromised, only mail that is external to the company can be read. Also, as this mail was to be broadcast on the Internet in any case, it should be already regarded as potentially insecure. Internal company mail remains safe from access over the Internet behind the firewall.

16.4 Configuring GMS as a Firewall

The GMS Firewall package combines several mail servers by acting as a company's central e-mail distribution point.

Many companies will want to have a firewall between the Internet and their internal network. The simplest way to do this is to use a machine to stop traffic flowing from one network to the other, like this:



To configure GMS as a firewall:

1. Install GMS on the server that is to act as a Firewall. This machine should have two Network Cards installed on it, one for the public side having a public IP address and one for the private or internal side having a non-public IP address. Make sure that IP forwarding is deselected on both cards.
2. During installation enter the name of the domain that GMS should use, for example, domain.dom.
3. Make sure that domain.dom is listed as an MX record in your DNS configuration. It should look something like this:

domain.dom. MX 10 firewall.domain.dom.
4. Point your Web browser at <http://firewall.domain.dom:8000> and log in using the account postmaster@domain.dom and the password you supplied during installation.
5. Change the Unknown User Action for domain.dom to send all mail for unknown users to your internal mail server. The internal mail server in turn must be configured to post all external mail to firewall.domain.dom, which will in turn post it all out to the Internet.

You can get a Firewall licence from sales@gordano.com. Simply install GMS as normal, obtain the key from sales and install it. You are ready to start.



When installed in a Firewall configuration the GMS Server is able to protect any internal messaging server. If that server supports LDAP lookup of user accounts (as does GMS, MS Exchange, Lotus Notes/Domino etc. GMS Firewall can authenticate the internal accounts and reject mail for unknown users. Please see "LDAP authentication configuration" on page 75.

16.5 Multiple Servers Sharing a Domain

This section describes the different ways in which multiple servers can be set up. You can check that any setup is OK by tracing e-mail through the system, then work out whether a reply would be returned correctly. If you have a requirement for multiple servers across a single domain then you should also take a look at the load sharing options available in GMS.

Normal forwarding

This is a simple setup when a company has just two mail servers. It works as follows:

1. All mail for the domain is handled by one server, the main mail server.
2. If a message arrives for a user for which the main server does not have an account, it looks at the Unknown User Action parameter.
3. The Unknown User Action on the main server is set to pass the message to the second server.
4. The second server is in turn set to forward all mail to the main server for onward posting. Its unknown user action should be set to forward all mail for unknown users to a specific account.

Resource utilisation

You can specify *Sending Rules* which control how outgoing mail is sent to particular domains. This information is held in the Post Servers file, postservers.txt.

To change the sending rules, follow the procedure in "Configuring outbound delivery rules (Smart Delivery)" on page 124.

The round-robin setup

The purpose of round-robin is to allow use of multiple SMTP servers (with identical contents) in order to distribute the connection loads. Round-robin is not random, though it appears to give a random effect. It operates in a round-robin fashion (as the name implies), in that it rotates the return record sequence by one for each response.

One address is handed out, put at the end of the list, and then the next one is handed out for the next translation request. This procedure is similar to the behaviour of a translation list.

In round-robin DNS, a random IP address is returned with each request if multiple entries exist in the DNS using A records. Round-robin can only be achieved using A records, like this:

```
domain.dom. MX 10 server1.domain.dom.  
server1.domain.dom. A 123.123.123.1  
server1.domain.dom. A 123.123.123.2
```

The advantages of a round-robin setup are:

- Any Bind server that supports DNS round-robin can serve the A records for any host. Your nameserver doesn't need to be running on the host(s) where you want to run round-robin.
- You can take one of the server systems out of the loop for maintenance. A simple removal at the nameserver level from the round-robin list allows almost no apparent loss to the client systems (except for those that cache).

The disadvantages of round-robin are:

- Possible confusion at the user level. When one system fails, it appears to the user as intermittent failure because the service seems intermittent. As a result, once connected, a user is less likely to report a failure.
- It does not provide true load balancing.
- It does not automatically handle hosts that go down (manual modification of DNS zone files and reloading of DNS is required).

16.6 Using Multiple MX Records

All domain names set up to receive mail should have at least one MX record in DNS. We recommend that your ISPs mail server is also added in with a lower MX priority, so that if your server is unavailable for some reason mail will be held on your ISPs server until your own becomes available. A typical MX record might look like this:

```
domain.dom. MX 10 server.domain.dom.  
domain.dom. MX 20 server.isp.net.
```

This means that if anyone is sending you mail they should try server.domain.dom first and, if they cannot connect to that, they should send mail to server.isp.net to be held until the highest priority server is available. The lower the number, the higher the priority.

Each machine or server must also have an A record set in DNS

If you have more than one mail server and do not mind which one mail is delivered to, you can set both to have the same priority but

there is then no way of specifying which of the two you would rather receive mail at. An example would be the following:

```
domain.dom. MX 10 server1.domain.dom.  
domain.dom. MX 10 server2.domain.dom.
```

This is sometimes used erroneously in an attempt to set up a round-robin system using MX records (see above).

The correct way to do this would be to set up MX as in the first example above, but give server.domain.dom two A records set in DNS. If you had sufficient mail servers available, you could also act as your own backup MX as in the following example:

```
domain.dom. MX 10 server1.domain.dom.  
domain.dom. MX 20 server2.domain.dom.
```

16.7 Load Sharing

If you run a single domain with a large number of users running under it then you may want to consider using GMS' load sharing feature.

Load sharing allows you to split the load of your users across a number of machines so that none of them are over worked. You would normally only set it up through the GUI if you do not have an existing installation of GMS, if you do have an existing installation please take a look at the file loadshare.txt in the GMS base directory.

If all machines in the load sharing array are fresh installations of GMS then please read on.

Enable Load Sharing

Check the box to enable Load sharing or uncheck it to disable.

Primary Server Location

All servers in a load sharing array need to know the location of the Primary Server in the array. There can only be one primary server in each array, if it is to be the machine you are currently working on simply select Local Server, if it is to be one of the other machines in the array select Remote Server and enter the fully qualified name of the remote server, i.e. server1.domain.dom.

Redirect WWW Requests

Select this option if you would like WWW requests initiated by users to the wrong server to be automatically redirected to the server that actually holds their user account.

Logon Redirected WWW Requests

Used in conjunction with the Redirect option above this will, if checked, allow them to be automatically logged on to the correct server.

Maximum number of WWW redirects

This option is useful in the case where a user does not match any of the load sharing rules of any of the servers in the array. If this is the case it is possible for the redirect requests to loop round and round all the servers continuously. If this option is enabled these loops will be terminated once the number of loops specified here is reached.

Once you have set all of the options above you also need to go and set the rules that will be applied to user redirection amongst the servers in the Load Sharing array.

Rules

To set up the required rules for the Load Sharing array click on the Edit Rules button. The rules can get fairly complex but once set up there should be no need to change them. The rules set up here determine how the server treats requests for users that are part of the domain but are not local to this server. You need to enter a set of rules for each of the other machines in the load sharing array. For instance if the machine you are currently working on is called main.domain.dom and the array consists of 3 servers then you must enter rules here for the other 2 servers only.

The rules you set can use the expressions given in the table below along with wildcards to determine which server deals with which user. If each of the three servers were to deal with one third of the users each depending on the first character of the user names, main.domain.dom deals with users whose names begin with "a" through to "h", server1.domain.dom deals with those beginning with "i" through "p", and server2.domain.dom the remainder you would end up with two rules on each server as follows

main.domain.dom

[i-p]*@domain.dom
[q-]*@domain.dom

server1.domain.dom
server2.domain.dom

server1.domain.dom

[-h]*@domain.dom
[q-]*@domain.dom

main.domain.dom
server2.domain.dom

server2.domain.dom

[-h]*@domain.dom
[i-p]*@domain.dom

main.domain.dom
server1.domain.dom

[abc]	matches exactly one of the characters "a", "b" or "c"
[-m]	Matches exactly one character that is less than or equal to "m"
[m-]	Matches exactly one character that is greater than or equal to "m"
[a-m]	matches exactly one character in the range "a" to "m" inclusive
[expression, expression,...]	matches exactly one character in one of the expressions listed where each expression is in one of the forms listed above

No support will be available for matching multiple characters with these range options. Note that no spaces are allowed in the range specifications.

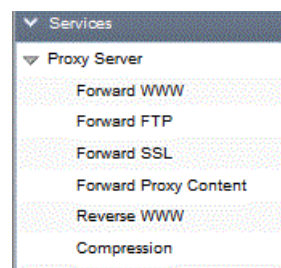
17 Providing Web Access

This section describes how to use the Web proxy facilities of GMS

This section describes:

- The facilities GMS provides.
- How to set up the proxy Web server — its cache, the MIME types it supports and its dial-up.
- How to configure Anti-Virus and Anti-Spam scanning on proxy content.

17.1 Facilities Available



GMS Proxy provides the following features:

- Forward Proxy — allows GMS to sit on an office Internet gateway and provide users' two most important requirements — delivery of Web pages and e-mail. This is ideal for use in a dial-up system.
- Anti Virus and Anti Spam Content Scanning — used in conjunction GMS Anti-Virus and GMS Anti-Spam the forward proxy can be configured to provide complete protection from malicious or undesirable web content.
- Reverse Proxy — allows GMS to provide boundary protection to your existing web server. Allows your web server to sit behind a firewall with the reverse proxy collecting the requested pages and serving them to the requester.
- Web Page Caching — helps reduce your bandwidth requirements by storing copies of frequently accessed files locally.
- Compression — allows the proxy server to compress data to enhance download times and reduce network bandwidth.

These features will be covered in detail in the subsequent sections of this chapter.

17.2 Configuring the Forward WWW Proxy Server

You configure the Web proxy server by selecting Services, Proxy Server, Forward WWW from the menu. There are three main elements to configure, the cache, authentication and MIME types.



Access to the WWW Proxy is limited to the IP addresses you have configured under System Administration, Security, Local IP. See "Adding addresses to the Local IP list" on page 175.

Parameters

To display the parameters which control how the cache stores and expires files, choose the Settings tab to display this page:

Settings | Mime Types | Bypass Sites | Bypass Requests | Bypass Responses

▼ Proxy

☐ Enable proxy server

Proxy host : John-VAIO

WWW Proxy port : 8080

☒ Enable proxy cache

Maximum page age : 0 hours

Page purge method : ☒ date cached ☐ date last used

Maximum cache size : 31 MB

▼ Authentication

☒ No authentication

Authentication method : ☐ Authenticate from user database ☐ Use fixed logon details

Username :

Password :

Authentication Type : ☒ Basic ☐ Digest

▼ Dialup

Connect using : Do not dialup

Retry using : Do not dialup

Disconnect delay : 2 minutes

Update Settings | Set to Default

You can specify the following parameters:

- WWW Proxy port — this the port your users browser should be configured to connect to, by default this is set to 8080 however any available port can be used.
- Maximum page age — the time after which data is removed from the cache.
- Page purge method — the means by which old pages are expired from the cache, either by the date they were last accessed (this is recommended) or by the date they were cached.

- Cache size — the maximum size of cache held on your local disk, in MB. If you have plenty of disk space, you may want to increase this from the default.

Cache

To view the cache contents, choose View Cache from the secondary toolbar.

To purge the cache:

1. Choose Purge Cache from the secondary toolbar.
2. In the "Keep last.... hours" box, type the number of hours' cache that you want to retain when you purge.
3. Select the Page purge method you want to use (see above for details).
4. Press the Purge Now button.

Authentication

By default GMS Proxy limits access to users within the local IP range, see "Allowing Relay" on page 152. GMS Proxy Authentication allows you to provide additional control over who can access the proxy by using the authentication options shown in the screen shot above.

Authentication Method

- No authentication
- Authenticate from user database — this option will require the user to enter their user account name and password when they first access the Internet via the proxy. The password will only be required on the first access, subsequent requests from the same browser window will not require the password to be entered again.
- Use fixed logon details — Enter a Username and password you wish to be used by all of your users. As mentioned above these will only be required on the first access, subsequent requests from the same browser window will not require the password to be entered again.

Authentication Type

- Basic — this option passes a base64 (Plain Text) encoded string to the proxy server, that contains the user name and password. Passing passwords in plain text is not a particularly secure method therefore this option should be used with caution.
- Digest — Digest authentication is a challenge-response scheme that challenges using a nonce (a server-specified data string) value. A valid response contains a checksum of the user name, the password, the given nonce value, the HTTP method, and the requested Uniform Resource Identifier (URI). This method provides greater security.

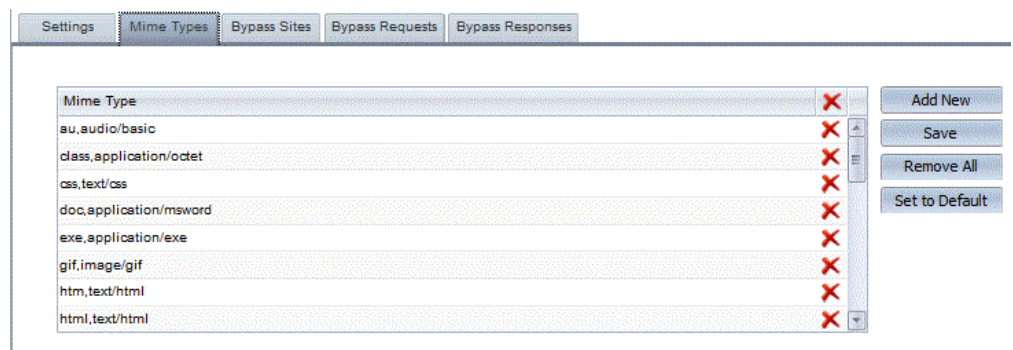
Note: Digest authentication cannot be used if you have configured your user authentication to use an external data source, for instance NT Sam or SQL.

MIME types

The Web proxy server automatically recognises a number of MIME (Multimedia Internet Message Exchange) file types. To list these, choose the MIME Types tab.

To add a new type:

1. Choose the MIME Types tab to display this page:



2. To enter a new Mime Type click on Add New then type the extension the type is known by (without the dot) and a description (separate by a comma) in the text area that opens then press Enter. For example, the extension might be "gif" and the description "image/gif".
3. Click the Save button to confirm the changes.

To remove a MIME type:

1. Choose the MIME Types tab.
2. Select the type in the list and click on the Delete button.
3. Click the Save button to confirm the changes.

To remove all MIME types click on the Remove All button.

1. Click the Save button to confirm the changes



The process of adding and removing entries can also be applied to other sections of this chapter.

Dial-up

You can configure the proxy dial-up parameters.

To configure dial-up:

1. Choose the Settings tab to display the page shown above:

2. In the "Connect using" drop-down list, choose one of these:
 - If psapi.dll is available and installed in the GMS directory, select MyDialUpServer.
 - If psapi.dll is not available and you need to initiate a RAS dial-up to collect mail, select "Proxy custom dialup" then press the Custom button. In the Schedule window which appears, type the phone number and your ISP account details.
 - If you use a dial-on-demand router, select "Do not dialup".
3. Press the Custom button if you need to set up account parameters. Type in values and press Update to return to the Dialup page.
4. In the "Retry using" drop-down list, choose one of the three methods listed above as the method to use if the first attempt fails. If you do not want to retry, select "Do not dialup".
5. The "Disconnect delay" box shows how long the connection is kept open for after sending and receiving of e-mail finishes. Do not reduce this to zero.
6. Press the Update button to effect your changes.

17.3 Configuring the Forward FTP Proxy Parameters

There are only two configuration options for the FTP Proxy.

Enable Proxy Server

Check or uncheck the box to enable/disable access to proxying of FTP connections.

Use FTP Shortcuts

Only used if proxying of ftp connections is enabled this option allows much quicker access to FTP sites, but it may also lead to more errors as there is no checking done for correct responses from the remote FTP server.

17.4 Configuring Forward SSL Proxy Parameters

Selecting this option allows SSL connections through the GMS Proxy. This option is required if your users require access to SSL sites.

The screenshot shows the 'SSL Proxy' configuration window. At the top, there is a checkbox labeled 'Enable SSL proxy server'. Below this is a table titled 'Ports to Use' with a red 'X' icon in the top right corner. The table has one row with the value '443' and a red 'X' icon in the right column. To the right of the table are three buttons: 'Add New', 'Save', and 'Remove All'. At the bottom of the window are two buttons: 'Update Settings' and 'Set to Default'.

Ports to Use	
443	

By default SSL uses port 443, however you can configure any port you wish to use. To edit the existing port double click on it, enter a new port number and press Enter.

To add a new port click on Add New and enter a new port number in the text area that opens then press Enter.

Click on Save to confirm your changes.

17.5 Configuring Forward Proxy Content Scanning

In conjunction with GMS Anti-Virus and GMS Anti-Spam the proxy server can be configured to protect the network from malicious and undesirable content. This is ideal if you allow users to browse the Internet or access their own private WebMail accounts with insecure providers, as it will protect your network from the risk of these users downloading viruses to their workstations.

Bypass sites.

This section allows you to specify sites you do not wish to be

The screenshot shows the 'Trusted sites' configuration window. At the top, there are three tabs: 'Settings', 'Trusted', and 'Banned'. The 'Trusted' tab is selected. Below the tabs, there is a section titled 'Trusted sites' with a dropdown arrow. Inside this section, there is a large empty rectangular box with the text 'No items to show.' in the center. To the right of this box are three buttons: 'Add New', 'Save', and 'Remove All'. Below the 'Trusted sites' section, there are two expandable sections: 'Trusted requests' and 'Trusted responses', both with upward-pointing arrows.

scanned for viruses. This will reduce server workload if you have a busy server and you are confident the sites are known to contain safe content.

To add a site click on the Add New button then enter the full URL (<http://domain.com>) and press Enter, repeat for each site. Click Save to confirm your changes.

To ensure virus scanning is enabled please see "Virus Scanning" on page 207.

Banned Sites

This section allows you to specify sites you wish to prevent users from accessing via the proxy.

The screenshot shows the 'Banned sites' configuration window. At the top, there are three tabs: 'Settings', 'Trusted', and 'Banned'. The 'Banned' tab is selected. Below the tabs, there is a section titled 'Banned sites' with a dropdown arrow. Inside this section, there are two checkboxes: 'Enable IP address lookup' (which is checked) and 'Ban IWF identified sites' (which is unchecked). Below these checkboxes is a large empty rectangular box with the text 'No items to show.' in the center. To the right of this box are three buttons: 'Add New', 'Save', and 'Remove All'.

To add a site click on the Add New button then enter the full URL (<http://domain.com>) and press Enter, repeat for each site. Click Save to confirm your changes.

Note: Wildcards "*" can be used to specify all variants of a domain name, for example http://*.yahoo.* will prevent access to any Yahoo site

Banned Requests

Banned requests allow you to specify attachment types you wish to prevent your users from downloading via the proxy server.

- Use banned attachments list — Select this option if you wish to use the existing banned attachments list you may have configured within GMS Anti-Spam, see “Ban attachments” on page 262.

Alternatively you can click on Add New and specify a file extension then press Enter. Repeat for each extension you wish to add. Click Save to confirm your changes.

Note: File extensions should be entered without the “*.” therefore to ban “.exe” extensions you should enter “exe” only.

Banned Responses

Banned responses allows you to specify response or MIME types that you do not want your users to access.

It is possible for a web server to provide a modified HTTP header, thereby letting virus-infected content pass through the proxy by disguising the true content type of the file being downloaded.

An example of a response type is:

application/msword

If a URL request returns a MIME-type that is in this list it will be blocked. This is a good way of blocking inappropriate content such as content streaming, movies or internet radio for example. It would not be advisable to ban the MIME-type text/html or image/*.

- Use banned content type list — Select this option if you wish to use the existing banned content type list you may have configured within GMS Anti-Spam, see “Content Types” on page 264.

Alternatively you can click on Add New and specify a content type then press Enter. Repeat for each content type you wish to add. Click Save to confirm your changes.

Note: The list must be in lower case.

Virus Scanning

GMS Proxy allows you to configure virus scanning upon the content retrieved via the proxy.

This can provide you with security from viruses which may be contained in web pages or from email content accessed via third party WebMail servers.

- Enable Virus Scanning — This option is available if you have installed and configured GMS Anti-Virus as your virus scanning

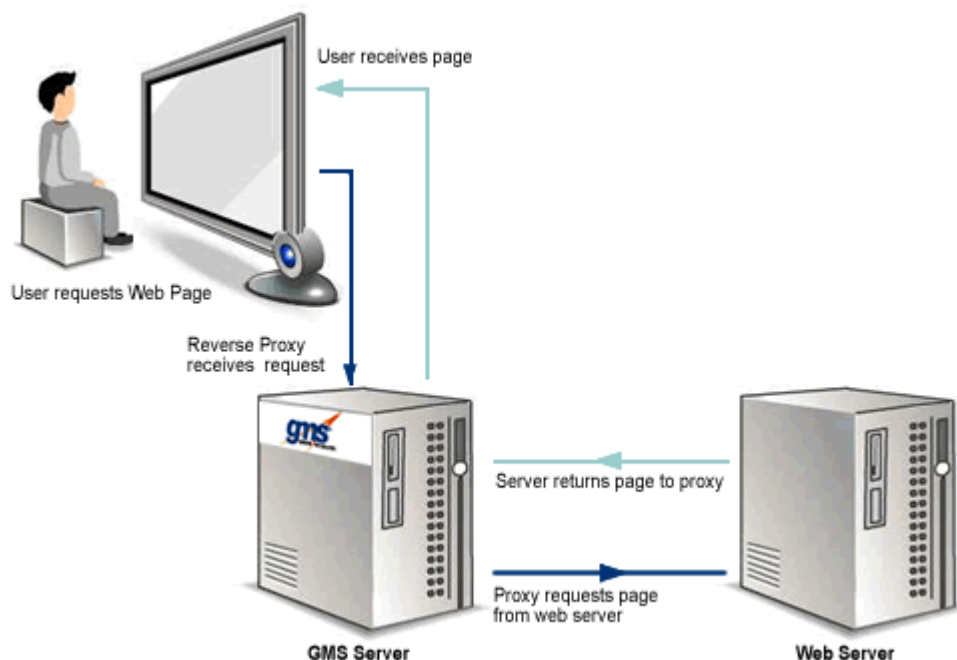
product. Enabling will virus scan all inbound and outbound traffic through the proxy server.

- Allow partial content download — A potential exploit used by the creators of viruses is to split files into segments to bypass virus scanning. Once the files are downloaded and the file is recompiled the virus is present, therefore it is advised this option should remain de-selected to secure against this exploit.

Virus scanning of proxy content is configured under Services, Proxy Server, Forward Proxy Content, Settings.

17.6 Configuring the Reverse WWW Proxy Server

GMS includes a Reverse Proxy server. Reverse proxy provides both boundary protection to protect your web server and load sharing when used in conjunction with other forward proxy servers.



The diagram shows how the process takes place when used as boundary protection.

1. The user requests the required web page
2. The reverse proxy receives the request from the browser and checks its Hosts table to ensure it is acting as a reverse proxy for this site.
3. The reverse proxy requests the web page from the web server.
4. The reverse proxy returns the required page to the users browser.

This process allows you to place the GMS server in a DMZ hence protecting the web server from potential attacks.

Parameters

To display the parameters which control how to activate the reverse proxy and how the cache stores and expires files, choose Services, Proxy Server, Reverse WWW, Settings to display this page:

Settings Hosts

☐ Enable reverse proxy server

Reverse proxy host : John-VAIO

Reverse proxy port : 81

Reverse proxy SSL port : 444

☒ Enable reverse proxy cache

Maximum page age : 0 hours

Page purge method : ☒ date cached ☐ date last used

Maximum cache size : 31 MB

Update Settings Set to Default

The following options can be configured

- Enable reverse proxy server — Select this option to enable the reverse proxy.
- WWW Reverse Proxy port — Enter the port you wish to accept connections on for standard HTTP connections. This value is set by default to port 81 to prevent port conflicts. You should change this port to 80 if you are intending to receive HTTP connections.
- WWW Reverse Proxy SSL port — Enter the port you wish to accept connections on for SSL (HTTPS) connections. This value is set by default to port 444 to prevent port conflicts. You should change this port to 443 if you are intending to receive SSL connections.
- Maximum page age — Specify the maximum proxy cache data age in days
- Page Purge Method — Page purge allows you to specify if the maximum page age is applied to:
 - Date cached - The maximum page age will be calculated from the date the file was originally cached.
 - Date last used - The maximum page age will be calculated from the date the file was last used.
- Maximum cache size — Enter the maximum proxy cache size in MB, the default is 32 MB but if you have plenty of disk space available you may want to increase this.

After changing any of these settings, click on the Update button to enter the new values for immediate use. Or you can use the Set to Default button to quickly return to the initial values.

Cache

To view the cache contents, select the View Cache button in the secondary toolbar.

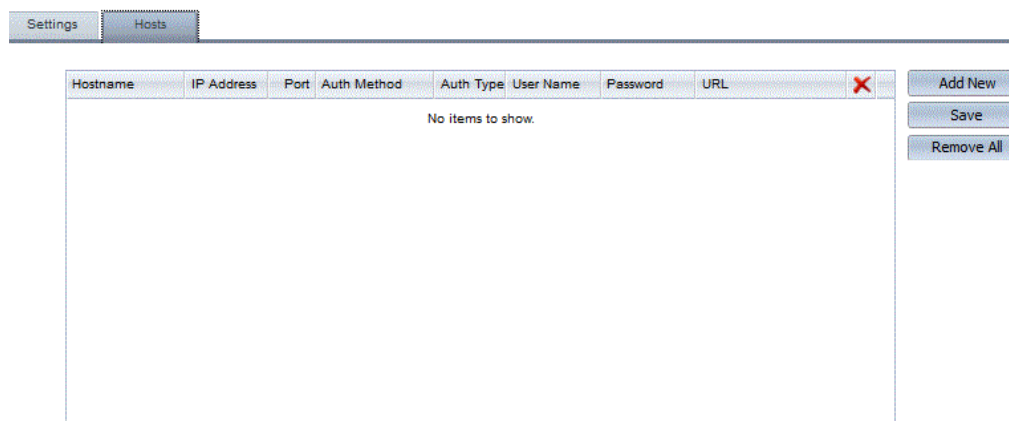
To purge the cache:

1. Select the Purge Cache button in the secondary toolbar.
2. In the "Keep last.... hours" box, type the number of hours' cache that you want to retain when you purge.
3. Select the Page purge method you want to use (see above for details).

Press the Purge Now button.

Hosts

This section enables you to add, edit and remove sites you wish to act as a reverse proxy for.



You must ensure the DNS records for the hostname are reconfigured to direct requests to the Reverse Proxy server

To add a new host click on the Add New button which will open a new dialogue displaying the page shown below.



To add a host

- Hostname - Enter the fully qualified domain name for the website you wish to act as a reverse proxy for. For example `www.gordano.com`.
- IP address - Enter the IP address of the Web Server for this host.
- Port - Enter the port that connections should be made upon on the destination web server.
- Security Type - This option specifies the type of connections used between the reverse proxy and the host. There are three connection options available:
 - NONE - Uses standard HTTP connections providing no security.
 - ANY - Uses either TLS (SSL) or standard connections as required.
 - TLS - Uses TLS (SSL) only.
- Authentication Method - GMS Proxy provides three authentication options, they are:
 - NONE - This option allows any connection from a local IP address to use the proxy.
 - USER DATABASE - Selecting this option forces the user to enter their user name and password to gain access to the proxy server.
 - FIXED LOGON - This option allows you to set a specific user name and password that all users who wish to access the proxy must use. Enter the user name and password you wish your users to use in the text boxes and click Update to confirm.
 - URL - The URL authentication option is unique to the reverse proxy and allows the password for a user to be obtained from the response header clause from a specified URL.
- Authentication Type - GMS Proxy provides two types of authentication, they are:
 - Basic - Basic authentication uses a base64 (Plain Text) encoded string that contains the user name and password. This is not a particularly secure method of passing a Username and password.
 - Digest - Digest authentication is a challenge-response scheme that challenges using a nonce (a server-specified data string) value. A valid response contains a checksum of the user name, the password, the given nonce value, the HTTP method, and the requested Uniform Resource Identifier (URI). This method provides greater security.

Note: If you are using an external user authentication method such as NT Sam or SQL authentication you must select Basic.

- Username - Enter the Username if you have specified the Fixed logon authentication method above.
- Password - Enter the password if you have specified the Fixed logon authentication method above.
- URL - Enter the URL for the page the authentication request should be sent to.

Click the Save button to confirm your settings or click the Cancel button return to the host listing.

To edit a host double click on the entry you wish to edit where the entries explained above can be edited.

To delete an entry, highlight the required record and click on the Delete button to permanently remove the entry or the Remove All button to delete them all.

17.7 Configuring Proxy Compression

Both the GMS forward and reverse proxy servers will support compression of pages into cache to accelerate download times upon a cache hit. These pages are decompressed and displayed by the browser in their original form once requested.

Requests

The Request section provides a list of file extensions for which a compressed version of the page should be created and served from the cache where possible.

The screenshot shows a web interface with four tabs: 'Request', 'Response', 'Bypass Request', and 'Bypass Response'. The 'Request' tab is selected. Below the tabs is a large rectangular area containing the text 'No items to show.' To the right of this area are four buttons: 'Add New', 'Save', 'Remove All', and 'Set to Default'.

If you wish to add specific files for the proxy server, click on Add New and enter the attachment type, ensuring that you enter the letters only, for example PDF, in the text area. To remove an entry highlight it in the list and click the Delete button. All entries can be removed at once by clicking the Remove All button. Click the Save button to save any changes.

Some file types are already compressed such as jpg and gif, therefore there will be no benefit in adding those to the list. Wildcards are supported.

By default this list is empty. To return to the default setting click the Set to Default button..



Certain file types such as "js" (JavaScript) and "css" (Cascading Style Sheets) can cause problems with specific browsers therefore it is not advisable to add these to the list.

Responses

The Responses tab provides a list of MIME types for which a compressed version of the page should be created and served from the cache where possible.

The screenshot shows the 'Responses' tab selected. The main area contains a text input field with 'text/*' and a red 'X' icon. To the right of the input field are four buttons: 'Add New', 'Save', 'Remove All', and 'Set to Default'.

If you wish to add specific MIME types for the proxy server, click on the Add New button then enter the MIME type in the text area provided and press Enter, an example response type is:
application/msword

Click the Save button to save any changes.

Wildcards are supported.

This list will contain text/* by default.

Bypass Requests

The Bypass Requests tab provides a list of file extensions for which page compression should be bypassed.

The screenshot shows the 'Bypass Requests' tab selected. The main area contains a text input field with 'No items to show.' To the right of the input field are four buttons: 'Add New', 'Save', 'Remove All', and 'Set to Default'.

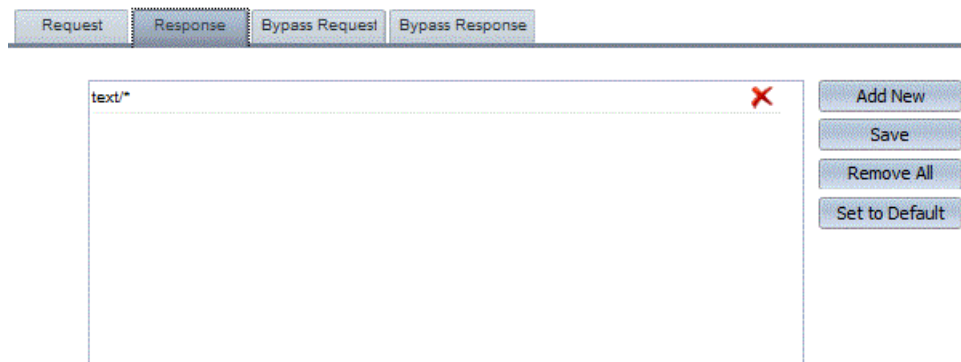
If you wish to add specific files for the proxy server, click on Add New and enter the attachment type in the text area, ensuring that you enter the letters only, for example pdf, and press Enter. To remove an entry highlight it in the list and click the Delete button. All entries can be removed at once by clicking the Remove All button. Click the Save button to save any changes.

Wildcards are supported.

This list is empty by default and takes precedence over the Compressible Request File Extensions list, see "Requests" on page 212.

Bypass Responses

The Bypass Responses tab provides a list of MIME types for which page compression should be bypassed.



If you wish to add specific MIME types for the proxy server, click on Add New and enter the MIME type, for example application/msword, in the text area and press Enter. To remove an entry highlight it in the list and click the Delete button. All entries can be removed at once by clicking the Remove All button. Click the Save button to save any changes.

Wildcards are supported.

This list will contain text/* by default as some browsers do not correctly handle this when compressed. This list takes precedence over the Compressible Response MIME Types list.

18 E-mail Clients

This section aims to help system or domain administrators who may set up mail clients for their users. It is not a substitute for the mail clients' own documentation.

This section:

- Describes the password server.
- Describes advantages and disadvantages of POP3, IMAP4 and Web browser clients.
- Gives some hints on how to set up some common POP3 and IMAP4 mail clients. For more detailed information, refer to the documentation that comes with the mail client.
- Explains the valid formats for account names in virtual and full domains.

Examples in this section use the following information:

- Mail Server Name — mail.company1.dom.
- Mail Domain — company1.dom.
- Account Name — user.
- Account Holder's name — Joe Bright.

Please see the GMS Users Guide for instructions on setting up Microsoft Outlook to work with the GMS Collaboration Server.

18.1 POP3, IMAP4 or Web Browser?

GMS Mail lets you access your e-mail using any one or all of these options (for an introduction, see "Methods of Collecting E-mail" on page 12). To help you choose the best solution, the following table lists the main advantages and disadvantages of each method of reading e-mail:

Metho d	Advantages	Disadvantages
POP3	<ul style="list-style-type: none">• Many mail clients to choose from.	<ul style="list-style-type: none">• All mail stored on PCs, making backup difficult.• Software maintenance cost high (installed on every PC).• More than one vendor required for mail solution (separate server and client).• Mail can only be read from one location.• Availability of additional clients may cause user to install their own software, increasing help desk costs.• Hot-desking not possible.• May need to increase disk size on many machines to cope with mail.

Method	Advantages	Disadvantages
IMAP4	<ul style="list-style-type: none"> • Some mail clients to choose from. • All mail stored on central server, making backup easy. • Mail can be read from many locations - although software needs configuring at each location independently. • Users can share mailbox. • Hot-desking possible. • Only one machine upgrade required to increase mail storage capacity. 	<ul style="list-style-type: none"> • Software maintenance cost high (installed on every PC). • IMAP4 standard is still undergoing rapid changes. • More than one vendor required for mail solution (separate server and client). • Server requires enough disk space for all e-mail to be stored. • Availability of additional clients may cause user to install their own software, increasing help desk costs.
Web Browser	<ul style="list-style-type: none"> • No software on PCs other than Web browser — reduces maintenance costs. • All mail stored on central server making backup easy. • Solution from one vendor reduces risk. • Mail can be read from any location. • Consistent interface reduces user help desk costs. • Hot-desking possible. • Only one machine upgrade required to increase mail storage capacity. 	<ul style="list-style-type: none"> • One interface available. • Server requires enough disk space for all e-mail to be stored.

18.2 Thunderbird

This section gives tips on setting up the Mozilla Thunderbird Mail client to work with your server.

If you are installing Thunderbird for the first time you will be asked for your account information during the installation process. You should use the same information as provided here although you will still need to complete the following steps to finalise the setting up of your account.

Open Thunderbird and choose Tools, Account Settings from the main menu. Under Account Action at the bottom left of the screen choose Add Mail Account. This will open a new dialogue allowing you to enter the details of the account you wish to add as follows:

- Your Name — enter the name you wish to be known as.
- Email Address — enter the email address of the account on the GMS server.
- Password — enter the password for the new above account, and check the Remember Password option.

Once you have completed the above details click on the Continue button.

Thunderbird will now try and auto detect your server settings using it's own database or via DNS lookups. If it fails to find them you can use the Manual Config option to enter them yourself or you to change the default settings but this should not be necessary. If you have multiple accounts on the same server it is best to just use a single outgoing SMTP server.

You should be given the option of using IMAP or POP for mail collection, we recommend the use of IMAP as this will maintain your mailbox on the server and allow access via WebMail if you do not have your mail client to hand. It also allows access to the account from multiple devices such as smart phones. If you opt for POP messages will be removed from the server and not accessible from other clients or devices.

Once the account is created you should select it and see your inbox being populated. You may need to right click on your account in the tree on the left and select Subscribe to access any additional folders that exist on your account in addition to the standard IMAP folders.

There are a number of additional settings you can change for your account to ensure Thunderbird operates in the way you would like. To access these select Tools, Account Settings again.

- Account — allows you to change your account name, your own name, set signatures, Outgoing Mail Server and so on.
- Server Settings — contains most of the important information relating to the operation of your account, security levels, how messages are handled etc..

- **Copies & Folders** — Covers options for saving sent mail, automated copying of replied to another account, Archiving of messages etc.
- **Composition & Addressing** — options relating to writing and addressing messages including use of additional address books.
- **Junk Settings** — determines how messages that Thunderbird thinks are spam are handled.
- **Synchronisation & Storage** — determines whether messages are also stored locally, this is useful if you have to work offline at any time. Also provides various options for minimising disk space usage.
- **Return Receipts** — various options for handling return receipts. From a security perspective it is not a good idea to enable automated responses to incoming messages as this can be used to confirm your address thereby making you more valuable to spammers.
- **Security** — allows for digital signing and encryption of messages.

Additional Features

Thunderbird has a number of advantages over other third party mail clients especially if you have the GMS Collaboration option enabled on your server.

- It can integrate with GMS address books via LDAP
- It can integrate with GMS calendars by using the Lightning calendar plug-in

Usage of both of these are described more fully in the GMS User Guide.

18.3 Microsoft Office Outlook Setup

Microsoft Outlook is part of MS Office. Be sure to install the latest patches from Microsoft.

To set Outlook up:

1. Go to Start > Control Panel and select the Mail Applet (You may need to alter the view to small/large icons)
2. A small window with some options will appear, click on Show Profiles
3. Click Add... in the profile window
4. Name your profile and click OK.
5. Click on Manual Setup or additional server types and click next
6. Select POP or IMAP and click next
7. Do the following:
 - Type your name as you wish it to appear in the Full name field, in our example this is "Joe Bright".
 - Type your e-mail address, "usera@company1.dom", in the field e-mail address.
 - Type your account name — your POP/IMAP Username (usera).
 - Type your password in the Password field.
 - Press Advanced Options, enter the SMTP server "mail.company1.dom" and press OK.
 - Check that the Internet Mail server is your assigned IMAP/POP server.
8. Press OK twice.
9. All other settings are preferences. If you were missing any components like Internet mail, see the startup and component section.

18.4 MS Outlook Express Setup

MS Outlook Express is part of the Internet Explorer installation. Be sure to install the latest patches from Microsoft.

To set Outlook Express up:

1. Start the MS Outlook Express program.
2. Press Tools on the menu bar and then the Accounts option.
3. Click the tab labelled Mail.
4. If you do not have any Mail Accounts listed press the Add button and choose Mail. (If your account is already listed go to step 5). The Add wizard settings are as follows:
 - Enter your name as you would like it to appear in the Name field, that is "Joe Bright", and press the Next button.
 - Enter your e-mail address, "usera@company1.dom", and press the Next button.

- Choose POP3 for the option 'My incoming mail server is.' In the "Incoming Mail (POP3 or IMAP) Server" field, enter your POP server "mail.company1.dom"
 - In the "Outgoing Mail (SMTP) Server" field, enter your SMTP server, again "mail.company1.dom". Press the Next button.
 - Choose the option Log on using: and enter your POP Username in the POP account field and your login Password. Press the Next button.
 - Type the name you want for the account name, "Joe Bright", and press the Next button.
 - Choose the Connect option you want to connect to the Internet using and press the Next button.
 - Press the Next button, then press Finish.
5. To access your mail settings without using the Setup wizard:
- Highlight your existing account name and choose Properties.
 - Under the General tab enter your Name ("Joe Bright") and Organization. For both E-mail address and Reply address, type "usera@company1.dom".
 - Click the Servers tab and verify the following:
 - Enter your SMTP server, "mail.company1.dom", in the Outgoing Mail (SMTP) field.
 - Enter your POP server, "mail.company1.dom", in the Incoming Mail (POP3) field.
 - Choose the option Log on using.
 - Enter your POP Username, "usera", in the Account field.
 - Enter your password in the Password field.
 - Click the Connection tab and specify you preferred means of connecting to the Internet.
 - Do not modify the Security tab settings.
 - Click Advanced Options and leave the port numbers at their default (110 for POP and 25 for SMTP). Do not check "Leave copy of messages on server" or your mailbox may fill up.
 - The rest of the Advanced options are preferences so press OK for these.

18.5 Mobile Device Mail Clients

There are many different types of mobile clients and most of them will contain a mail client, and will also allow you to install third party mail clients via the relevant app store. For the purposes of this user guide we will outline how to set up the default mail client that ships with Android 4.0 otherwise known as Ice Cream Sandwich.

To begin configuring the mail client open Apps and then select the Email app. The first time you open the App you will be presented with a screen allowing you to configure the account it should work with.

Enter the fully qualified account name and the password associated with that account. This will normally be the same information you enter in your normal desktop client. Once entered click on **Next** at the bottom of the screen and then select "IMAP account" from the following screen.



If you will also access this account from another device or client be sure to not select "POP3 account" as the POP protocol will remove the messages from the server and thus they will be unavailable to the other client.

This will open a further screen allowing you to continue configuring the IMAP settings as follows:

- **Username** - the domain portion of the account you entered previously will have been removed. Please re-instate it so the entry looks like username@domain.name
- **Password** - there should be no need to change this
- **IMAP Server** - this will have defaulted to imap.domain.name. If this is not correct you will need to change it, your System Administrator will be able to advise you, or simply copy the settings in your desktop client.
- **Security type** - If your email provider supports it we would recommend using SSL security, and as you know where you are connecting to that you do not worry unduly about the type of certificate. Select the option "SSL (Accept all certificates)".
- **Port** - this will depend on your choice for the security type above. The standard IMAP port of 143 should be used for all of the options other than SSL, for which you should use a port of 993
- **IMAP path prefix** - please leave this blank unless you are advised otherwise by your system administrator

When complete click on **Next** to continue setting up the account by configuring the SMTP settings as follows:

- **SMTP server** - this will have defaulted to mail.domain.name. If this is not correct you will need to change it, your System Administrator will be able to advise you, or simply copy the settings in your desktop client.
- **Security type** - If your email provider supports it we would recommend using SSL security, and as you know where you are connecting to that you do not worry unduly about the type of certificate. Select the option "SSL (Accept all certificates)".
- **Port** - this will depend on your choice for the security type above. The standard IMAP port of 143 should be used for all of

the options other than SSL, for which you should use a port of 993

- **Require sign-in** - as you are using a mobile device it is highly unlikely you will be connecting from a known IP address, therefore you will likely fail a lot of the security checks on the mail server. Selecting this option allows authentication to the server allowing you to be treated as if you were on a local client
 - **Username** - the fully qualified username to authenticate with. Normally your email address
 - **Password** - the password for the above account

When complete click **Next** to continue setting up the account options as follows

- **Email check frequency** - select the desired frequency from the drop down. The more frequent the check the greater the impact on your battery life
- **Sync Email** - selecting this option will ensure that your mobile device and the account on the server are kept synchronised with each other
- **Notify me when email arrives** - if selected your mobile device will notify you when a new email is available, so there is no need to keep checking your device
- **Automatically download attachments when connected to WiFi** - some attachments can be very large, and some WiFi connections very slow. Unless you are confident in the speed of your WiFi connection we would recommend that you leave this option unchecked. Attachments will then only be downloaded when you request them.

When complete click **Next** to open the final screen where you can name the account and provide your personal details.

- **Give this account a name** (Optional) - if you are setting up multiple accounts on the mobile device it is important to give them names allowing you to distinguish between them. This can be anything you like as it is not used anywhere else
- **Your name** (displayed on outgoing messages) - This is the name that will appear in the From field of any messages you send from the device. If you also use a desktop mail client then it would normally be the same name as you have set there

Finally click on **Done**. The email account is now set up and ready for use. It will automatically connect to your server and obtain an up to date copy of all email in your inbox. Further connections will depend on the Email check frequency you set above.



If you use a third party mail client the process for setting it up will be very similar to the above. If this client supports the IMAP IDLE command we would recommend using this over setting a frequency to check for new email, it is much lighter on resources and you will get immediate notification on the arrival of new email.

18.6 Virtual domain users

If you are setting up a client for a user who is in a virtual domain you can specify their account name in three ways as below:

1. username@virtual.dom
2. username.postfix
3. username.postfix@full.dom

This is different to normal domains where the account name takes one of the following forms:

1. username@full.dom
2. username

19 SMS and Pager Gateway

The SMS (Short Message Service) gateway is a service for sending short text messages to mobile phones. The pager gateway provides the ability to send messages to specified pagers and also to receive messages from SMS devices directly into an email account, this is often referred to as 2-Way SMS.

The SMS Gateway provides a gateway from your server to a SMS broker, who will forward these messages to their specified destination.

GMS allows you to configure this option in two different ways depending upon the software licenses you have.

This section provides information on:

- Enabling the DLL (GMS Mail)
- Choosing the gateway to use (GMS WebMail)
- Allowing users access to SMS



Before you can configure the SMS Gateway you will require an active account with an SMS broker.

The process to configure the pager gateway is identical to the configuration of the SMS gateway, therefore the latter is described here only.

19.1 GMS Mail configuration

Enabling the DLL

Before the SMS Gateway can be configured it must be assigned to a mail account. The following stages provide details on how the SMS Gateway is enabled.

- **Create the user account**
Go to Domains & Users, Domain and select New User from the secondary toolbar, enter a username and password for the account you are creating. Click **Add**
- **Select the DLL**
Select the user you just created under the domain and then the

Mail Processing tab and from the "Select DLL" drop down list select SMS Gateway. Click **Configure**



- **Configuring the DLL**

To configure the SMS Gateway you must have a valid account with an SMS broker. A list of suggested brokers is available in the "Gateway" select box.

- Via Phone Number - Select this option to restrict all SMS messages to a single specified phone.
- Via Access File - Select this option and click "Edit Access File" to configure rules on which phones receive messages from specified users. "Editing the access file" on page 227
- Gateway - Select the gateway for the broker you are using.
- Username - Enter the username for the account with the selected broker
- Password - Enter the password for the account with the selected broker



By default the access file will allow messages to be sent by any user to any phone. You can control access to use the gateway via profiles to restrict usage.

- Click **Update** to confirm the settings.

The SMS DLL is now configured.

Editing the access file

Rules can be configured to specify which users can use the SMS dll

Access	Email Address	Telephone	Cost Group
<input checked="" type="checkbox"/>	*	*	1

Buttons: Add, Save, Cancel

and which mobile phones their messages are sent to.

Access - Select this option to activate a rule

Email address - enter the message originators email address here. You may use the * wildcard if required.

Telephone - Enter the specific number the SMS messages should be sent to for the specified email address. You may use the * wildcard if required.

Cost Group - If you wish to track SMS usage you can enter a cost group value here, searching the log files will show cost groups and enable usage to be calculated.



The rule shown in the example would allow any user to send a message to any mobile phone.

Sending Messages



If the broker you have selected is situated in a different country to the server, you may need to specify an International dialling code in any telephone numbers you specify in messages. Your broker will be able to provide you with additional details of International dialling codes you may require.

To send an SMS message using the account above a user would send an email message to:

<accountname>.<mobile number>@<domainname>

For example:

sms.0777711111@company.dom

19.2 GMS WebMail configuration

Enabling the Outbound SMS Gateway

Please select Services, SMS from the menu then the Outbound tab on the right of the page.



Gateway - Select the broker from the drop down box that you have configured an account with.

Username - Enter the username of your account with the SMS broker.

Password - Enter the password provided by the SMS broker.

International dialling code - In many instances the broker may be situated in a different country to the location of the server, if an international access code is required enter it here.

National trunk prefix - Enter a number here if your messages need to be sent to a specific range of numbers specific to a single phone network.



Your broker will be able to provide you with additional details of International dialling codes and national trunk prefixes to use.

Enabling the Inbound SMS Gateway

The setup for this is identical to the Outbound Gateway. You will normally also need to have a SIM card hosted with your SMS provider as well.

Allowed IPs

The Allowed IPs option is designed to contain a list of IP addresses that are allowed to send you inbound SMS messages. If no addresses are added then anyone will be able to send you SMS messages. As SMS messages arrive on the server via the HTTP protocol you may wish to restrict this to only the IP range used by your SMS service provider to prevent unwanted SMS messages.

Edit Numbers

It is necessary to associate each SMS number you have with a particular email address on your server so that the server knows where to send inbound SMS messages. Clicking the Edit Numbers button will allow you to configure this. Click Update to confirm the settings.

Sending messages

Users can send messages to mobile phones in the same way in which they send an email. Clicking the compose icon in GMS WebMail will open a compose window. If they select the "SMS" icon the window will change to a SMS format and the user can enter a mobile number and compose their message. See *"Composing a SMS Message" on page 26 of the GMS User Guide for further details.*

19.3 Allowing users access to SMS

Access to use the SMS Gateway is controlled by profiles assigned to the user or users. Amending these profiles can permit or deny the user the ability to send SMS messages. See *"Mobile Gateway (requires GMS SMS/Pager Gateway)" on page 106 for further details.*

20 GMS Instant Messaging

GMS offers an Instant Messaging (IM) component that allows your users to have real time text conversations with other users on your email system. Depending on user and profile settings IM also allows users to see and offer presence information including whether they are busy, in a meeting, in the office, at home etc. They can also configure their preferred contact method when not online, for example by email or cell phone.

This chapter explains the configuration options that are available for administrators of IM. For user level options please see the *GMS Users Guide*.

20.1 Installing GMS Instant Messaging

If you installed all products when GMS was first installed on your server you will not need to install any additional software to activate GMS Instant Messaging. You can determine if the product is installed by clicking on **Licensing** in the left hand menu tree.

This will display the products installed and the date upon which the license keys will expire.

Installing the software

GMS Instant Messaging can be installed by running the downloaded GMS installation program. See "Installation" on page 19 for further details.



If you already have some GMS components installed you will need a valid maintenance (upgrade) key before you can install GMS Instant Messaging.

Activating Instant Messaging

Once you have confirmed the software is installed upon your system you can enter the product license key, restart the GMS services and the product will become active.

20.2 Profile options - Access to Instant Messaging

There are a number of IM privileges that administrators can grant to users via profiles. For example users will not be able to use IM unless they are assigned to a profile that permits them to use it. For detailed information on profile options see "Privileges - setting user privileges" on page 103.

20.3 Setting the Instant Messaging port

By default Instant Messaging uses port 8367. If this causes a conflict on the server or you would like to change this

configuration to a different port you can amend this value by going to System Administration, Performance, Ports and changing the value for IM Port to the port number desired.



You will need to stop and restart the service for the new port to be recognised.

20.4 Logging Instant Messages

GMS provides the facility to record all conversations conducted through the IM interface. You can configure instant message logging by selecting the domain from the drop down then going to Domain Administration, Logging in the menu. See "Managing Logs" on page 67.

20.5 Location Map

When logging in to IM a user's IP address can be mapped to a specified location and displayed when the mouse cursor is placed over the user's name in the IM window. This location map is configured from within the GMS Administration GUI. Once you have logged on as an administrator open Services, Instant Messaging in the left hand menu. This will display a dialog listing the current mappings

IP Address	Location
10.10.10.1	Sales Office
10.10.10.2	Support Office

From the above example if the user Jack logs on to IM from the machine with IP 10.10.10.1 and he has allowed his presence information to be displayed, other IM users will be able to see that Jack is currently in the sales office by hovering their mouse over Jack's name in their list of contacts.

To add new mappings click on the **Add New** button. To edit an existing entry double click on an entry in the list and make your changes then press Enter. In a similar way to delete an entry select it in the list and click on **Delete**. Click on Save to confirm your changes.

21 GMS Anti-Spam

21.1 Concepts

This section:

- Defines Unsolicited Commercial E-mail (UCE).
- Explains why UCE is a problem.
- Explains how GMS Anti-Spam and the GMS Anti Spam Update Service allows spam to be kept to a minimum.

What is UCE?

UCE is e-mail delivered over the Internet to someone who has not asked for it and does not want it. This unsolicited mail is usually commercial, hence the term Unsolicited Commercial E-mail. It is sometimes referred to as Unsolicited Bulk E-mail (UBE) and more commonly referred to as Spam. The person who sends UCE is often termed a *Spammer*.

UCE imposes three types of cost on its recipient:

- Each message sent over the network consumes bandwidth.
- Each message is either stored locally or "bounced" back to the sender, taking up storage space and even more bandwidth.
- Each recipient is forced to spend time dealing with the message. If system administrators are then consulted by the affected users, this multiplies the time wasted.

The main non-commercial UCE area is use of e-mail in *denial-of-service* attacks. These use various methods to flood a mailbox with so many messages that its user's e-mail system becomes unusable. Types of denial-of-service attack include mailbombing, ping flooding, and SYN flooding.

To understand how some UCE works, you also need to know what a *mail relay* is. A mail relay is a server which forwards mail from one server to another. Spammers try to use a third party mail server for two reasons:

- To disguise the original source of their e-mails.
- To steal additional resources for sending e-mail, increasing the number of messages they can send. If they can obtain use of a powerful mail server with a fast net connection, a Spammer can send out much more junk mail. They may even be able to relay through several mail servers in parallel.

A responsible administrator should ensure that their servers cannot be used for mail relay in this way.

Spamming Techniques and Countermeasures

To understand UCE, it's useful to think of its development as a sequence of events. The following sequence makes it easy to understand the problem, though it's not historically accurate:

1. As e-mail becomes popular, list server software is developed, making it easy to send e-mails to many users in one go. It is also cheap; sending one message costs little more than sending 100 messages. Not all UCE uses list servers, but they do make multiple messages easier to send.

The e-mails are usually advertisements, but there are also financial scams, chain letters and pleas for financial assistance. Unless the sender offers to sell illegal items, sending UCE is currently not illegal.

The main non-commercial area is use of e-mail in *denial-of-service* attacks, as described above.

2. Spammers collect lists of potential recipients by automatically searching the Internet for e-mail addresses, generally either by scanning Usenet postings or searching the World Wide Web.
3. After a time, software is developed to counter the flood of junk e-mail. Two easy countermeasures are introduced into mail servers, which start to:
 - Search incoming e-mail for particular phrases (for example, "amazing deals!") and discard messages which contain these.
 - Limit the number of RCPT clauses a message can have. This can stop a message addressed to a thousand users, for example, from being delivered.
4. Servers which send out UCE become familiar and as a public service some users compile lists of these, called DNS based Black Lists (DNSBL). These list mail servers that are known sources of UCE or let UCE be relayed through them.
5. Spammers try to avoid the address checks by using *mail relay*. That is, they pass their e-mail to another mail server to deliver it on their behalf, disguising its original source. Neither the sender nor the recipient is a local user. The relay's owner may not know that this is happening, or they may collaborate with a Spammer.
6. As a countermeasure to (5), mail servers are given the capability to define the local users whose mail can be sent externally. This is often done by defining the IP addresses allocated to them.
7. Spammers forge the names in the MAIL and RCPT clauses of a message sent after the opening HELO command. For details of this, see "Forging a message source" at the end of this section.
8. Mail servers start using MX lookup to check that the message's MAIL and RCPT clauses are genuine. This tests whether a message really does come from where it claims to be from.

9. Spammers become more and more sophisticated using genuine MAIL and RCPT clauses, setting up their own MX records in DNS, including so much good text in messages that standard phrase type checks become useless, and finally they introduce spam with no text at all only an image. Image based spam makes content filtering all but useless.
10. The concept of Zero Hour (or Recurrent Pattern Detection [RPD]) is introduced to combat the above. Instead of analysing the content of a message billions of emails are analysed and patterns developed for each of them, if multiple copies of a similar pattern are detected the email must be either a genuine bulk email or spam. The decision between these is easy to make. RPD or Zero Hour has a very high success rate in eliminating spam.
11. GMS Anti-Spam supports all the countermeasures outlined above. If a spammer manages to get around all these checks, GMS Anti-Spam has one last defence — it uses Artificial Intelligence (AI) to monitor e-mail coming in and recognises any unusual patterns. For example, if a user who normally only gets about ten e-mails a day suddenly receives 40, these can be rejected or otherwise dealt with. These unusual patterns normally result from an attempt to relay through your server.

Forging a message's source

This section briefly explains how a Spammer can forge a message source. This elaborates on step 7 in the above sequence.

When a remote sending server at companyA.dom (referred to as the "client" here) connects to your server (companyZ.dom), your server sends a response like this (actually on a single line):

```
220 mail.companyZ.dom Gordano Messaging Suite (v8.00.3073/  
AB0000.00.719cfeeb) ready for ESMTP transfer
```

The client "signs on" to your server using the HELO command and announcing its name:

```
HELO mail.companyA.dom
```

Your server responds, giving its own name then repeating the client's (all messages from your server are preceded by "250"):

```
250 mail.companyZ.dom mail.companyA.dom
```

The client must now tell your server who the mail is coming from and who it's going to. It does this using the MAIL and RCPT clauses. This transaction will look something like this:

```
MAIL From:<customer@companyA.dom>  
250 OK.
```

```
RCPT To:<sales@companyZ.dom>  
250 OK.
```

The two "250 OK" lines are issued by your server. After this exchange, the client would use the DATA command to tell your server that the message (header and body) is about to be sent. This is not shown here, as the parts which can be forged are the two addresses shown in the From and To clauses above.

At each stage your server, if GMS Anti-Spam is configured properly, can check for forgery:

- The MAIL clause — GMS Mail and GMS WebMail can perform a DNS Lookup on the IP address of the connecting host and ensure that it matches the address of the domain given in the MAIL clause (CompanyA.dom).
- The RCPT clause — GMS Mail and GMS WebMail can perform a DNS Lookup on the IP address of the given host and ensure that it matches the address given in the RCPT clause.

If either does not match, the message will be refused.

What GMS Anti-Spam Can Do for You

GMS Anti-Spam supports all the countermeasures described in the previous section. Using GMS Anti-Spam should let you eradicate almost all the junk mail from your system. Current users see a reduction of over 97% in junk e-mail entering their system and a complete eradication of mail relay through their server. This means you can reserve all your resources and bandwidth for your own use.

This section summarises GMS Anti-Spam capabilities under five headings:

- Message content — checks for restricted words in the message body and/or header. More complex filters can be set up, giving weighting to particular words or phrases.
- Connections — checking servers against DNSBLs, defining local clients and only allowing connections from these, stopping relay from all servers except those you allow, limiting message sizes and the number of recipients.
- Identity checks — checking a server's IP address is genuine and testing that the Mail and RCPT clauses are genuine.
- AI — recognising unusual traffic and preventing it from entering your system.
- Anti-Spam filters (GMS WebMail) — user level filtering can check for known spam message characteristics, messages from

blocked addresses and can request message confirmations before allowing quarantined messages into the users inbox.



*At the end of each explanation below there is some information which explains where in the GMS Anti Spam interface the feature can be found. For example **Anti Spam, Connection, DNSBL** means you can configure the feature by clicking on the **Connection** menu item under **Anti Spam** then selecting the **DNSBL** tab on the right.*

Message Content

There are six distinct types of check:

- **Restricted words** — e-mail containing prohibited words is stopped from entering your system. Every message passing through the server, inbound or outbound, is checked.
Restricted words or phrases can be set in 4 distinct areas. In addition a word scoring algorithm can also be enabled operating on a separate list of words or phrases that will only act when a given threshold is exceeded.
 - Anti Spam, Message Content, Content, Relay Words
 - Anti Spam, Message Content, Content, Global Words
 - Anti Spam, Message Content, Content, Dynamic Words
 - Domain, Anti Spam, Message Content, Content, Words.
- **Filters** — a filter gives a weighting to particular words. For example, you could set up a filter which only operates if one word occurs five times and another word three times. If a filter finds what it's looking for in a mail message, various actions can be taken, such as rejecting the message or copying it to another account for checking later. Filters can be global or domain-specific.
 - Anti Spam, Message Content, Filters
 - Domain, Anti Spam, Message Content, Filters
- **Quality** — up to 52 distinct message quality checks can be enabled. These are applied to all messages passing through a system.
 - Anti Spam, Message Content, Content, Quality
 - Domain, Anti Spam, Message Content, Content, Quality
- **Zero Hour** — Based on Recurrent Pattern Detection (RPD) technology this option is proving highly effective in the fight against UCE. Requires no manual intervention.
 - Domain, Anti Spam, Message Content, Content, Words
 - Anti Spam, Message Content, Content, Relay Words
 - Anti Spam, Message Content, Content, Global Words
- **Bayesian** — uses a mathematical algorithm to detect UCE based on sampling levels of both UCE and non UCE email

already handled by the system. Requires to be regularly updated with new samples to maintain performance.

- Domain, Anti Spam, Message Content, Content, Words
- Anti Spam, Message Content, Content, Relay Words
- Anti Spam, Message Content, Content, Global Words
- Anti Spam, Message Content, Content, Dynamic Words
- Attachments — Allows you to specify file extensions that should not be allowed such as .exe or .vbs files.
 - Anti Spam, Message Content, Attachments



All of the checks under Dynamic Words along with the Zero Hour checks require a subscription to the GMS Anti-Spam Update Service.

Connections

These tests control which servers can send mail to yours:

- You can ban the IP addresses of servers listed on a DNSBL from connecting to your server.
 - Anti Spam, Connection, DNSBL
- You can list “local clients”, IP addresses that are allowed to send mail using the domain’s address. If a message is received from an IP address other than those listed and the domain is used in the MAIL clause, the message is refused.
 - Domain, Anti Spam, Connection, Local Clients
- Allowed IPs — you can ban specific IP addresses from connecting to your server, perhaps because they are known Spammers.
 - Anti Spam, Connection, Allowed IPs
- Relay — you can define the non-local domains whose mail can be relayed out to the external world through your server. Attempts to relay from a server which is not on the list are rejected. If you are acting as a backup or relay for another server, you must allow relay for it.
 - Anti Spam, Connection, Relay
- Message limits — you can limit the maximum number of messages passed from a specific domain or to a specific user. You can also limit the maximum outgoing message sizes passed through your Gordano mail server.
 - Anti Spam, Limits, Messages
 - Anti Spam, Limits, Outbound size
- Max RCPT clauses — you can specify how mail with multiple recipients is handled. This prevents simple attempts to send UCE by sending one message to a large number of people.
 - Anti Spam, Limits, Recipients

- Authentication — you can allow relay for roaming users as long as they authenticate using a username and password before they send a message. It works by requiring the user's client to check for mail first using POP or IMAP thereby providing the authentication details. That connection is then allowed to relay for a defined period of time.
 - Anti Spam, Connection, Authenticated IPs
- Connections — you can over-ride the system settings for connections to the SMTP, POP and IMAP services on a per IP address basis. If a particular sending domain is clogging up your server with too much mail you can limit the connections they are allowed to make.
 - Anti Spam, Limits, Connections

Scripts

You can write your own scripts in GMS Anti Spam to carry out any check and subsequent action on messages at any stage of the delivery process:

- Connect
- HELOEHLO
- MAIL
- RCPT
- DATA
- End of Message

Identity checks

These check that the sending server really is what it claims to be:

- Machine name — you can force the use of the machine's IP address in the logs, or perform a reverse lookup on the connecting IP address and record the results in the logs. You can perform a reverse lookup on the machine and terminate the connection if it's not the same as that given at the HELO stage.
 - Anti Spam, Identity, Machine name
- Sender of message — you can run a DNS Lookup on the IP address of the connecting host and ensure that it matches the address given in the MAIL clause.
 - Anti-spam, Identity, Sender
- Receiver of message — you can run a DNS Lookup on the IP address of the given host and ensure that it matches the address given in the RCPT clause.
 - Anti Spam, Identity, Receiver

Artificial Intelligence — the AI module

The AI feature keeps watch on the traffic passing through your system, spots any unusual traffic and takes steps to prevent this traffic from entering your system. Normally such traffic results from an unauthorised person using your system as a relay server.

AI is a fail-safe feature that acts on the RCPT clause, the MAIL clause and on the IP address of the sending server before a message is accepted for delivery. It requires little or no configuration and only acts in extreme circumstances.

GMS monitors the messages passing through the server and counts the number from a given e-mail address, to a given e-mail address and from an IP address. Over a period of time it builds up a profile of the messages that pass through the server under normal conditions. Once the profile has been created, the server checks to see that the number of messages for that mail address in any particular day does not exceed the average number of messages per day multiplied by a specified factor. You can specify what action is taken when unusual traffic occurs.

- Anti Spam, AI, Machine name
- Anti Spam, AI, Sender
- Anti Spam, AI, Receiver

Bypasses

There are a large number of bypasses that can be set allowing the anti-spam checks to be over-ridden. These should be used with care as if you are too liberal with the settings the amount of spam blocked by the filters can be reduced considerably.

- Trusted Sessions - allow you to trust particular remote IP addresses, remote hosts, Senders or Recipients.
 - Anti Spam, ByPasses, Trusted Sessions
- Authenticated IPs - allow you treat particular IPs as if they had authenticated to the system. All bypasses for authenticated users will apply to them such as the ability to relay through the system.
 - Anti Spam, ByPasses, Authenticated IPs
- Authenticated Clients - provides various options as to how connections from authenticated clients should be treated.
 - Anti Spam, ByPasses, Authenticated Clients
- Relay Words - allows you to specify IP addresses that should be allowed to relay through the system without being subject to content checks.
 - Anti Spam, ByPasses, Relay Words

Anti-Spam filters (GMS WebMail)

The anti-spam filters are only available to users with GMS WebMail installed. They are configured on a user basis. Users can configure these to:

- Reject messages exhibiting known spam characteristics, for example, many spam messages have no reply address specified or no subject. These will be rejected.
- Reject messages from users listed in the blocklist address book
- Quarantine messages from unknown users and issue a confirmation request. Upon receipt of a reply to the confirmation the message is delivered to the inbox and the users address is added to the list of accepted addresses.

21.2 Setting Up GMS Anti Spam

This section describes how to set up GMS Anti Spam. This is quick and easy, especially since you should not initially need to change any of the messages returned to senders from their defaults.

If you need full information on any parameter when you configure GMS Anti Spam, use the context sensitive online help.

The Anti Spam functions are grouped into five categories, as introduced in the previous chapter:

- Checking the content of messages — checking for restricted words and setting up global or domain-specific filters.
- Connection options — using DNSBL lists to check for Spammers, listing banned hosts, stopping mail relay, limiting message sizes or the number of RCPT clauses and banning attachment types.
- Checking the identity of machines sending e-mail, and of the message sender and receiver.
- AI (Artificial Intelligence) — looking for unusual patterns of e-mail activity.
- Anti-Spam filters (GMS WebMail) — filtering inbound email for listed addresses and blocking or quarantining mail.

21.3 Messages and reply codes

Many of the GMS Anti Spam functions return a message to the sender of an e-mail which is rejected. You will see a default message on the page for any function which does this, usually in a text box labelled "Reject with" or "Retry later with". Where these two alternatives occur, the first rejects the e-mail permanently while the second tells the sender they can try again later if they wish.

If you want to change the message on any page, just type in the new message you want in place of the default which is shown. For

example on the Anti Spam, Connection, DNSBL page the message is "Mail not accepted from server in DNSBL".

SMTP reply codes

A message returned to a sender will be preceded by an SMTP reply code. For example, if a page shows "Phrase in e-mail not acceptable" as the message, the sender will receive a message "500 Phrase in e-mail not acceptable". All responses have three digits followed by a space and a free format text response.

For full details of SMTP error codes, see the *Gordano Reference Guide*, but here is a quick summary:

- Responses starting "2" indicate success.
- Responses starting "4" indicate a transient failure. Retrying later may succeed.
- Responses starting "5" indicate a permanent failure. The message will never be accepted and should be returned to the sender.

Here are some examples of reply codes used by GMS Anti Spam at the various stages of the SMTP protocol:

Clause	Code	Default message
HELO	453	Exceeded IP count - please try later.
	550	Your server has been banned from this server.
	450	Too many messages from you today.
MAIL	453	Exceeded MAIL count - please try later.
	550	Domain has no MX or A record.
RCPT	550	Too many RCPT clauses.
	450	Too many messages to this user today.
	453	Exceeded RCPT count - please try later.
DATA	550	This mail is not local.
	550	You are not allowed to post to this address.
End of Message	452	Insufficient system storage.
	552	Exceeded maximum message size.

21.4 Checking Message Content

You can check for restricted words within messages. You can also set up global or domain-specific filters, which let you return messages to the sender with some explanation, or redirect them to another account.

Word based checks

There are 2 distinct types of word based files within GMS, Restricted Word lists and Scored Restricted Word lists. Both of these run content checks in three areas using separate word lists although the checks they perform are all similar. Prior to running any checks the individual lists for each type are all amalgamated into one large list, depending on which options are enabled, and this large list is used to run the checks.

Each of the separate options are described further below.

Restricted Words

Dynamic Words

The Dynamic Word file can be automatically updated using the update service provided by Gordano Limited. Other than obtaining automatic updates this can only be enabled or disabled. The contents of the file can also be viewed to aid with troubleshooting.

With junk mailers being more and more innovative with the content of mail messages in attempts to bypass filtering tools, it is essential that filters are kept as up to date as possible. It is very easy for a busy administrator to forget or delay updates to the files so Gordano have added an automatic update facility to Anti Spam. The automatic updates feature allows up to the minute awareness of current junk mail threats. see "Anti Spam" on page 294.



The dynamic word file can not be edited. This file is automatically updated at predefined intervals from information supplied by Gordano Limited .

Note that there are certain words or phrases that are specifically not included in the Dynamic Word list, these are:

- No domain names
- No URLs
- No trademark names
- No product or brand names

If you wish to restrict message containing any of the above items you will need to specifically add these items to either the Global or Domain Word lists.

Global Words

The Global Words file is a universal file that can be used by any domain on the system in addition to the domain specific word file. It is an idea to keep all common words in this file and reserve the domain level file for checks particular to that domain. The domains can only use the Global Word file if it has been enabled. Editing the file is similar to the process for the Domain Words file described below.

Domain Words

Various checks can be performed against the content of incoming mail. The headers and message body can both be checked.

To configure content checking:

1. Choose Domain, Anti Spam, Message Content, Words, and then select the options you would like enabled.
2. If you wish to use the same Global checks for each domain on your system select "Use global checks", otherwise leave this option unchecked. All options enabled under Global Words will be used.
3. If you wish to use the same Dynamic checks for each domain on your system select "Use Dynamic Checks", otherwise leave this option unchecked. All options enabled under Dynamic Words will be used.
4. The **Restricted Word File** can be edited directly by entering your restricted words and phrases, each entry on its own line.
5. The **Scored Restricted Word File** can be edited directly by entering your score level and restricted words and phrases, each entry on its own line.
6. Set any bypasses you would like enabled (sending IP addresses that should not be checked).
7. Set the various check modes, the most sensible are already selected by default.

Restricted Words

The Restricted Word check is an "all or nothing" check, i.e. any incoming message containing one of the words or phrases in this list will immediately apply whichever action you have configured. When entering words and phrases there are a couple of things to be aware of. If you enter the word "and" as a restricted word this will also block messages that contain any derivative of the word "and". So words like "band" and "sandy" would also be caught by the filter. One solution to this is to enter " and ". Note the space before and after the word. However if the message contains a dot after the word "and" to denote the end of the sentence it won't be caught by the filter. In this case you may need two rules: " and ", " and. ".

In reality the Restricted Word filter is more suitable for use with phrases rather than single words, as the use of single words will increase the possibilities of false positives.



A false positive is when an incoming message is inadvertently marked as being a spam message when in fact it is a legitimate message.

Each phrase that you would like to check for should be included in the file on a line of its own. Wild card matching is supported and there is a good range of regular expressions that can be used to provide ranges and location matching.

Scored Restricted Words

The Scored Restricted Word lists are basically similar to the restricted word lists described above and the same regular expressions can be used within them. However there are also major differences which will become obvious as the functionality is described.

Scored restricted word lists are more suited to containing single words rather than phrases as may be preferred for the standard restricted word lists. Each word entered into the file is given a particular score, which may be either positive or negative. Each occurrence of a word in an incoming message will result in the score for that word being added to a running total for the message. If the total for the message exceeds the given threshold then the action set will be applied.

If the user level Anti Spam filter is being used then the messages can be allowed through to this filter to allow end users direct control over the threshold.

The following provides an example of the scored restricted word filter in action. Imagine that the scored restricted word file contained the following entries:

- 10: email
- 10: message
- 30: sales
- 50: gordano

The following message was then sent into the mail server destined for the postmaster:

From: "Sales" <sales@gordano.com>
To: "Postmaster" <postmaster@test.dom>
Subject: Scored Restricted Word filter

This is a sample email message to prove the workings of the new scored restricted word filter available in GMS Anti-Spam.

Regards
Gordano Limited.

Looking at the message we can see that the word "sales" occurs twice giving a score of 60, the word "email" occurs once and adds a further 10 to the score giving 70. The word "message" adds yet another 10 giving a total so far of 80, and finally the word "gordano" occurs once and has a score of -50 which is subtracted from 80 to give an overall total for the message of 30.

As can be clearly seen, once a decent word list is built up, this is a very powerful method of assessing the potential of any incoming message. Particularly when used in conjunction with the standard restricted word list above, which is more designed to catch very specific messages without doing any analysis.

As for the standard restricted word lists this facility is available on a Global, Domain and Relay basis.

If you are a subscriber to the Anti Spam Update Service a scored restricted word file is also available that is maintained by Gordano Limited and dynamically uploaded to your server at pre defined intervals. see "Anti Spam" on page 294.

Regular Expressions

Filter rules also support the use of regular expressions or wildcards. For example a rule of " and?" would catch both of the following " and ", " and.". Supported regular expressions are:

[abc]	matches exactly one of the characters "a", "b" or "c"
[-m]	Matches exactly one character that is less than or equal to "m"
[m-]	Matches exactly one character that is greater than or equal to "m"
[a-m]	matches exactly one character in the range "a" to "m" inclusive
[expression,expression,...]	matches exactly one character in one of the expressions listed where the each expression is in one of the forms listed above
(abc)	Round brackets may be used in place of square brackets to provide an optional character. For example, using the rules above to check for "pill[s]" would only match exactly if the word "pills" existed in the message but using "pill(s)" would match against either "pill" or "pills".
*	matches anything in a line of text. For example "some text *" will match "some text goes here"
?	matches any single character. For example "some ?ext" will match both "some text" and "some next"

[abc]	matches exactly one of the characters "a", "b" or "c"
\	Escape character. For example, the character ? is a wildcard as described above, if you want to specifically look for ? rather than matching any character you would need to escape it thus \?, i.e. "word\" would only match "word?" and not "words"
^	Indicates the start of a line. For example, "^word" would only match if "word" was at the very start of the line.
\$	Indicates the end of a line. For example, "word\$" would only match if "word" was at the very end of the line.
+	+ is an over ride indicator, used either to balance out another entry in the combined word files or to specifically allow messages containing the word or phrase. For example, if the word "spam" exists in the dynamic word file you could create an entry of "+spam" in the domain word file to cancel out the previous entry.

If the word "spam" did not appear in any of the word files then "+spam" means to explicitly allow messages contain the word. If "spam" did appear in one of the word files and you wanted to specifically allow messages containing it then you would need to enter "+spam" twice, each on its own line in the domain word file.

No support will be available for matching multiple characters with these range options. Note also that no spaces are allowed in the range specifications.

Example:

Restricted Word Entry: tr*i[l-o]

Matches: train, trail

Non-Matches: triangle, trill, trial



*The regular expression characters * and ? can be escaped by placing them in square brackets. For example a restricted word entry of "why[?]" will catch "why?" but will allow "why." A restricted word entry of "why?" will treat the question mark as a wild card and will catch "why?", "why.", "whys" etc.*

The \ character is a generic escape character that can be used to escape any character, for example if you wanted to check for the string "[ADV]" you would need to escape the [and] characters thus "\[ADV\]"

Over-rides

You may find that you want to use the automatically updated dynamic word file or the Global Word file for all of your

domains but there may be one domain on your system that requires to accept mail containing a particular phrase. This is easily configured by simply adding the phrase to the Domain Word file preceding it with a + sign.

Say for example that there is a phrase in the Dynamic Word list that reads "I don't want this message", if you wanted to allow this you would add an entry to the Domain Word list that looks like:

+I don't want this message



The + character must be the very first character on the line, otherwise it will be treated as a new phrase.

If you wanted to ensure that any message containing the phrase "I don't want this message" can enter your system no matter what other banned words or phrases it contains then you would need to enter the phrase twice on two separate lines so that the word list looks like:

+I don't want this message

+I don't want this message

The word lists are amalgamated in the specific order Dynamic followed by Global followed by Domain. So if you wished to override a phrase in the Dynamic list for all domains on your system you could put the over-ride in the Global Word list as opposed to having an individual entry in each of the Domain Word lists.

Restricted Word Mode

This option, which applies to both the Restricted Word and Scored Restricted Word filters, is only available under the System level Relay Words filter or the Domain Words filter but will affect all messages to or from the domain it is set for. Open the relevant area of the page to specify a range of options to be used when checking messages. The options are:

Search Mode

This determines which parts of a message are checked, the default is to check both the headers and the body.

- Headers and body — This option will check the entire message content including headers message body and encoded attachment sections.
- Headers only — This option will only check the message headers for matching words or phrases.
- Body only — This option will check the whole message except for the headers. Encoded attachment sections will also be checked.

- **First [n] lines** — This option will check the specified number of lines in the entire message including the message headers.



The "First [n] lines" option is advisable for busy systems that have a lot of messages with attachments passing through them. Messages with attachments can be made up of 100's of lines of encoded text. Because attachments sections are encoded there is no point in checking those sections. Typically the first 100 lines of a message are sufficient to check against. If you find messages have matching words later in the message you can increase this figure as required.

1. **Scan binary files**

Selecting this option enables scanning of binary files. This may slow down processing especially for large files.

2. **Case-sensitive checks**

Selecting this option enables the use of case-sensitive checks rather than the default case-insensitive checks.

3. **Check raw HTML**

Selecting this option enables the content of HTML tags to be checked.

4. **Check filtered HTML**

Selecting this option enables the removal of HTML tags before checking content.

5. **Remove punctuation**

Selecting this option enables the filter which removes punctuation prior to restricted word checks. For example "**t+e+s+t**" will be reduced to "test" before checking.

6. **Compress multiple spaces**

Selecting this option enables the filter which reduces multiple adjacent whitespace (space, tab) characters to a single space character. For example "**test this**" (with 5 spaces) will be reduced to "test **this**" (with just 1 space).

7. **Character substitution**

Selecting this option enables the filter which allows limited character substitution. For example, it allows **1** (digit one) to be substituted for **i** (letter i) allowing "test **th1s**" to be detected by the restricted word pattern "test **this**". Other substitutions are **0** (digit zero) for **o** (letter o), **5** (digit five) for **s** (letter ess), **@** for letter **a** and so on.

8. **Multibyte Character substitution**

Selecting this option allows substitution of Multibyte characters with the single character equivalent. Examples of this would be the multiple characters **()** (two round brackets) substituted with the letter **O**, **|/|** (pipe, back slash, forward slash, pip) substituted with the letter **M**, and so on.

9. **Accent Character substitution**

Selecting this option allows substitution of accented characters with their non accented equivalents. For example, the letters **À**

or à would be substituted with **A** and **a** respectively, and the letter Î or î substituted with **I** and **i** respectively.

10. Ignore CR/LF characters

Selecting this option enables the filter which combines adjacent lines of text into one line prior to checking.

11. Translate HTML entities

Selecting this option enables the filter which translates HTML entities such as ' ' to ' ' (single space) and 'A' to '**A**' prior to checking.

Press **Update** to save your settings

Restricted Word Bypass

Again this option is only available for the System Relay Words and the Domain, Words filters and will affect all messages to or from that domain. If there are certain IP addresses whose mail you do not want to be checked, select the Edit Bypass button. Now type an IP address that you do not want mail from to be checked and click on the Add button. Repeat for each IP address you wish checks to be bypassed for. IP address ranges may be specified using the normal notation.

Press **Update** to save your settings

Bayesian filter (System Level)

Bayesian based filters calculate the probability of a message being junk based on the contents of that message. Unlike simple content-based filters, Bayesian filtering learns from both good and bad messages, resulting in a very efficient, self learning, anti-spam system that will return very few false positives. Ideally, you should start with a large number of messages that you have already classified as bad, and another which you have classified as good. These should then be fed into the Bayesian filter to prime it with content. The filter will look at both good and bad messages, analyzing both to calculate the probability of various characteristics appearing in both good and bad messages.

For the Bayesian filter to be available the files required to run the filter must be installed in the gordano\bin directory on your server. Once the files are in place the Bayesian filter option will automatically become enabled. The required files can be downloaded from the Gordano website <http://www.gordano.com>, please select the appropriate files for your operating system.

Operating System	File name
Windows	af-win-intel.zip
Linux	af-linux-intel.tar.gz

Operating System	File name
Solaris	af-solaris-sparc.tar.gz
AIX	af-aix-rs6000.tar.gz

The Bayesian filter is available at two different levels, Dynamic and Global. The Dynamic option will only be available if you have subscribed to the GMS Anti-Spam Update Service. Use of the Dynamic and Global checks can also be enabled/disabled on a per domain basis.

The first step in setting up the Bayesian filter should always be to prime the Global Bayesian filter. To do this go to Domains & Users, Domain and select a user account whose mail folders will be used to prime the filter. Having selected the user, click on Bayesian Dictionary in the secondary toolbar, select from the first drop down menu which of their folders to use and from the second how mail from that folder should be seen. The options are **as Mail** for good mail that you want entering your system, and **as Junk** for bad mail that you do not want to see.

Enabling the **Check dictionary before adding** option allows the import filter to check for the presence of the message in the existing filter. If the dictionary already knows about the message and thinks it is classified the same as you are importing it as, it will ignore it. If it is classified differently then the filter will automatically try and change the classification to match that which you are currently importing the message as.



If you have subscribed to the GMS Anti Spam Update Service you must prime the Bayesian filter prior to enabling use of the Dynamic Bayesian filter.

Thresholds for the Bayesian filter are set on either the Domain Words or Relay Words pages and are expressed as a percentage. The default setting is to act on any message that has a 90% probability of being spam. You can change this but you should be aware that the higher you set the probability the more likely you are to suffer from false positives while the lower you set it the greater the likelihood of spam passing through the filter.

If the user level Anti Spam filter is being used then the messages can be allowed through to this filter to allow end users direct control over the threshold.

Zero Hour

GMS Zero Hour technology is highly effective in stopping UCE. We regularly see over 97% success rate with virtually zero false positives. Setup is extremely straightforward and there is no ongoing maintenance to perform whatsoever, a truly "set it and forget it" solution to the UCE problem. Should you choose to move

messages to quarantine, you can use the Quarantine Report (see "Quarantine (domain and system)" on page 144.) to mark messages as junk, or to report false positives.

Zero-hour classification is unlike conventional Anti Spam techniques, because it does not work by examining the content of your message, or by looking for particular key words or combinations of words. Instead, a mathematical calculation is performed on the incoming message to create a unique signature, which is then sent to online servers which monitor the delivery of millions of email messages daily and contain signatures for upwards of 10 million known unique junk email messages at any one time.

A local cache of signatures is stored on the GMS server, to prevent continued requests to the online stores - these local caches should detect upwards of 70% of your junk email reducing the already small bandwidth requirements even further.

Use Zero Hour Classification checks

Enables or disables the Zero Hour protection. Zero Hour classification checks are run prior to the other content based anti-spam checks. This will help reduce load on the server as the checks are run as early in the process as possible. If a message fails the checks then the standard Anti-spam actions will be applied.

Use Strict Zero Hour Classification Checks

There are two levels of activity reported, Confirmed Spam and Bulk. If this option is enabled both Confirmed and Bulk are treated as spam. If it is not enabled only the Confirmed option is treated as spam.

Fail On Zero Hour Classification Error

If this option is enabled messages that the Zero Hour protection module has been unable to classify will be treated as if they have failed the checks.

Reading Zero Hour information

The Zero Hour spam protection will write information into the headers of messages it has processed. This information can be used to determine how the Zero Hour check has processed the message and to determine the results of that processing.

X-Zero-Hour-AS-Classification: 1 [62.172.232.191]

X-Zero-Hour-AS-Classification-RefId:

str=0001.0A0B0204.444DCF65.004C,ss=1,fgs=0

Classifications are:

0 - None

1 - Unknown

2 - Suspect

3 - Bulk

4 - Confirmed Spam

Only messages classified as 4 will be blocked by the Zero-Hour classification, if you enable strict mode messages with a classification of 3 will also be blocked.

The RefId is an internal reference used when reporting false positives via the Quarantine reports. If you ever need to query the status of a false positive report you will need to quote the RefId.

Setting up filters

You can pass incoming mail through two types of filter:

- Global filters — apply to all incoming mail.
- Domain filters — apply to mail for one domain.

If a filter finds what it's looking for in a mail message, various actions can be carried out on the message, such as rejecting it or copying it to another account for checking later.

You can add multiple words but not phrases and give each of these a weighting. For example, you can configure a filter which operates only if one word occurs five times and another word occurs three times.

To add a new filter:

1. Choose Anti Spam, Message Content, Filters or for a domain select it in the drop down then select Anti Spam, Message Content, Filters.
2. Click Add New and name the rule.
3. Click Add New again in the list box immediately below the Rule Name, type a word in the text area and then specify a count that should be applied to that word to specify how many times it must occur to trigger the filter then press Enter. Add further words as necessary then click on Save.
4. Specify the action to take when a mail message matches the rule:
 - Reject it with a permanent or temporary failure reply code.
 - Forward it to a given e-mail address instead of to the intended recipient. This could be somebody who is investigating UCE for you.
 - Accept the message and copy it to another recipient as well as the addressee.
 - "Ignore this rule for now" — lets you set up the rule now for activation later.
5. Press the Update button to save your settings and bring the rule into effect.

Deleting and Editing Rules

To delete a rule, choose Anti Spam, Message Content, Filters at either the System or Domain level, highlight it in the list and click on the Delete button.

To edit a rule, simply highlight it in the list and amend the details shown below.

Message Quality

Malformed MIME content is often used to try and bypass the ability of anti virus software to correctly identify viruses and anti spam software to detect unsolicited email. Messages that contain malformed MIME can also cause problems with certain email clients when reading or downloading these messages.

This section provides the ability to look for and reject messages that contain malformed mime content. The checks can be set either globally or on a per domain basis, global checks taking priority over domain checks.

Message lines not terminated by CRLF

According to RFC standards all lines must be terminated with a carriage return, line feed pair. Unfortunately, some mail servers (especially old versions of Sendmail) only terminate with a carriage return. Selecting this option will reject messages that do not conform to this standard.

Message line exceeds RFC2822 limits

According to RFC standards there are two limits placed characters in a line. Each line of characters must be no more than 998 characters, and should be no more than 78 characters, excluding the CRLF. Select this option to enforce character line length.

Message line not folding according to RFC2822

RFC 2822 specifies a method of folding long header lines in order to conform to the 78 character line limit. Enabling this option will detect messages where either there is no folding of long header lines, or the folding is not done in accordance with the RFC.

Message has no body

There is no RFC requirement for a message to contain a body and it may quite correctly terminate immediately after the headers. However a number of email clients such as MS Outlook have difficulty coping with such messages. Enabling this option will ensure that they never get into a users mailbox.

Message text contains binary data

Binary data should never be transmitted in email messages without being encoded in one of the available mime formats. If any raw binary data is detected in a message this option will cause it to be rejected.

Headers contain required RFC822 Headers

RFC822 requires emails to have a certain set of header lines. Some mail clients do not insert the required headers, with typically the From: field missing. Select this option to enforce RFC822 header compliance.

Headers contain suspicious header field name

Each header field should end with a : (colon) character, for example Received:. If a field does not end with this character this option will reject the message.

Attachment name is too long

If the attachment name exceeds 256 characters the message will be rejected if this option is selected.

Suspicious attachment name

If the attachment name contains:

- multiple adjacent spaces
- multiple dots in file names, for example file.doc.bat
- mismatched quotes in mime boundary

The message will be rejected if this option is selected.

Empty attachment

If the message references an attachment that contains no content it will be rejected.

CLSID in attachment name

The default operation performed to open a file type is determined by referencing the file type's CLSID. It is possible to specify a different default action for a given file than would normally be used. As a result, seemingly harmless files (.txt, .jpg etc.) may be opened in a non-standard, attacker specified manner. For example, a program ("trojan.exe") could be renamed "trojan.jpg.{CLSID_of_executables}" and when opened by the target user, this file will be executed instead of opened by their default .jpg viewer. Selecting this option rejects messages with attachments containing CLSID.

UUEncode begin in subject

The UUEncode begin statement should never appear in the subject line of the message. It is placed in the subject line as a method to bypass virus scanners, therefore selecting this option will protect against this exploit.

UUEncode begin incomplete

A typical UUEncode begin string would be

```
begin 666 image.jpg
```

Selecting this option will reject messages where this is not correctly specified.

UUEncode data with blank lines

UUEncoded files should not have any blank lines within the encoded section. Spaces will prevent the attachment from being decoded correctly. Selecting this option will reject these messages.

UUEncode data with spaces

UUEncoded files should not have any spaces within the encoded section. Spaces will prevent the attachment from being decoded correctly. Selecting this option will reject these messages.

UUEncode data line too long

A UUEncoded line should be no longer than 45 characters. Messages with longer lines will be rejected if this option is selected.

UUEncode data invalid

UUEncoded data should only contain ASCII text. Selecting this option will reject messages with invalid characters within the UUEncoded data.

UUEncode data invalid decode

When a message is received with UUEncoding GMS will decode the attachment, to allow it to be checked. Selecting this option will reject the message if invalid data is found during this decoding process.

Base64 encoding of inline text

Base64 encoding of inline text can be used to bypass filters that scan messages for specific words. Selecting this option will reject messages with Base64 encoded inline text. **Note:** Some email clients Base64 encode inline text by default, therefore this option should be used with caution.

Base64 data invalid

If the Base64 MIME section contains invalid data the message will be rejected if this option is selected.

Base64 data invalid length

Base64 encoding has a line limit of 76 characters. All lines, with the exception of the final line, must be 76 characters. If a message contains data with lines of the incorrect length this option will reject the message.

Base64 data has leading '=' signs

The '=' character is used in Base64 encoding as padding, to ensure the last line of encoding contains the correct number of bytes. Therefore this character will only appear at the end of the encoded data. This option will reject messages when the '=' is found at the beginning of the data.

Base64 data has too many '=' signs

The '=' character is used in Base64 encoding as padding, to ensure the last line of encoding contains the correct number of bytes. This character should not appear more than twice at the end of the encoding if the message is correctly formatted. This option will reject messages with more than two occurrences of the '=' if selected.

Base64 data after end of decode

The encoded section is always ended with a string similar to

```
-----=_NextPart_000_012D_01C2D8FD.FF311F10--
```

The -- section at the end of the line indicates this is the end of decode. No data should be included after this string, unless it is contained within further MIME boundaries. Select this option to reject messages with this characteristic.

Base64 data line too long

Base64 encoding has a line limit of 76 characters. If a message has a line or lines in excess of this length this option will reject the message.

Binhex data in text section

BinHex is an especially common format for Macintosh files. Selecting this option will reject messages that have BinHex data in the message text section.

BinHex data invalid

Binhex data must contain lines of 64 characters, a statement at the beginning of the data stating the data is BinHex encoded and other specific attributes. This option will reject the message if the data is not correct in regards to these mandatory factors.

MIME no start boundary

MIME encoded data must contain a starting boundary, similar to

```
-----=_NextPart_000_012D_01C2D8FD.FF311F10--
```

Selecting this option will reject messages where this boundary has not been included.

MIME no final boundary

MIME encoded data must contain a final boundary, similar to

```
-----=_NextPart_000_012D_01C2D8FD.FF311F10--
```

Selecting this option will reject messages where this boundary has not been included.

MIME empty boundary

While an empty MIME boundary is in theory valid, we are not aware of any legitimate application that creates such a boundary. It is more likely to be used in an attempt to bypass content checking.

MIME 8 bit characters in header field

8 bit MIME characters are not permitted in message headers fields. Select this option to delete messages with these characters in the header field.

MIME partial message fragment

A common exploit to attempt to bypass virus scanners is to split a message into several smaller messages with partial MIME content. When these messages are received the client may reconstruct the message into its original format. Select this option to reject these messages.

MIME invalid fieldname format

MIME encoded data headers contain fieldnames such as

```
Content-Transfer-Encoding:  
Content-Disposition:
```

These fieldnames end with a ":" which must follow immediately after the fieldname. Selecting this option will reject messages that do not adhere to this rule.

MIME invalid message/rfc822 content type

If a message includes the "rfc 822 content type" it can be used to include a message within a message as an attempt to bypass virus or anti spam scanning. Select this option to prevent these messages being accepted.

MIME invalid content transfer encoding

Each MIME message must include a section defining the content transfer encoding used. There are a finite number of encoding types and this option will reject any messages containing a non standard type.

MIME invalid RFC2047 encoding

RFC 2047 defines a method of encoding non-US-ASCII data within the headers of a message. This option will reject any messages containing such data unless it is encoded according to the RFC.

MIME comment detected

It is possible to add comments to the MIME content type in the MIME boundaries. To reject messages with these comments select this option.

MIME section in prolog or epilog

MIME sections start with a prolog, such as:

This is a multi-part message in MIME format.

There should be no data between this and the initial MIME boundary. The epilog is the section after the final MIME Boundary and the end of the message. No content should be included in this section. Select this option to reject these messages.

MIME contains duplicate headers

Valid MIME encoded messages should never contain duplicate headers. This is indicative of a message specifically enabled for bulk transmission. Such messages can be rejected via this option.

MIME contains RFC2231 encodings

RFC 2231 defines methods of defining the language to be used in association with MIME sections. Enabling this option allows rejection of messages containing such language definitions.

HTML component has IFrame entities

If a message contains an IFrame it could be used to link the browser or email client to remote content such .exe files, which could contain a virus. Selecting this option rejects messages containing IFrames.

HTML component uses CID to load file.

CID can be used to instruct an email to call and load external content and is used as an exploit to bypass virus scanning. Select this option to reject these messages.

HTML component has Object entities

Object entities can be used to load external content on the server or workstation and is used as an exploit to bypass virus scanning. Select this option to reject these messages.

HTML component has unnecessary encodings

There is no need for standard emails to encode alpha-numeric characters as numeric entities in HTML. This option will catch any that are. For example the letter "A" may be written as A etc.

HTML Component contains Javascript

There should be no requirement for an email to contain JavaScript as it has the ability to run on the client and potentially cause problems. Enabling this option will reject all emails containing JavaScript.

HTML Component contains JScript

There should be no requirement for an email to contain JScript as it has the ability to run on the client and potentially cause problems. Enabling this option will reject all emails containing JScript.

HTML Component contains VBScript

There should be no requirement for an email to contain VBScript as it has the ability to run on the client and potentially cause problems. Enabling this option will reject all emails containing VBScript.

HTML Component contains encoded scripts

There should be no requirement for an email to contain any encoded scripts whatsoever. The only possible reason to encode scripts in this way is to hide their purpose. Usually a good sign of malicious intent. Enabling this option will reject all emails containing encoded scripts.

URL has IP rather than hostname

Every HTTP URL should have a hostname rather than an IP in the address part of the URL. The code detects normal dotted IP addresses and obfuscated IP addresses, for example those presented in binary, octal, decimal and hexadecimal formats with and without numeric overflow.

URL is obfuscated

Obfuscated URLs are often used by spammers in an attempt to hide the true URL that they are trying to entice you to or to foil legitimate traffic analysis, there is no reason for such a URL in legitimate mail.

URL parameters are suspicious

This check looks for entries within URLs that are likely to run computer code that you are unaware of. Specifically it looks for the presence of "script", "object", "applet", "embed" or "form". If any are found the message will be rejected.

Configuring Actions

There are a choice of actions available to you which will be carried out when any of the Content based checks are breached, including the thresholds for Scored Words and Bayesian filters.

Reject message with

Allows you to immediately reject any message that fails the content checks at the SMTP Protocol level, returning the message entered in the text area to the right of the field.

Redirect to

Provides the option of redirecting the message to another address to allow for manual checking at a later time.

Accept and discard message

This option allows the message to be accepted on to your server so that the sender is not aware that it has failed. The message is then simply thrown away.

Deliver message as usual

If you wish the message to be passed on to the users for them to apply their own filters then this is the option you should select. The message can optionally be delivered to the recipients quarantine folder rather than their inbox.



If you would like your users to manage their own quarantine folders then it is necessary to choose to have messages delivered to the recipients quarantine folder above.

Bypass checks for reporting accounts

All of the word based checks can be bypassed for two special accounts on your system, that is postmaster@yourdomain and abuse@yourdomain. The messaging RFCs require that all mail systems have a postmaster account and that this account should

always accept mail in order that remote people may report issues to you.

Copy message to Quarantine folder

Enable this option if you would like a copy of the message saved to the appropriate Quarantine folder in addition to the above actions. see "Quarantine (domain and system)" on page 144.

Add Reason to Message Header

This option will add the reason that the message failed Content checks into the headers of the email itself. This can then be used by filters at the user level to determine the action to take on the message.

Domain Actions

Actions can be configured separately for each domain or you can simply elect to use the global values that are set under Actions.

Configuring Alerts

You can alert a number of people of any attempt to send a spam or UCE through the system. Choose Anti Spam, Message Content, Content, Alerts at either System or Domain level and select one or more of the following:

- **Alert Postmaster** — to send an alert to the administrator of the system select this check box. If you would like the alert to go to someone other than the postmaster please enter their email address in the box provided, otherwise the default of postmaster@domain.name is used.
- **Alert User** — to inform the intended recipient of a virus that someone has attempted to send them an infected file.
- **Alert Sender** — send a message to the sender of the file alerting them to the fact that they attempted to send an infected file through the system. (They may not know that the message contained a virus.)

Domain Alerts

Alerts can be configured separately for each domain or you can simply elect to use the System settings.

21.5 Attachments

Ban attachments

The Anti Spam, Message Content, Attachments page in the interface provides a means to ban certain attachment types from

entering your system altogether dependant on the file extension of the attachment.

Simply click on Add New and enter the extension that you would like to ban in the Extensions text area. Repeat for each attachment type that you would like to ban, and once complete click on the Save button, followed by the Update button.

To remove an attachment type from the list, highlight and click on the Delete button followed by Update.



Note - only the attachment extension itself should be included, do not include the "." for example to ban "virus.exe" and all other files ending ".exe" you would enter "exe" not ".exe".

There are additional options on this page that you may also wish to consider enabling due to the increasing usage of password protected zip files to propagate viruses.

Check TNEF files for banned extensions

Enabling this option will allow the attachment blocking to be applied to the contents of TNEF files (to non Microsoft mail clients these appear normally as winmail.dat files). For example, if you had banned attachment with an exe extension above then checking this option will also check within TNEF for files with the an exe extension and reject any matching messages.

Check zip files for banned extensions

Enabling this will allow the attachment blocking to also be applied to the contents of zip files. For example, if you had banned attachment with an exe extension above then checking this option will also check within zip archives for files with the an exe extension and reject any matching messages.

Reject password protected zip files

Use of this option will completely ban all password protected zip files from your server.

Reject zip files within zip files

If a zip file contains another zip file and you have enabled this option the message will be rejected. This option does not require that an extension of zip is applied in the blocking list above.

Reject corrupt or unreadable zip files

If for any reason GMS is unable to inspect the contents of zip file due to it being corrupt or unreadable in any way it will be rejected by enabling this option.

Reject office packages

If this option is enabled then all emails containing attachments in the new Office 2007 document format will be rejected.

Reject protected office packages

If an email contains protected Office 2007 documents it will be rejected if this option is enabled.

Reject macro enabled office packages

Enabling this option will reject emails with Office 2007 documents which contain macros.

Reject OpenDoc packages

Similar to the above option for Office 2007 documents enabling this option will reject all emails containing OpenDoc format documents.

Content Types

The standard encoding for email messages today is MIME encoding. The MIME RFCs specify that each attachment be specified in its own MIME section and that a Content Type for that MIME section should also be specified which determines how the receiving client handles the specific attachment. Thus Microsoft Word documents would have one Content Type, executable files would have another and so on.

The Content Types page allows you to specify MIME types that you do not want to enter your system. It is possible however for message to contain a modified MIME type, thereby potentially letting content you thought you had banned pass through the server by disguising the true content type of the encapsulated file.

An example of a Content Type is:

application/msword

This example would prevent any Microsoft Word documents being received via email.

Click on Add New and enter the content type in the text area provided and press Enter to add it to the list below. To remove an entry highlight it in the list and click the Delete button. All entries can be removed at once by clicking the Remove All button. Click Save when you have finished adding entries, then the Update button to save any changes.

Actions

There are a choice of actions available to you which will be carried out when any of the attachment and content type checks are breached.

Reject message with

Allows you to immediately reject any message that fails the checks at the SMTP Protocol level, returning the message entered in the text area to the right of the field.

Redirect to

Provides the option of redirecting the message to another address to allow for manual checking at a later time.

Accept and discard message

This option allows the message to be accepted on to your server so that the sender is not aware that it has failed. The message is then simply thrown away.

Deliver message as usual

If you wish the message to be passed on to the users for them to apply their own filters then this is the option you should select. The message can optionally be delivered to the recipients quarantine folder rather than their inbox.



If you would like your users to manage their own quarantine folders then it is necessary to choose to have messages delivered to the recipients quarantine folder above.

Bypass checks for reporting accounts

All of the checks can be bypassed for two special accounts on your system, that is postmaster@yourdomain and abuse@yourdomain. The messaging RFCs require that all mail systems have a postmaster account and that this account should always accept mail in order that remote people may report issues to you.

Copy message to Quarantine folder

Enable this option if you would like a copy of the message saved to the appropriate Quarantine folder in addition to the above actions. see "Quarantine (domain and system)" on page 144.

Add Reason to Message Header

This option will add the reason that the message failed checks into the headers of the email itself. This can then be used by filters at the user level to determine the action to take on the message.

21.6 Connect Options

The Connect options control which servers can send mail to yours.

Checking servers against a DNSBL

DNS based Black Lists (DNSBLs) are used to maintain a list of mail servers that are known to allow the transmission of UCE.

When DNSBL checking is set up the IP address of each server connecting via SMTP is checked against the DNSBL and, if a match is found, the connection is rejected with the message you specify.

By default, DNSBL checking is set to "Check on Connect". However no checking will be carried out until you define at least one DNSBL server.

In addition to "Check on Connect" you can also set GMS to wait until the MAIL From: clause has been issued before the connecting IP address is checked against the DNSBL. This is only necessary if you would like your banned hosts settings or an HELO/EHLO script to be acted on prior to the DNSBL check being made. You may also choose this option if you want to log the MAIL From: prior to the connection being rejected.

To set up an DNSBL server:

1. Choose Anti Spam, Connection, DNSBL.
2. Click on Add New and enter the name of the DNSBL Server you would like to use in the text area provided.
3. Select the action to be taken when an entry is found in the DNSBL Server from the drop down menu provided. The options are:
 - Accept
 - Try Next
 - Fail
4. Edit the IP response field, most DNSBL servers respond with 127.0.0.2 but some respond with other additional IP addresses. You will need to check with the provider of your particular DNSBL.
5. Enter the response message returned when a match is found. Then press Enter to enter these settings into your configuration followed by clicking on Save.

Once an entry has been made to the configuration it can be edited by double clicking on the entry or removed altogether by clicking on Delete. The order in which DNSBL servers are checked can be changed by highlighting an entry and using the Move Up and Move Down buttons.



If you choose to accept mail from sites listed in the DNSBL, GMS Anti Spam will add a header called X-DNSBL to indicate which DNSBL it was listed on. This allows for filtering later on.

Local clients

The Local clients page maintains a list of IP addresses that you allow to send mail using the address of the specified domain. If a message is received from an IP address other than those listed which uses the domain in its MAIL clause, the message is refused. There are no local clients by default.

To add local clients:

1. Select the domain from the drop down then Anti Spam, Connection, Local Clients.
2. Click on Add New and type the IP address of the first host in the text area and press the Enter button to add it to the list. Add any further IP addresses then click on Save.
3. Specify the action to take when mail arrives from an IP address which is not in the list, customising the rejection message as required then click on the Update button.

Check on connection

Enable this option if you would like the check to take place immediately on connection. If unchecked the check will be delayed to give the sender the opportunity to authenticate to the server.

Check Allowed IP first

If this option is selected SMTP will first check to see if the sender is either in the LocalIP range or has authenticated to the server. If they are found to be connecting from a trusted IP address then the Local Client check is not applied.

Allowed IPs

You can ban specific IP addresses from connecting to your server, perhaps because they are known Spammers. By default no hosts are banned. Unlike most of the others, setting this function up is quite complex, so it's described here in detail.

To ban hosts:

1. Choose Anti Spam, Connection, Allowed IPs to display this page:

The screenshot shows the 'Allowed IPs' configuration page. At the top, there are four tabs: 'DNSBL', 'Allowed IPs' (selected), 'Relay', and 'Authenticated IPs'. Below the tabs, there are two checkboxes: 'Check on connection' and 'Check Local IP first', both of which are unchecked. In the center, there is a list of IP addresses. The list contains three entries: an asterisk (*), '22.22.44.44', and '33.33.33.55'. Each entry has a red 'X' icon to its right. To the right of the list are three buttons: 'Add New', 'Save', and 'Remove All'. Below the list, there are two radio buttons: 'Reject with' (selected) and 'Retry later with'. To the right of the 'Retry later with' radio button is a text input field containing the message 'Your server has been banned from this server'. At the bottom of the form is an 'Update Settings' button.

2. The list of IP addresses will initially be empty.

3. The list must begin with an asterisk (*) on its own. This means allow all IP addresses initially. To add this, click on Add New then type an asterisk in the text area and press Enter.
4. Now specify the banned IP addresses using exclamation marks. In the text area, click Add New again then type an exclamation mark (!) followed immediately by the IP address of the first host you would like to ban the press Enter to add this to the list. In the above example, the entry "!22.22.44.44" shows how entries appear in the list. Now if the IP address 22.22.44.44 ever attempts to connect to your server they will not be able to send any mail and will receive the message indicated below.
5. To ban more hosts, repeat step 2. In the above example, the entry "!33.33.33.55" shows how further entries appear in the list. Click on Save when you have finished adding entries.
6. To remove a host, select it in the list on the right and press the Delete button. You can remove all the entries in one go by clicking on the Remove All button.
7. Specify the action to be taken when mail from a banned host arrives (this applies to all hosts in the list), customising the rejection message if necessary.
8. Click on the Update button.

Maximum recipients

You can specify how e-mail with multiple recipients is handled. This is an ideal method of dealing with UCE that is generated by sending a single e-mail message to a mail server, making it expand a large number of "To" or "cc" header clauses. The mail server does this by issuing multiple RCPT commands, so limiting the number of RCPT clauses on your mail server restricts the expansion. This should be enough to make the Spammer use another, unprotected, mail server.

Having said this, there are reasons for setting a high RCPT value:

- Many legitimate mail servers use multiple RCPT clauses to reduce network traffic for a common message. List servers do this.
- Mail clients often use multiple RCPT clauses to send "cc" and "bcc" copies of messages.
- Some messaging systems are incapable of recovery if a failure occurs part way through a list of RCPT clauses.

We recommend a value between five and 10 for the maximum number of RCPT clauses.

To configure the maximum number of recipients:

1. Choose Anti Spam, Limits, Recipients.
2. In the "Default maximum RCPT clauses" box, specify the default maximum allowed. RFC 821 specifies that this should

- be no greater than 100 but you can set it higher — see the above advice on choosing a value.
3. If you want a particular domain to use a limit other than the default, specify its IP Address and default, and add it to the list. See the help for details on this.
 4. Specify the action to be taken when mail fails the test, customising the rejection message if necessary.

Outbound message sizes

You can specify the maximum size of outbound messages that will be accepted for onward transmission from a domain through the server.

To limit outbound message sizes:

1. Choose Anti Spam, Limits, Outbound Sizes at either the System or Domain levels.
2. In the "Maximum Outbound Message Size" box, type the maximum size in KB that messages leaving this domain will be restricted to then click on the Update button.

Relay

By default, no mail relay is allowed — all RCPT clauses must be local. If your server acts as a backup or relay for another server in a non-local domain, you must allow relay for it as described here.

The mail relay check takes effect:

- After a remote mail server has connected to yours and informed it who the mail is from and who it's addressed to.
- Before the message itself is transferred.



If you select "Allow relay" this lets anyone anywhere send mail through your mail server. You'll probably end up relaying UCE and could be added to DNS-BLs with the result your legitimate mail will not be sent either.

To configure relay:

1. Choose Anti Spam, Connection, Relay and select one of the following:
 - "Disallow relay but allow mail where MAIL clause or more than one RCPT clause is local" — to deny access to your mail server to all e-mail except that addressed to or being sent from one of your local domains. This automatically recognises local domains including POP domains.
 - "Disallow relay, all RCPT clauses must be local" — to only relay mail with local RCPT clauses. A remote mail server can avoid the previous restriction by "spoofing", pretending that e-mail was sent from your domain. To stop this, use the Local IP option because IP addresses are much more difficult to forge; see "Local clients" on page 266.
2. If your mail server is acting as a backup or relay server for any non-local domains, add these to the "Allow relay for the following." list. You can combine this with either of the above options.
3. Specify the action to be taken when mail fails the test, customising the rejection message if necessary.

Maximum messages

You can specify the maximum number of messages that will be accepted in any 24 hour period, defined in two ways:

- From a particular domain, determined by the sending server's IP address. For example, you might specify that server 196.198.12.12 can send a maximum of five messages in any 24 hour period. This would produce an entry like this:

196.198.12.12:5
- To a particular user on the local server. For instance, you could specify that user1@domain.dom can only receive 15 messages in any 24 hour period. This would produce an entry like this:

user1@domain.dom:15

To configure message limits:

1. Choose Anti Spam, Limits, Messages.
2. To add a server click on Add New, type its IP address in the text box on the left and the number of messages in the right-hand box then press Enter.
3. To add a user click on Add New, type their fully-qualified name in the text box (e.g., user@CompanyA.dom) on the left and the number of messages in the right-hand box and press Enter to add them to the list.
4. When you are finished adding entries click on the Save button.
5. Keep the default failure messages and press the Update button.

Authenticate

You can set up GMS Anti Spam so that successful POP/IMAP logon from a non-local client adds that client to the list of IP addresses who are allowed to relay mail through your server. This is particularly useful if you have a number of roaming users but still want to maintain a strict anti-relay policy on your server. Similar settings are also available to those authenticating directly to the SMTP service. To do this:

1. Select Anti Spam, Bypasses, Authenticated Clients.
2. Choose one of the following for POP and IMAP
 - Normal Anti Spam checks - This option disables POP/IMAP before SMTP in that the normal GMS Anti-Spam anti-relay checks will be enforced in addition to other Anti Spam checks such as against DNSBL lists and filters.
 - Allow relay but allow other checks - This option allows relay for users who have previously authenticated over POP/IMAP with their username and password. Once they are authenticated they will be allowed to relay for the period you specify as the expiry period. Other Anti Spam checks such as filters and DNSBL lists will still be performed.
 - Bypass all Anti Spam checks - This option allows relay for users who have previously authenticated over POP with their username and password. Any other Anti Spam checks will be ignored for authenticated users.

Additionally you may specify whether or not any of the authentication options above will also enable access to the included Free/Busy information service.

An option to allow Free/Busy access for those authenticating to the GMS Collaboration Service is also included, as the ability to specify the longevity of these rights for both Relay and Free/Busy access.

An authentication expiry time can also be specified for POP, IMAP and Collaboration logons. This setting does not apply to SMTP Authentication.

Authenticated IPs

This option allows you to enter a list of IP Addresses or IP Address ranges that you would like to treat as if they had authenticated to the server, whether they have actually authenticated or not.

Scripts

This option allows you to define an MML script which is able to act on incoming mail at the stage of the protocol as defined by selecting from the drop down menu. Multiple scripts may be run at any point in the SMTP protocol.

To add a script go to the Anti Spam, Scripts page and click on the Add New button. You will now be presented with a drop down menu from which you can select the part of the protocol you would like the script to act on, give the script a unique name, enter the MML code into the large text area and click on the Update button.

If scripts already exist when you go to the Anti Spam, Scripts page you will be presented with a list of these scripts. To remove a script highlight it in the list and click on the Delete button. To edit the script simply highlight it in the list and edit the details below.

For further information on MML scripts and how they work please see the MML Programmers Guide available as part of the Gordano Accessory Pack.

Connections

The number of connections to each of the SMTP, POP and IMAP services can be restricted from the Anti Spam, Limits, Connections page.

You can either allow unlimited connections to the service or globally limit them by entering a figure in the "Limit to" box and then pressing the Update button.

In addition, certain IP addresses can also be given different limits to those set above by clicking on Add New and entering the IP address and allowed number of connections in the appropriate boxes and then pressing Enter to add them to the list. Again once you have completed adding to the list press the Save button followed by the Update button to confirm the changes.

21.7 Checking Identity

You can set up checks that the sending server really is what it claims to be. There are four types of check:

Sender of message

This will run a DNS Lookup on the IP address of the connecting host to check that it matches the address given in the MAIL clause. For details of how Spammers can change MAIL clauses, see "Forging a message's source" on page 235.

To turn on sender checking, press Identity on the toolbar and simply select the "Do Reverse MX Lookup on FROM email address" check box on the page Anti Spam, Identity, Sender. Specify the action that should be applied to messages failing the check then click on the Update button.

You can also specify if the checks should be applied to mail sent FROM a local domain or not.

Receiver of message

This will run a DNS Lookup on the IP address of the given host to check that it matches the address given in the RCPT clause. For details of how Spammers can change RCPT clauses, see "Forging a message's source" on page 235.

To turn on receiver checking, press Identity on the toolbar and simply select the "Do Reverse MX Lookup on RCPT email address" check box on the page Anti Spam, Identity, Receiver. Specify the action that should be applied to messages failing the check then click on the Update button.

Machine name

This option forces use of the machine's IP address in the logs, or performs a reverse lookup on the connecting IP address and records the results in the logs. The machine name check ensures that the connecting machine is what it claims to be. It performs a reverse lookup on the IP address of a connecting machine. If this does not match the name in the HELO command, the connection is rejected.

For example, if the remote machine sends the SMTP message "HELO mail.companyA.dom" and its IP address does resolve to mail.companyA.dom, the connection is accepted. If the result of the lookup does not match, the connection is refused.



Some servers may have a non-existent or incorrect reverse lookup entry in their name servers. If this is the case, the real source of the message will be lost.

To enable this option choose Anti Spam, Identity, Machine Name and select one of the following options:

- "Use raw IP address in logs" — if you want the raw IP address of the machine used in the Gordano logs rather than the machine name.
- "Reverse lookup on IP and reject if no reverse lookup" — if you want Anti Spam to perform a reverse DNS Lookup on the IP address of the connecting machine and terminate the connection if one does not exist.
- "Reverse lookup on IP and reject if not the same" — if you want Anti Spam to perform a reverse DNS Lookup on the IP address of the connecting machine and terminate the connection if the results do not match. You can also elect to drop the connection immediately after sending a response.
- "Accept and discard the message" — if you want Anti Spam to perform a reverse DNS Lookup on the IP address of the connecting machine and throw the message away if the results do not match.
- "Deliver message as usual" — if this option is selected the message will have any Reasons for failure added to the headers for later filtering but will otherwise be delivered to the user as normal. You can optionally elect to have the message delivered to the users Quarantine folder rather than their Inbox.
- "Use result of reverse lookup in logs" — if you want Anti Spam to use the result gathered from the reverse lookup in the logs rather than the information given out by the connecting machine.
- Finally you can elect to have the message copied to the system Quarantine folder, but bear in mind this is only possible where the message has actually been accepted by the server.

SPF

Sender Policy Framework (SPF) allows Domain owners to identify approved sending mail servers for their domain in DNS. GMS can verify the envelope sender address against this information, and can distinguish authentic messages from forgeries before any message data is transmitted.

Use TXT record

Traditionally SPF information is contained in TXT records in DNS and this is the default setting. An example SPF record would look like

```
v=spf1 a mx ptr a:office.ntmail.co.uk mx:mail.gordano.com  
mx:gate05.gordano.com ip4:62.172.232.231 ~all
```

Use SPF record

TXT record types are not ideally suited to holding SPF records so a new DNS Record type of SPF is being proposed. This uses the same format as TXT records.

Check HELO clause identity

Enabling this option will cause the SPF check to be applied against the identifier passed in the SMTP protocol HELO/EHLO clause.

Check MAIL clause identity

Enabling this option will cause the SPF check to be applied against the domain passed in the SMTP protocol MAIL clause.

Use local policy

A local policy can be determined which can be applied to all SPF checks. The default is to also include `spf.trusted-forwarder.org` in checks. This is a white list for SPF checks and provides early adopters of SPF a way of allowing legitimate email that is sent through known, trusted email forwarders from being blocked by SPF checks simply because the forwarders do not use some sort of envelope-from rewriting system.

Use default SPF record

Specifies a default SPF record that should be used where the sending domain does not have any SPF records at all. By default this includes any A or MX records specified for the sending domain.

Reject if no SPF record

If no SPF record exists for the sending domain then simply reject the connection.

Reject neutral results

The domain owner has explicitly stated that they cannot or do not want to assert whether the IP address is authorized or not. A neutral result MUST be treated exactly like the None result; the distinction exists only for informational purposes.

Reject soft fail results

A soft fail should be treated as somewhere between a hard fail and neutral. The domain believes the host isn't authorized but isn't willing to make that strong a statement.

Reject hard fail results

A hard fail is an explicit statement that the client is not authorized to use the domain in the given identity. The checking software can

choose to mark the mail based on this, or to reject the mail outright.

Reject permanent errors

A permanent error means that the domain's published records couldn't be correctly interpreted. This signals an error condition that requires manual intervention to be resolved, as opposed to the temporary error.

Reject temporary errors

A temporary error means that the SPF client encountered a transient error while performing the check. Checking software can choose to accept or temporarily reject the message.

Add SPF header

If this option is enabled an SPF header will be added to each incoming email indicating the result of the SPF lookup.

Permanent Reject with

The textual error to be returned when a permanent failure is encountered, this is always preceded by a 550 SMTP reply code.

Temporary Reject with

The textual error to be returned when a temporary failure is encountered, this is always preceded by a 451 SMTP reply code.

21.8 AI Checks

The AI feature keeps watch on the traffic passing through your system, spots any unusual traffic and prevents it from entering your system. Unusual traffic may result from an unauthorised person trying to use your system as a relay server. AI needs little or no configuration and only acts in extreme circumstances.

Quick configuration

To turn AI checking on, select the "Allow xxxx clause checking" check box on each page. The default AI values are adequate for most circumstances. You only need to change anything if you want to fine tune the system, or to replace temporary rejection of messages with permanent rejection.

Details

AI acts on the MAIL clause, the RCPT clause or the IP address of the sending server before a message is accepted for delivery. GMS monitors messages passing through the server and counts how many:

- Come from a given e-mail address, shown in the MAIL clause.
- Come from a given IP address.
- Go to a given e-mail address, shown in the RCPT clause.

Over a period of time the AI software builds up a profile of the messages that pass through the Gordano mail server under normal conditions. Once this profile has been created, the server checks to see that the number of messages for that mail address in any particular day does not exceed the average number of messages multiplied by a factor you specify.

You can either reject the excess messages permanently or send a "Retry later" message to show that the rejection is only temporary. Note the following before making your choice:

- Temporary rejection lets the rejected e-mail be resent at a later date. This may cause problems if the sending server is set up to resend rejected messages after just a few seconds. If this does happen, switch to permanent rejection.
- Permanent rejection may reject legitimate e-mail. For example, a user may receive unusual amounts of e-mail for a genuine reason.

Rejection messages must always be preceded by a three digit code indicating the reason for refusal.

Defining "unusual traffic"

Anti Spam can run three types of check, all of which use these parameters:

- **Average Multiplier** — the multiplier applied to the running average. Only when the number of e-mails exceeds the product of the two does Anti Spam start rejecting e-mails. This allows for some natural fluctuation around the average on particular days.

For example, if you set an Average Multiplier of two and the Running Average for a particular user is three, the maximum number of e-mail messages allowed per day will be six. The seventh message will be rejected with the failure message you specify.

- **Required Samples** — the number of days for which GMS Anti-Spam AI must sample your mail server traffic to build up a profile of its e-mail throughput.

Over time the average is adjusted automatically at a maximum rate of (Average Multiplier divided by Required Samples) messages, giving a changing upper band.

- **Running Average Minimum** — this is needed because no typical statistics are available for a new account before it sends or receives e-mail. When a new account is set up, Anti Spam, AI allows a maximum throughput of messages to the account before rejecting e-mail. This is calculated as:

Running Average Minimum * Average Multiplier

Any remote mail server exceeding this threshold will not be able to deliver the excess e-mail until the following day.

Tuning the setup

The three pages which control AI are almost identical, so this section uses the Sender page as an example. This controls how Anti Spam monitors the MAIL clause to check how much e-mail is coming from a particular user. For most purposes, the defaults should be acceptable.

To configure MAIL clause AI checking:

1. Choose Anti Spam, AI, Sender to display this page:

2. Select the "Allow MAIL Clause AI checking" check box.

3. In the Average Multiplier box, type the multiplier to apply to the running average before Anti Spam AI starts rejecting mail.
4. In the Required Samples (days) box, specify the number of days for which Anti Spam AI should sample your mail server traffic to build up a profile of your e-mail throughput.
5. In the Running Average Minimum box, specify the threshold for e-mail checking.
6. Specify the action to be taken when mail fails the test, customising the rejection message if necessary.
7. Press the Update button.

21.9 Anti Spam Log entries

Anti Spam log names start with SL, followed by the date, then the extension ".LOG". For example SL990328.LOG. A typical GMS Anti-Spam log entry might look like this:

```
SPAM 25 Sep 2002 15:26:12.234 H 08039 2 62.172.232.181 rates@mortgages.dom
sandy@company.dom Reject with "550 Phrase in email not acceptable" - Matched "*best rates
available*"
```

21.10 Anti-Spam Filters (User Level)

Defeating UCE is an ongoing battle not only against the "spammers" but also in regards to the configuration you set for your network. Using the options detailed above can lead to compromises which may prevent some users from receiving legitimate email or you may allow some content through that some users may be offended by. The Anti Spam filters allows your users to determine the level of protection they wish to set.

Anti Spam provides 1 user filter in the administration interface which provides user level control over the Scored Words, Bayesian and Message Quality filters for non GMS WebMail users. GMS WebMail provides users with 5 further anti spam filters to enable control of the messages they wish to receive in their inbox. GMS WebMail users have a greater level of control over filters so if available we would recommend that these are used in preference.

Below you will find details on how the user configures these files. Further information can be found in the *GMS Users Guide*.

Junk Mail Filter

The Junk Mail Filter provides 3 settings to control how messages failing the Scored Words, Bayesian and Message Quality filters are treated. High is the most rigorous, through Medium to Low which will give the lowest false positive chances but consequently the highest probability of letting spam through to the users mailbox. The options enforced with each setting are shown in the table below.

High	Scored Rwords: 75
	Bayesian Probability: 75
	Maximum Allowed Message Defects: 0
Medium	Scored Rwords: 100
	Bayesian Probability: 90
	Maximum Allowed Message Defects: 1
Low	Scored Rwords: 200
	Bayesian Probability: 95
	Maximum Allowed Message Defects: 3

The user has the option of either immediately deleting or moving to their quarantine folder any messages that fail the filter.

Anti Spam filter

The Anti Spam filter is designed in such a way that when it is enabled it should greatly reduce the amount of spam the user sees in their mailbox. This filter is configured by clicking on Quarantine in the user area in the top left of the screen then clicking on Filter Settings on the right hand side.

This filter checks for messages with the following characteristics and if found allows the user to carry out a number of filtering actions. The characteristics are:

- Not addressed to me
- No reply address specified
- Reply address does not match from address
- Subject is all capitals
- No subject



*Further information regarding this filter can be found in the GMS User Guide.
"The dedicated anti-spam filter" on page 83*

Bayesian filter (User Level)

Bayesian based filters calculate the probability of a message being junk based on the contents of that message. Unlike simple content-based filters, Bayesian filtering learns from both good and bad messages, resulting in a very efficient, self learning, anti-spam system that will return very few false positives. Ideally, you should start with a large number of messages that you have already classified as bad, and another which you have classified as good. These should then be fed into the Bayesian filter to prime it with content. The filter will look at both good and bad messages, analyzing both to calculate the probability of various characteristics appearing in both good and bad messages.

For the Bayesian filter to be available to your users the files required to run the filter must be installed in the `gordano\bin` directory on your server. Once the files are in place the Bayesian filter option will automatically become enabled. The required files can be downloaded from the Gordano website <http://www.gordano.com>, please select the appropriate files for your operating system.

Operating System	File name
Windows	af-win-intel.zip
Linux	af-linux-intel.tar.gz
Solaris	af-solaris-sparc.tar.gz
AIX	af-aix-rs6000.tar.gz



*Further information regarding this filter can be found in the GMS User Guide.
"The Bayesian Filter" on page 88*

Blocklist filter

The blocklist filter checks incoming email against entries in the users blocklist address book. If a match is found the actions

configured for this filter are applied. This filter can either quarantine messages or delete them.



Further information regarding this filter can be found in the GMS User Guide. "The Block List filter" on page 94

Confirmation filter

The confirmation filter is most likely the most powerful filter the user has access to. Once configured inbound messages are checked to determine if the senders address matches the search criteria the user has set. For example the user may set the filter to detect messages where the senders address does not appear in any of their address books. Once a message is detected the server will generate a confirmation request which is sent to the original sender asking them to reply, to confirm their identity. During this period the original message is stored in the users quarantine folder. When the confirmation request is returned, the original message is moved from the quarantine folder to the inbox.

If the confirmation request is not returned the message remains in the quarantine folder until such time as this folder is purged. Once purged GMS WebMail can be configured to add this address to the Blocklist address book, as described above, and hence any further mail from this address will be rejected.



Further information regarding this filter can be found in the GMS User Guide. "Setting up Confirmation" on page 79

White List filter

The white list filter checks incoming email against entries in the users address books, other than the Quarantine and Blocklist address books. If a match is found the actions configured for this filter are applied.

As the intention of this filter is to allow mail through that otherwise may be caught by the other filters it is advisable to configure this filter to be the first one run, that is the topmost filter in the list.



Further information regarding this filter can be found in the GMS User Guide. "The White List Filter" on page 94

21.11 Spam Reporting Account

Each installation of GMS includes an account to which users can report any spam they receive to allow the administrator to fine tune the servers anti-spam settings. The account is by default called spam@yourdomain although you may change this if you wish via the system variables.

Messages can be sent directly to this account from local users only, i.e. mail from external users will be refused unless they have first authenticated to the server. GMS WebMail users will have an additional button available in the message status bar which they can click on to automatically forward the mail to the spam reporting account.

A **Reported Junk Mail** report is available to Anti Spam administrators to allow them to decide how to treat this reported spam, including the ability to add it to the system Bayesian filter.

22 Anti Virus

22.1 Concepts

This section:

- Explains what viruses are.
- Explains why viruses are a problem.
- Explains how viruses can be sent within e-mail messages.
- Explains how Anti Virus stops viruses reaching your system.

What is a Virus?

A virus is a program designed to replicate itself without permission. In addition, some make great efforts to avoid detection, damage programs and/or data and transfer information and/or funds out of the company to third parties. Viruses must be executed before they can do anything to your computer system. To aid this, viruses usually try to avoid detection by disguising themselves as a legitimate program or attaching themselves to a trusted program. Viruses are not only executable programs, but may also be contained in the macros used by programs such as word processors, spreadsheets etc.

Viruses, once introduced, can quickly propagate round a network causing anything from service loss to destroyed document archives.

There are four types of Virus: hoax, non-malicious, malicious and security breaching. For more details on these and their effects, see the Virus primer on the Gordano Web site.

It is essential that you stop viruses reaching your system. For example, a malicious virus may attack a system and cause data loss. There are two major types of malicious virus that affect PCs:

- Boot-sector viruses affect the boot sector of system disks and are run at startup, ensuring they are always placed in memory before anything else on the system. They may also prevent the system loading.
- File-infecting viruses infect executable files and are triggered when these files are run.

The Cost of Virus Attacks

It can take many days of work to remove a virus from even a small network of computers - for example, to remove a Word macro virus that has successfully propagated round the network, the same software must be run on each networked computer. While this is being done, no employees can use Word. As well as scanning all these machines for the virus, floppy disks and other removable media must also be checked so that they cannot re-introduce the virus to the network.

The total cost of the virus attack can be significant, given the loss of time by all employees plus time spent scanning the machines and disks to remove the virus.

Viruses and E-mail

Many viruses are introduced to networks by e-mail messages. Any serious virus needs to introduce an executable file onto your system and e-mail, with its capacity to attach files, is an ideal way to do this.

To protect your system from these viruses you must run a Virus Checker at the point of entry, that is, on the mail server itself so that messages and their attachments can be checked as they enter your system and before they get the opportunity to propagate through the network.



Hoax viruses cannot be stopped by virus checking software as they do not contain any files to pass through the virus checker. You may want to try other means of stopping them such as applying the restricted word filter in Anti Spam. See "GMS Anti-Spam" on page 233.

How the Anti Virus Operates

Anti Virus can be configured to work with any Internet mail server to provide automatic scanning and disinfection of email messages and attachments. This bi-directional process can remove potentially damaging viruses before they enter (or leave) the user's system. This capability is now essential given the emergence of viruses such as Nimda and Klez, which can infect Outlook users and their correspondents when they open, or simply preview, an infected email.

Anti Virus is integrated into the GMS server using a set of custom DLLs or shared libraries. Due to the close integration of these products performance is significantly increased. Coupled with the fact that Anti Virus is multi-threaded this results in significantly faster virus checking with minimal resource use. Multi-threading means many messages can be scanned at the same time. Anti Virus also removes the hassle of installing and configuring a separate third party virus checker, not to mention the mailbox corruption that can be caused by third party software editing mailboxes unbeknown to GMS.

Gordano's Anti Virus comes with two distinct Anti Virus engines, providing both normal virus protection and protection from so called Zero Hour threats.

The first of these, supplied by Authentium, provides an interface between MIME and TNEF encoded messages and the virus checking engine. It takes the encoded files, decodes them and passes them to the virus checking software. If it finds a virus in the

decoded file, it acts as you specify. Otherwise, the attachment is re-attached and it is passed to the recipient in the normal way.



To maintain protection from viruses, keep your Anti Virus active, operational and update it regularly.

The second engine, provided by CommTouch, protects from Zero Hour threats. This engine is only called for messages that have successfully passed through the Authentium engine. This provides a second ring of defences against virus attack, specifically targeting those viruses that are actively being transmitted across the Internet at the time of checking.

If a message fails the check, it can be returned to the sender, rejected, quarantined, re-directed to another mailbox for dealing with later or allowed to pass through the system in the normal way. In addition, you can generate an alert message for sending to the Postmaster, the recipient and/or the sender of the message. If you return the message to the sender you can append a message warning them that there may be a virus in the message attachment. Anti Virus will also allow you to dis-infect a virus before it is sent on.

This dual approach to Virus protection is essential to provide full protection from both new and existing virus threats. Zero Hour cover provides protection from the time a new virus is released into the wild until such time as the traditional Anti Virus companies have time to implement and distribute a definition file specifically designed to capture the virus. After a period of time, dependant on how prolific the virus is, it will drop out of the scope of Zero Hour protection.

Automatic Updates

With up to 300 new viruses being written each month regular updates to your anti virus solution are essential in protecting your system and your organisation's reputation. It is very easy for a busy administrator to forget or delay updates to virus signature files so Gordano have added an automatic update facility to Anti Virus. The automatic virus updates feature allows up to the minute awareness of current viral threats. Being directly integrated with Gordano's products, the Anti Virus interface allows the Administrator to determine when and how often the updates are to be received and implemented. If preferred, updates may still be received automatically but manually deployed. (see "Automatic updates" on page 293).

22.2 Setting Up Anti Virus

This section describes how to set up Anti Virus. When you first install Gordano products on your machine if you have chosen to

install the anti virus options GMS Anti Virus will be automatically enabled. GMS Anti Virus will operate for 28 days as a fully functioning demonstration. Licence keys to extend operation beyond that point can be obtained from sales@gordano.com



Although GMS Anti Virus is enabled on install the latest definition files may not be present. See "Automatic updates" on page 293

Configuration

This screen allows you to configure all of the options pertaining to the operation of both the traditional definition (or signature) based Anti Virus engine and the Zero Hour protection based engine.



Zero Hour is a term given to the period between a virus being released in the wild and Anti Virus vendors making updated virus definition files available.

Scanning Options

The options set here control the operation of the virus scanner, which protocols it operates on and which activities cause the message to be checked for viruses.

- Scan SMTP inbound/outbound messages — scans all internal and external SMTP traffic. Enabled by default, this is the only virus checking action normally carried out by other less security conscious vendors.
- Scan POP messages on read — scans messages as they are read from the POP service. Disabled by default as it has the effect of slowing the performance of the POP service. Enabling this option will provide further coverage for the zero hour period due to the normal delay between a message being received on the server and it being retrieved by a POP client.
- Scan WebMail attachments on attach — the scanning of attachments as they are being attached to a message within GMS WebMail not only provides protection against the transmission of viruses but also stops viruses being stored on the server prior to being delivered onwards where they can also pose a risk.
- Scan WebMail messages on read — unlike POP and IMAP scanning on read this option does not have a detrimental affect on WebMail performance so is enabled by default.
- Scan IMAP messages on append — enabled by default this option prevents messages infected with a virus entering the server, or users mailbox, by the back door. To illustrate this imagine a user has two accounts, one corporate on the company mail server, and the other personal hosted by a third party. The user sets both accounts up in Outlook and copies a

- message from the unprotected third party server to his account on the corporate server.
- Scan IMAP messages on read — scans messages as they are read from the IMAP service. Disabled by default as it has the effect of slowing the performance of the IMAP service. Enabling this option will provide further coverage for the zero hour period due to the normal delay between a message being received on the server and it being retrieved by a IMAP client.
 - Scan Collaboration attachments on attach — enabled by default this option will scan any files associated with calendar entries prior to uploading those to the server. This also applies to notes, tasks, etc.
 - Scan Collaboration attachments on read — likewise enabled by default this option will scan any files associated with calendar entries prior to delivery to the client. This also applies to notes, tasks, etc.

Signature Scanning

To set up the way in which each message is treated with regards to passing encapsulated files to the virus scanner select one of the following:

- Decode email messages — this is the default action for messages. Each message is broken into its constituent parts and each of these passed to the scanner separately.
- Scan whole email messages — this option may be enabled in addition to the above option to provide a secondary check of the message. While this requires additional processing time for a message you may want to enable it.
- Decode TNEF files — this is the default action for TNEF files. Each file is broken into its constituent parts and passed separately to the scanner.
- Scan whole TNEF files — this option may be enabled in addition to the above option to provide a secondary check of the TNEF file. While this requires additional processing time for a message you may want to enable it.
- Scan inline text — enabling this option provides scanning of all text that should be displayed in line within a mail client. This check is useful if you suspect that a message may, for example, contain malicious JavaScript.

Zero Hour Classification

The behaviour of the Zero Hour scanner is controlled with the following settings:

- Enable Zero Hour classification checks — enabled by default. The Zero Hour option is run after a standard virus check so is only applied to messages that have already passed the signature based check.

- Use strict checks — there are two levels of activity reported, Medium and High. If this option is enabled both Medium and High are treated as a potential virus. If it is not enabled only the High option is treated as a virus. This option is disabled by default as it can lead to a number of false positive results due to being very cautious. If you enable this option we would recommend that messages failing the check are placed in quarantine and rescanned 24 hours later.
- Fail on error — if this option is enabled messages that the Zero Hour protection has been unable to classify, for whatever reason, will fail the checks.
- Re-scan messages on read if less than n days old — disabled by default this option was added in to provide an even higher level of protection. No matter how quickly any solution updates, there is always the possibility of the odd message slipping through the system. If this is enabled the checks will be re-run against messages when they are read from the server.

Actions

By default the Anti Virus scanning engine is enabled. To disable it choose Anti Virus, Actions and ensure the "Virus scanner enabled" check box is not selected.

To set up the way an infected message is handled, select one of the following:

- Return with — this is the default action. The message is rejected and returned to the sender along with any message you supply.
- Reject Message — the mail is rejected with a "500 This message contained a virus" SMTP reply code.
- Redirect To — the message is redirected to the given account.
- Deliver Message as Usual — the message is delivered to the intended recipient in the normal manner.
- Copy message to Quarantine folder — the message will be copied to the quarantine folder. This folder can be accessed to manage the quarantined messages allowing you to accept, delete or forward these messages. See "Quarantine (domain and system)" on page 144.
- Disinfect Message — this option can be set to disinfect viruses before the message is returned, redirected or delivered as usual.



Note that proprietary media subtypes such as ms-tnef or x-msdownload cannot be disinfected if they contain a virus. This is due to the proprietary format of these files. GMS Anti-Virus will however still recognise a virus contained in files of this type.

Configuring Alerts

You can alert a number of people of any attempt to send a virus through the system. Choose Anti Virus, Alerts and select one or more of the following:

- Alert Postmaster — to send an alert to the administrator of the system select this check box. If you would like the alert to go to someone other than the postmaster please enter their email address in the box provided, otherwise the default of postmaster@domain.name is used.
- Alert User — to inform the intended recipient of a virus that someone has attempted to send them an infected file.
- Alert Sender — send a message to the sender of the file alerting them to the fact that they attempted to send an infected file through the system. (They may not know that the message contained a virus.)

Domain Actions

Anti Virus actions can be configured separately for each domain or you can simply elect to use the global values that are set under Actions and Alerts. You can also disable GMS Anti-Virus altogether for a selected domain or domains. This allows you to provide a value added service to selected customers.

Domain Alerts

As for Domain Actions you can over-ride the global settings on a domain by domain basis by entering details here for the currently selected domain.

User Level Actions and Alerts

User Profiles provide a method of setting Anti Virus Actions and Alerts down to the user level. The user level settings may differ from the System and Domain level settings outlined above. This is useful where you may want to provide a more relaxed set of actions for some users on the system while maintaining a strict Anti Virus policy for others.

For more information on this and other profile options See "Profile Management" on page 99.

Virus Reports

The Reports option in the menu provides 2 reports relating to GMS Anti-Virus. They are:

- Virus Scan report - this report shows messages that have passed through the virus scanner and whether or not they were found to contain a virus. The first step asks you what you would like

included in the report. You can choose to display results for all messages that have been scanned and/or messages that were found to contain a virus. Simply check the options you require, select the days you would like the report to cover from the list of dates then click on the Report button. You can select multiple days from the list by holding down the "Control" key on your keyboard while selecting the dates with the mouse pointer. See "Virus Scan Report (domain and system)" on page 146.

- Virus List report - A list of Viruses the system is protected from can be displayed when selecting this report. Enter the name of the virus you wish to check the system is protected from and click Report. If you are unsure of the complete name of the virus you can use the wildcard "*". For example searching for nim* would return results including the following:

Nimda.A@mm
Nimda.B@mm
Nimda.E@mm

See "Virus List Report (domain and system)" on page 147.

Reading Zero Hour information

The Zero Hour virus protection will write information into the headers of messages it has processed. This information can be used to determine how the Zero Hour check has processed the message and to determine the results of that processing.

X-Zero-Hour-AV-Classification: 0 [62.172.232.100]

X-Zero-Hour-AV-Classification-RefId:

str=0001.0A0B0203.444C8E3E.0011,ss=1,fgs=0

Classifications are:

0 - Unknown\Undetermined

1 - Medium

2 - High

4 - Non Virus

We treat 2 as a virus and 1 if strict mode is enabled.

The RefId is an internal reference used when reporting false positives via the Quarantine reports. If you ever need to query the status of a false positive report you will need to quote the RefId.

23 Automatic updates

23.1 What are automatic updates?

Both GMS Anti-Virus and GMS Anti-Spam provide the facility of obtaining automatic updates to virus signatures and dynamic word lists respectively. These are controlled from the automatic updates pages with each of the options being individually described below.



The technology used to perform automatic updates is patented in the United Kingdom under patent number GB2374163. A patent application has been filed in the United States and is pending approval.

23.2 How updates work

GMS contacts Gordano via email at the intervals you have defined to check if there are any updates that should be applied. If there are, the Gordano server will send a reply with the new files attached. The files are then placed in the "update" directory.

They stay in this directory until the Gordano Manager service moves them to their normal working directory. This is done upon their arrival in the folder specified above.

The reason for writing the files to this location is to allow GMS to dynamically unload the SMTP and Configuration Server services. GMS does not need to stop and restart any services ensuring a smooth definition file update process.

Request Update Now option

There is a Request Update Now option on each of the individual product update pages of the interface. This sends the request email to Gordano immediately and the update files are returned within a few minutes.



The files in the installation may not be the latest files available. For the latest files use the Request Update Now option.



If you have just installed GMS you should use the Request Update Now option to retrieve the updates as soon as possible.

23.3 General Update information

Some of the information required for updates to progress correctly is common to all updatable products. This information includes:

Send update warnings

If you would like to be notified if an update event occurs then select this option, you will receive warnings of successful updates as well as any update failures.

Send warnings to

Enter the address that you would like warnings of any problems arising out of the update procedure mailed to, this is pre filled with the email address of the system administrator but may be changed to any valid email address you wish.

Passphrase

This will be supplied to you at the time you purchase your license for the relevant products from Gordano Ltd. Once your purchase has been completed and a passphrase issued to you please enter it here. The passphrase is essential to allow you access to the updated files. Please take care to enter the passphrase correctly, an incorrect passphrase will stop you receiving your updates.



When you purchase a key for GMS Anti-Virus sales will ask you for a passphrase. You should enter the same phrase here that you gave to the Gordano sales person. Note that these passphrase are case sensitive. If you are just running a demo of the software you can just elect to use the default pass phrase by leaving the box blank.

23.4 Anti Spam

This feature allows you to automatically obtain the latest dynamic word files and Bayesian filter from Gordano Limited. With Anti Spam installed there is no need to go and retrieve updates manually, the software does it for you.

The topmost line on this page will show you the date of the most recently applied dynamic word list.

To configure this option select System Administration, Automatic Updates, Anti Spam and select one or more of the following:

- Send Updates To — The email address that updates should be sent to. By default this is set to gmsas@<domainname>. If this account exists on your system as a valid user you should change this address to an account that does not exist on your server.
- Automatic updates — Enables/disables the automatic update of dynamic word files and Bayesian filter.
- Update Every — The interval in days, hours or minutes between each check for new updates.

Once you have completed your configuration click on the **Update** button to confirm the changes.

The **Request Update Now** button allows you to immediately send off a request for the most recent updates without having to reconfigure your schedule.

23.5 Anti Virus

This feature allows you to automatically obtain the latest virus signature files. With GMS Anti-Virus installed there is no need to go and retrieve updates manually, GMS Anti-Virus does it for you.

The topmost line on this page will show you the current state of your GMS Anti-Virus installation. It contains three sets of numbers, the first of these shows the version of the AV engine you are running, the second the date of the virus signature files currently installed and the third the date of the macro signature files installed.

The virus signature files contain all the information required to enable Anti Virus to recognise any standard viruses while the macro signature files are specifically for macro viruses, e.g. viruses written in Microsoft Word or Excel macro languages.

To configure this option select System Administration, Automatic Updates, Anti Virus and select one or more of the following:

- Send Updates To — The email address that updates should be sent to. By default this is set to gmsav@<domainname>. If this account exists on your system as a valid user you should change this address to an account that does not exist on your server.
- Automatic Virus definition updates — Enables/disables the automatic update of virus definitions.
- Update Every — The interval in days, hours or minutes between each check for new updates.

Once you have completed your configuration click on the **Update** button to confirm the changes.

The **Request Update Now** button allows you to immediately send off a request for the most recent updates without having to reconfigure your schedule.

23.6 Zero Hour Proxy

The Zero Hour Proxy settings only need to be set if you do not have direct outbound access to the Internet on Port 80 from your GMS server.

Use Proxy server

Enable this option if you need to use a Proxy server to access external web sites from your GMS server.

Address

The fully qualified address of your Proxy server, i.e.
proxy.domain.com

Port

The port that your Proxy server answers requests on, this is normally 8080.

Authentication Method

Most Proxy servers do not require authentication so you should not need to change this from the default. In the event that your Proxy server does require authentication there are two options available to you.

1. Basic — A plain text username and password combination are required to access the Proxy server
2. NTLM — The Proxy server uses a challenge/response mechanism to authenticate users. Commonly used by Microsoft based servers such as IIS.

Username

Specify the username required to authenticate to the Proxy server.

Password

Specify the password associated with the username entered above.

23.7 Freebusy

This page allows you to enable the automatic pushing out of updates to the GMS Outlook connector. Once the Connector has been installed on a client PC all future updates to the connector can be pushed out to the client automatically.

In order to be pushed out to the client the updates must be placed in the following directory on the server where basedir is the root of the Gordano installation.

`\<basedir>\collaboration\update`

The following files can be updated:

- gmsmapi32.dll (compulsory)
- gmsdb.dll (optional)
- gmszlib.dll (optional)
- gmssseay32.dll (optional)
- gmslibeay32.dll (optional)

To enable automatic updates for all clients connecting to the server first place the files in the correct directory then select the option Enable Automatic Updates and click on the Update button. Each

client that connects to the server will then check it is running the latest versions of the above files and if required will have the updates pushed out to them automatically.



We strongly recommend copying all of the files each time to avoid any consistency issues.

24 GMS Collaboration Server

24.1 What is GMS Collaboration Server?

GMS Collaboration Server allows you to integrate Microsoft Outlook tightly with your email system and allow your users to work collaboratively by sharing information between users. Users can use and share with others advanced Outlook features such as tasks, journals, notes, address books, contacts, calendars and shared/public folders, without the need for Microsoft Exchange. Support for these facilities is also available in the GMS WebMail client allowing remote web based access to email, calendar events, alarms and contact lists.

Outlook Contacts are automatically mapped to the users personal address book in GMS WebMail and vice versa, while access to global address books is via the Outlook Address Book interface.

Access rights are obeyed at all times, setting up those rights was described earlier. See "Shared and Public Folders" on page 154..

The GMS Collaboration client fully supports standard Outlook features such as voting, scheduling, task assignment, read receipts, automatic archiving and so on. External e-mail editors such as MS Word are also completely compatible.

Both the Collaboration Server and Client are fully UTF-8 aware to provide full support for multiple languages including multi-byte languages such as Japanese and Chinese.

In order to use the GMS Collaboration Server the GMS server must have a valid GMS Collaboration key installed, and the machine running Microsoft Outlook must have the GMS Collaboration client installed. The Collaboration client is a Microsoft Outlook plug-in that integrates tightly into the Outlook user interface providing seamless integration with the GMS server software. No license is required for the client installation, however only the licensed number of clients may connect to the server.

Full installation instructions for the GMS Collaboration client are included in the GMS User Guide.

Like other products developed by Gordano Ltd, the GMS Collaboration Server has been developed with open standards in mind at all times. As a consequence of this a number of other clients are able to access shared Calendars and Tasks such as Apple iCal, Mozilla Calendar, Bloomba, EventSherpa, KDE Kontact, and so on. In fact any client that supports the iCal standard should be compatible with GMS Collaboration server. Full details of how to configure these additional clients can also be found in the GMS Users Guide.

24.2 Collaboration free/busy

GMS Collaboration Server has the ability to act as an Internet free/busy publisher for all users on a GMS Server. Scheduling is also supported using this feature. The provision of a free/busy server negates any security worries associated with the use of public free/busy servers.

Enabling publishing of free/busy information allows all users of MS Outlook on the same server to automatically see whether other MS Outlook users are free or busy at certain times of the day dependant on the entries in their Outlook Calendars. Free/busy information is also published for GMS WebMail users allowing their information to be available to Outlook Scheduling.

Invitations to meetings or events can be sent to users to invite them to attend meetings and their responses can be used to finalise meeting plans in the normal way.

Private entries may either be returned to free/busy queries or not, depending on your preferences. All private entries will be shown as busy.

You may also set the length of time that information should be published for, the default is 61 days, approximately two months, but you may set this to whatever period you prefer in days.

Individual users may over ride these settings if they wish by editing their private information under My Account, Freebusy.

24.3 Email only mode

The GMS Collaboration client may also be used without the GMS Collaboration Server being enabled, this is known as email only mode. Using the client in email only mode provides full access to sharing of mail folders only. Personal calendars, tasks and notes are still available within Outlook but these can not be shared with other users on the system unless the GMS Collaboration Server is enabled.

Gordano believes that at this time Outlook with the GMS Collaboration client installed in email only mode, is the only standard mail client that allows both the setting of and accessing of Access Control Lists in order to allow full sharing of mail folders amongst groups of users.

Full instructions on using the GMS Collaboration client for MS Outlook are available in the GMS User Guide.

24.4 Automatic client updates

Once the GMS Outlook Connector has been installed on a client PC all future updates to the connector can be pushed out to the client automatically. In order to be pushed out to the client the updates

must be placed in the following directory on the server
\\<basedir>\collaboration\update where basedir is the root of the
gordano installation.

The following files can be updated:

- gmsmapi32.dll (compulsory)
- gmsdb.dll (optional)
- gmszlib.dll (optional)
- gmssseay32.dll (optional)
- gmslibeay32.dll (optional)

We strongly recommend copying all of the files each time to avoid any consistency issues.

To enable automatic updates for all clients connecting to the server first place the files in the correct directory then go to System Administration, Automatic Updates, Freebusy and enable the option "Enable automatic updates". Each client that connects to the server will then have the updates automatically pushed out to them.

It is also possible to enable/disable automatic updates at the domain and individual user levels but you will need to edit the domain or user variables directly as there is no configuration page. The relevant variable is "CollaborationEnableUpdates", set this to "0" to disable updates and "1" to enable updates. The standard user/domain/system hierarchy is followed so that you can enable updates globally but switch them off for specific users.

Client Updates

There is no interface on the client side to handle automatic updates. However some new directories and files will be present as follows.

<base>/GMS/MAPI/Updates - This is where downloaded updates are stored until they can be installed.

<base>/GMS/MAPI - This is where installed updates are stored.

Updates are downloaded on startup and are only installed once Outlook has been re-started. The user is sent an email to remind them that they will need to re-start Outlook in order for the updates to be applied.

For the update mechanism to work the version number of the updates must be greater than, or equal to the installed version number AND the MD5 of the DLLs must be different.

To remove a set up updates, stop Outlook and delete all DLLs in the GMS/MAPI directory. You will probably want to disable updates for the user before doing this to prevent the update being downloaded from the server again.

How do I obtain updated client files

There are two methods of obtaining new client files to use with the automatic update service.

1. Install the new Outlook connector on a client PC and take a copy of the files from the windows\system32 directory on that PC; or
2. Run "msiexec /a GMS-Collab-MSIv1.0-3625.msi" and specify a local directory for the network location drive. The files will be automatically extracted into the specified directory for you.

We would recommend option 2 above as the most suitable option for the majority of situations.

24.5 GMS & Microsoft® Exchange ActiveSync

What is EAS?

Microsoft® Exchange ActiveSync is an XML-based protocol that communicates over HTTP (or HTTPS). It is used to synchronise email, contacts, calendar, tasks and notes between a messaging server and a mobile device without the need to install a client application on the mobile device. The protocol also provides mobile device management and policy controls.

Initially a client will use the Autodiscover command to get a user's account configuration. The client can then view and modify server data related to that account, this data can include email messages and attachments, folders, contacts, and calendar requests. The client then uses the Provision command to send device information to the server and to get and subsequently acknowledge security policy settings from the server. Next, the client uses the FolderSync command to retrieve the folder hierarchy of the user.

How do I use EAS?

The use of EAS requires you to have an active GMS Collaboration license in place and is controlled via your GMS profiles for users. A user must be in a profile that has EAS active under the privileges section.

To activate EAS under profiles, you will need to select a domain from the administration interface dropdown, located in the top left hand corner. From there, go to Profiles > (Name of profile you wish to enable EAS under) > Privileges. Here you will see a tick box for "May use Microsoft® Exchange ActiveSync", which you will need to tick and then click on Update Settings to activate the feature.

GMS

Home My Account Quarantine Sharing

Select Domain
gordano.com

Profiles

Document Sharing

Domain Admin

Domain Base Profile

fax

List Admin

Mail only Webmail

No Collab

webmail only

Groups

Domains and Users

Domain Administration

Anti Spam

Anti Virus

Reports

Support

Profiles - Domain Admin

Account Settings Access Rights Configuration Rights Privileges Preferences Users

☒ May collect email from POP3/IMAP4 servers

☒ May send HTML email

☒ May CC email

☒ May Bcc email

☒ May use Calendars, Tasks and Notes

☒ May use Gizmos

Mobile Gateway

☐ May use SMS Gateway

☐ May use Pager Gateway

Instant Messaging

☒ May use GMS Instant Messenger

☒ Launch GMS Instant Messenger on logon

☐ Include the following image

Image URL :

Alt Text :

Link To URL :

☐ Allow user selected image

☐ Allow user presence indication

Offline Image URL :

Online Image URL :

Collaboration

☒ May use GMS Collaboration

Microsoft® Exchange ActiveSync

☐ May use Microsoft® Exchange ActiveSync

Documents

☒ May use documents

Document store capacity : 20 MB

Maximum revisions :

Update Settings

EAS Troubleshooting

EAS in GMS has been designed to use the GMS Collaboration port, which is set in the administration interface under System Administration > Performance > Ports. By default, this is usually either 8376 for non-secure access or 8377 for secure/SSL connections. For some users attempting to set up their Android devices for use with EAS, this can be a potential issue as some devices do not allow you to specify the port to connect on and uses the default port 80 dictated by the device. In these instances, a workaround is possible by using the IP Connection feature in GMS, to redirect traffic from Collaboration attempting to connect on port 80 to the correct port specified for the service.

You can find further information on the IP Connection feature and how to set it up, on section 13.3, page 164 of this Administrators guide.

24.6 CalDav and CardDav Functionality

What is CalDav and CardDav?

CalDAV is an Internet standard allowing a client to access scheduling information on a remote server. It extends WebDAV (HTTP-based protocol for data manipulation) specification and uses iCalendar format for the data. The access protocol is defined by RFC 4791.

CardDAV is an address book client/server protocol designed to allow users to access and share contact data on a server. The CardDAV protocol was developed by the IETF and has been published as RFC 6352, and uses vCard format for the data.

CalDav/CardDav are an XML-based protocol that communicates over HTTP (or HTTPS) and which is an extension of WebDav protocol. It is used to synchronise contacts, calendar, tasks between a messaging server and a mobile device without the need to install a client application on iOS devices, but is needed for Android mobile devices.

In Short, CalDav allows users to set up a connection to their messaging server, in order to sync their calendar data from GMS to mobile devices, Mac OSX computers and Outlook (with an additional plugin). CardDav allows users to sync their contacts with their own clients from GMS.

How can I use CalDav and CardDav?

The only requirement for using CalDav and CardDav in GMS is to have a GMS Collaboration license in place. Details on how to set up a device or Outlook to use these features can be found in the GMS User guide and on our Knowledge base located on the GMS website.

24.7 GMS Drive & WebDav

What is GMS Drive & WebDav?

Web Distributed Authoring and Versioning (WebDAV) is an extension of the Hypertext Transfer Protocol (HTTP) that allows clients to perform remote Web content authoring operations. A working group of the Internet Engineering Task Force (IETF) defined WebDAV in RFC 4918.

The WebDAV protocol provides a framework for users to create, change and move documents on a server, typically a web server or web share.

GMS Drive, like WebDAV, is a feature that allows you to view your stored Webmail documents on your desktop, via a network drive,

set up by the user on their PCs. Documents placed on the network drive will also be uploaded to your documents in Webmail. This also introduces WebDav features which allows you to sync your documents to mobile devices (with a 3rd party application) and Mac OSX computers

How Can I use GMS Drive/WebDav

A GMS Collaboration license is required for Drive/WebDAV usage on your devices. Assuming you have the license in place, you can download the GMS Drive application from your top level Documents folder in Webmail. The setup process and information on how to setup WebDAV usage with GMS, can be found in the GMS User Guide.

25 GMS Archiver

25.1 Setting up GMS Archiver

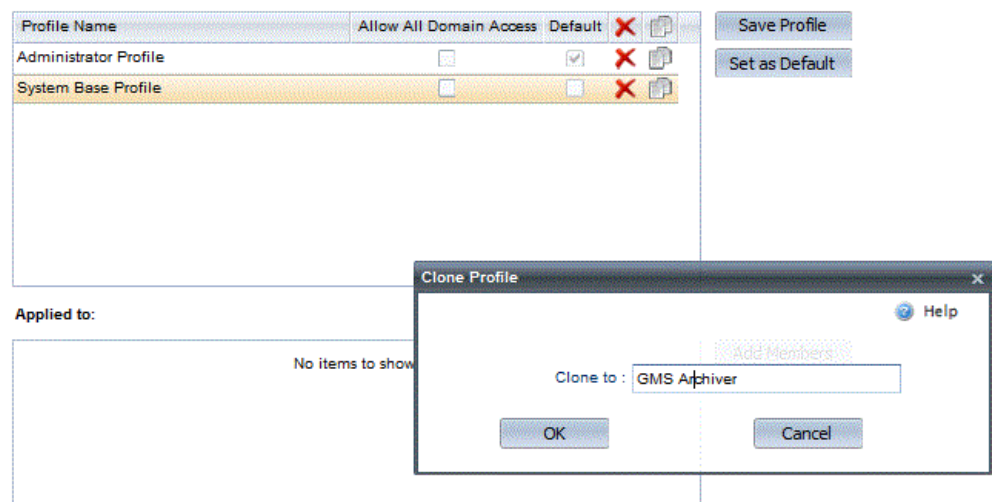
The following steps are necessary to get your GMS Archiver account up and running:

- Add a user profile for GMS Archiver.
- Add a GMS mail account.
- Disable the account's mailbox.
- Configure the account to use the GMS Archiver robot.
- Configure your server to send message logs to the GMS Archive account.

Adding a GMS Archiver profile

Since the GMS Archiver account will be storing archives of all the messages that pass through your mail server the account size can grow quite large. If you impose account size limits on some of your users it is important that the GMS Archiver account is not assigned to a user profile with a small account limit. For this reason it is good practice to create a separate profile just for the GMS Archiver account. This is done in the following way:

1. Logon to the Gordano interface as a system administrator.
2. Select System Administration, Profiles.
3. Select the System Base Profile in the list of profiles.
4. Click on the "Clone To" icon and give the new profile a name, for example "GMS Archiver".
5. Click on the OK button.



You can then edit this profile at any time to increase or decrease the account size limits. The limit you set will be governed by the amount of mail that passes through a domain. For example if your domain processes 100 messages per day with an average size of

1MB you should allow a mailbox and account size of about 50MB. The message logs are zipped before being sent to the GMS Archiver account so in the above example the zipped logs would be approximately 40MB. Setting a limit of 50MB will allow for days where email traffic is greater than usual. Note that if the message containing the zipped messages exceeds the size you set here the message will be rejected as too large and that day's email will not be archived.

Adding a mail account

Log on to the Gordano interface on the machine that has the GMS Archive executable installed. Then select the Domains & Users, Domain page in the interface and click on the New User button in the secondary toolbar. Enter the name of the account to be added, for example "GMSArchiver". Then enter and confirm a password for the account.

Make sure the option "Create mailbox for each new account" is unchecked then select the profile you have just created for GMS Archiver and click on the Add button to complete the addition.



You can add as many accounts as your mail server license permits and configure all of them to use the GMS Archive robot. For example you might want to have a separate GMS Archive account for each domain on your main mail server in order to simplify message retrieval on a domain by domain basis.

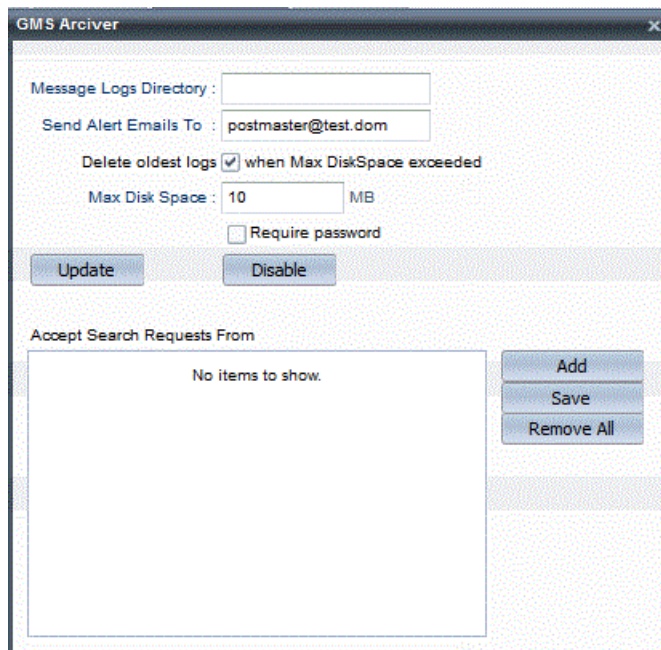
Disabling the mailbox

GMS Archiver stores the archives it receives in a directory that you specify. This is a separate area from where the account's mailbox is kept. In order to avoid ending up with two copies of the messages that GMS Archiver receives it is a good idea to ensure the mailbox for the GMSArchiver account is disabled. This also prevents all the search requests sent to GMS Archiver being kept needlessly.

To disable the mailbox, assuming you mistakenly enabled it above, log on to the Gordano administration interface and select the Domains & Users, Domain, Username, Preferences page. Then ensure that the "Save nothing locally" option is selected then click on the Update button.

Configuring the GMS Archiver robot

Once the mail account has been added select the Domains & Users, Domain, Username and then the Mail Processing tab for the user account you have just added. Now select "GMS Archiver" from the drop down marked "Select Robot" and click on the Configure button. This will display the configuration options for GMS Archiver as described below:

The screenshot shows a window titled "GMS Archiver". It contains several configuration fields: "Message Logs Directory" (empty), "Send Alert Emails To" (filled with "postmaster@test.dom"), "Delete oldest logs" (checked) with a sub-label "when Max DiskSpace exceeded", "Max Disk Space" (filled with "10" and "MB" next to it), and "Require password" (unchecked). Below these fields are "Update" and "Disable" buttons. At the bottom, there is a section "Accept Search Requests From" with a list box containing "No items to show." and three buttons: "Add", "Save", and "Remove All".

- **Message Logs Directory**

Specify the directory where the message logs for this GMS Archiver account should be stored. This directory should exist on your server.

- **Send Alert Emails To**

Enter an email account that will receive alerts of any problems with the account, i.e. disk space exceeded.

- **Delete Oldest Logs**

If the maximum disk space entered is reached and this box is checked the logs will be deleted strictly in order of oldest first. This option is enabled by default.

- **Max Disk Space**

The maximum amount of disk space allocated to the archive store measured in MB. This will depend on the amount of mail you receive and how long you want to keep messages for. For example if you have 100 messages pass through your domain each day, averaging 1MB in size, you can expect your zipped daily archive files to have an average size of 40MB. If you want to keep messages for a year you will need to specify a disk space of at least $365 \times 40 = 14,600\text{MB}$. It is a good idea to add 10% to this to cover any busy mail days. It is also recommended that you review this setting periodically as the

amount of daily email traffic in most organisations is steadily increasing. Once this limit is reached the oldest messages will be deleted until there is enough space for the new messages.

- **Require Password**

Check this option if you wish to enforce a password requirement for all archive searches. The password used is the password entered for the account created earlier in this section.

- **Accept Search Requests from**

A list of email addresses that the GMS Archiver robot will accept requests from. To add an email address click on the Add button then enter the address in the text area and press Enter. Repeat for any further addresses then click on the Save button. To remove an address simply highlight it in the list and click on Delete. Clicking on the Remove All button will remove all addresses at once.



Search requests from any address not listed will be refused. If no addresses are entered searches will be accepted from any address.

When you have finished setting up all the details for the GMS Archiver account click on the Update button. To disable the robot click on the Disable button, the robot will no longer be associated with the account.

Sending the message logs to the GMS Archiver robot

Now that the GMS Archiver account is configured and ready to compile an archive you need to tell GMS to send daily updates of messages passing through the server to the GMS Archiver account. This is done in the following way.

1. Log on to the GMS interface on the machine that the messages will pass through.
2. Select the domain from the drop down and then go to the Domain Administration, Logging, Message Logging page.
3. Select the "Configuration for GMS Archiver account" option and enter the fully qualified address of the GMS Archiver account, i.e. GMSArchiver@domain.dom in the space provided.



Early versions of GMS Archiver may refer to this setting as "Configuration for eSarah account"

4. Click on the Update button.
5. The "Manual configuration" option will now be selected and the other log options will have been automatically configured to their optimum settings for GMS Archiver.
6. Repeat this process for each domain that you wish to archive.

7. If you wish to archive your relay logs as well as your message logs select the System Administration, Logging, Relay Logging page.

The screenshot shows the 'Relay Logging' tab selected in a toolbar with other tabs like 'Logs', 'W3C Logging', 'Transaction Logging', 'Quarantine', 'Reported Junk Mail', and 'Watch'. Below the tabs, there are two radio buttons: 'Configuration for GMS Archiver Account' (unselected) and 'Manual Configuration' (selected). Under 'Manual Configuration', there are three checkboxes: 'ZIP logs after' (unchecked), 'Email logs to' (unchecked), and 'Delete logs after' (unchecked). Each checkbox has a corresponding text input field and the word 'days'. The 'Email logs to' field has an 'after' label and another text input field followed by 'days'. At the bottom left, there is a button labeled 'Update Settings'.

25.2 Retrieving messages from the archives

There are two methods of searching and retrieving messages from the GMS Archiver archives

- Using the Gordano Interface
- Via an email request to the GMS Archiver account.

Interface method

The GMS Archiver archives can be queried by going to System Administration, Logging and clicking on the Off Site Search button in the secondary toolbar. On this page enter the name of the GMS Archive account and the password you gave the GMSArchiver account when you created it. Then enter your search criteria. Wildcards may be used when making searches, for example

entering "user*" in the From field would find both user@somedomain.dom and user@otherdomain.dom.

Select the dates that the search should be run on from the drop down boxes provided, and enter the email address that the results of the search should be sent to.

The information returned by the search can be limited by setting the number of matching results to return. While the Return option allows you to select how the results of the search are returned to you. There are three options available for this, as follows:

- **Index** - Returns an index of the results, you can then select which messages you would like to see from this index file and request them back from GMS Archiver. For example an index might contain the following message details:

```
[] id = company.dom,2012-09-25,00000014
# From: "GMS Communicator" <List@Company.dom>
# To: "Jacks@Company.dom" <Jacks@Company.dom>
# Subject: Welcome to new list
```

If you want to see the full message click on reply and enter a X between the square brackets [] For example:

```
>[X] id = company.dom,2012-09-25,00000014
># From: "GMS Communicator" <List@Company.dom>
># To: "Jacks@Company.dom" <Jacks@Company.dom>
># Subject: Welcome to new list
```

Click on send and in a short time GMS Archiver will send you the full contents of any messages you have marked with an X.

- **Messages in a single email** - All messages matching the search will be returned to you in a single email.
- **Messages in a separate email** - All messages matching the search results will be returned to you, each in an individual email message.

Email method

You can send an email message to the GMS Archiver account from an email address that is authorised to query the GMS Archiver archives. The email message must be in the following format:



To save time, if you have a GMS WebMail account you could set up a template that has these details pre filled.

```
Password = GMSArchivepassword
SearchToDate = 2012-09-24 00:00:00
SearchFromDate = 2012-09-20 00:00:00
From = *
To = *
BodyContains = *
Subject = *
ResultsLimit = 50
ResultsFormat = Index
ResultsTo = postmaster@company.dom
```

Lets look at the lines of the message in more detail

Password

This is the password you gave the GMS Archiver account when you first set it up. If this line is not present then the search will be rejected.

SearchToDate

This date must be specified in the format "yyyy-mm-dd hh:mm:ss". GMS Archiver will return messages logged prior to this date that match your other search criteria. This line is optional and can be removed if you don't want to specify a date.

SearchFromDate

This date must be specified in the format "yyyy-mm-dd hh:mm:ss". GMS Archiver will return messages logged after this date that match your other search criteria. This line is optional and can be removed if you don't want to specify a date.

From, To, BodyContains, Subject

These define the search terms that GMS Archive will use to find the messages you want to retrieve. For example if you want to retrieve all messages to and from userA@company.dom you would have:

```
From = userA@Company.dom  
To = userA@Company.dom
```

At least one of these lines should be included in the message. The others can be removed if required. You can use standard wildcards in your search terms such as * and ?.

ResultsLimit

Specify the number of results that you want the search to return. If you don't want a specific number you should enter "All".

ResultsFormat

This is the format the results will be returned in. There are three options available for this, as follows:

- **Index** - Returns an index of the results, you can then select which messages you would like to see from this index file and request them back from GMS Archiver. Type "Index" to get the results in this format.
- **Messages in a single email** - All messages matching the search will be returned to you in a single email. Type "SingleMessage" to get the results in this format.

Messages in a separate email - All messages matching the search results will be returned to you, each in an individual email message. Type "Manymessages" to get the results in this format.

ResultsTo

This is the email address you want the results to be sent to. This allows you to direct search results straight to the person that requested the search.

26 Troubleshooting

Start with this section if you have problems with GMS. It indicates where to look to fault find problems and gives examples of typical problems.

This section covers:

- What you need to know to find faults on your network.
- Testing the GMS installation.
- Checking the network.
- Checking your DNS.
- Checking sending of mail.
- Checking collection of mail by POP3.

All administrators who have GMS problems or solve problems for others should read this section.



For answers to frequently-asked questions which do not relate to problems, see "Frequently-asked Questions" on page 333.

26.1 Preparing to Find Faults

This section explains what you need to know to find faults on your network.

In order to diagnose Internet connectivity and mail problems, you need the following information. In this section we use the examples given here for illustration:

Description	Example value
IP address of your mail server	123.123.123.123
IP address of your DNS server	123.123.100.100
A Name of your mail server	mail.company.dom
MX name of your mail server	company.dom
A well known Web site.	www.gordano.com

Unless stated, we assume you are working on your mail server.

26.2 Testing the Installation

Once GMS is installed, carry out the following tests to ensure that it is working correctly.

Mail the postmaster, as follows:

1. Open your mail client and set it to use the name of the mail server for both SMTP and IMAP/POP servers.
2. Set your mail client to use the username "postmaster".
3. Send mail to "postmaster@domain.dom" (<domain.dom> being the domain you specified during installation).
4. Retrieve mail from the postmaster account — you should see the message you just sent.

Mail a new user, as follows:

1. Point your web browser at `http://server.domain.dom:8000`.
2. Log on using the account `postmaster@domain.dom` and the password that you supplied during installation.
3. Add a new user to the server, then send mail to them and make sure it arrives safely in their mailbox.

Mail a remote user, as follows:

1. Send a mail message to someone on a remote mail server and ask them to respond to you. Check that the mail has been sent out correctly and that a response is indeed received. This may take some time.



If you have problems with any of these, the most likely cause is that DNS is not set up correctly. There are some useful tips on checking this in "Troubleshooting" on page 317.

2. There is a special account `test@gordano.com` that you can use for this test. It automatically sends a response back to you.
3. If you are on a dial-up connection, you must set up a dial-up schedule first.

26.3 Checking the Network

Using ping

To check that the network is working, use the program called **ping**. This is an MS-DOS program so can only be run from a command prompt. It sends a packet to a remote machine and displays the time it takes to get a reply from it.

To ping a machine, type **ping** followed by the mail server's IP address:

```
ping 123.123.123.123
```

There are several likely responses:

- A set of replies like those shown below confirms that the Internet Protocol is successfully installed on the machine.

```
C:\>ping 194.205.1.2
```

Pinging 194.205.1.2 with 32 bytes of data

Reply from 194.205.1.2: bytes=32 time=15ms TTL=125

Reply from 194.205.1.2: bytes=32 time=15ms TTL=125

Reply from 194.205.1.2: bytes=32 time=15ms TTL=125

Reply from 194.205.1.2: bytes=32 time=15ms TTL=125

C:\>

- Command not found — this occurs if IP (Internet Protocol) has not been installed on your mail server. Choose Control Panel, Network and install “Microsoft TCP/IP” from the appropriate installation disk.
- Request timed out — you have probably either typed the wrong IP address or the mail server has a different IP address to that you typed. Check the IP address in Microsoft’s network setup.

Checking connectivity between mail and DNS servers

The next task is to test connectivity out from your mail server to the DNS server. If you are using a dial-up connection, dial-up now. This time type **ping 123.123.100.100**.

Again there are several likely responses:

- Timed out — if your line is busy, the response from the remote machine may be lost. If this happens, type:

```
ping -w 5000 123.123.100.100
```

If you still receive no response, check that the DNS server is up and working correctly. Contact the ISP and check that the IP address you typed is correct.

- “Reply from 125.88.25.1:destination host unreachable”.
This is a response from a router informing you that the DNS server cannot be reached. Check your DNS IP address.
- “Reply from 123.123.100.100:bytes 32 time=521 ms TTL=123”.

A reply like this confirms that there is an IP connection to your DNS server. Note that if the time reported exceeds 1000 ms (one second), you will probably have difficulty resolving addresses, since the network between your server and the DNS server is saturated somewhere in between the two ends.

26.4 Checking your DNS

There are two parts to checking your DNS:

- Checking that DNS works.
- Checking that DNS has the right information for your mail domain.

Checking that DNS works

To check that DNS is working (correctly converting domain names into IP addresses), do the following:

1. From an MS-DOS window use **ping** to test whether DNS is working by using a well known Web site. If you are on a dial-up connection, dial up and log on manually. For example:

```
ping www.gordano.com
```

2. After a short time you should see a response like this in the MS-DOS window (the IP address may differ):

```
C:\>ping www.gordano.com
```

```
Pinging w3.net-shopper.co.uk [194.205.1.3] with 32 bytes of data
```

```
Reply from 194.205.1.3: bytes=32 time=15ms TTL=125
```

```
Reply from 194.205.1.3: bytes=32 time=15ms TTL=125
```

```
Reply from 194.205.1.3: bytes=32 time=15ms TTL=125
```

```
Reply from 194.205.1.3: bytes=32 time=15ms TTL=125
```

```
C:\>
```

3. This confirms that the name has been converted to a number by DNS. If you see the response, this confirms that the network between you and the Gordano Ltd. Web site is complete.
4. If you do **ping** a site which you cannot reach, you'll see a response like this:

```
C:\>ping www.testsite.dom
```

```
Bad IP address www.testsite.dom
```

```
C:\>
```

then you need to:

- Firstly, check that you've used the correct Web site address.
- Secondly, check the IP address you entered for the DNS server.
- Thirdly, check the IP address with your ISP.

Does DNS have the correct mail domain information?

If you are on a dial-up connection, do not close the connection. Do the following:

1. Start your Web browser and log into GMS. For our example, you would point it to: `http://123.123.123.123:8000`.
2. Go to Domains & Users, Domain and select Check Domain in the secondary toolbar then click on the Check button. GMS will perform two checks:
 - Using your domain name, it will find the MX records.
 - It will find the reverse address for your mail machine.
3. For example, you may get this response:

MX Lookup Results

```
Company.dom  IN MX 10 mail.company.dom
              IN MX 20 mail.isp.dom
```

```
mail.company.dom  IN A 123.123.123.123
mail.isp.dom      IN A 123.123.200.200
```

Reverse Lookup Results

```
123.123.123.123 is mail.company.dom
```

Check all the names and IP addresses. If they are correct, your MX records are set up correctly.

If there are any errors or you find any of the following, you must change your DNS information:

- If you have one line containing the text "IN MX", obtain permission to use a backup mail server then add this to your MX records. Failure to do this may result in e-mail being returned. This is especially important if you use an intermittent connection.
- If the reverse lookup does not return the name of your mail server, you must change your DNS server. To reduce Spam, some system administrators set up their systems to prevent e-mail from those domains where the reverse lookup does not match the claimed name. GMS Anti Spam supports this option.
- If there's no response after 30 seconds, check that your DNS server is configured correctly. Depending on your operating system version, you may need to explicitly tell GMS the DNS server's IP address — choose System Administration, Performance, MX and type this into the DNS Servers text box. Click on the Update button to effect the change.

You should now have DNS and your network working correctly. You can now go on to look at GMS configuration issues.

26.5 Checking How Mail is Sent

The first question to resolve is "where does e-mail sent to GMS go?". To do this:

1. Stop the POST and POP services by typing **net stop post** and **net stop pop** in the command prompt, using Control Panel, Services or from the System Administration page in the GUI.
2. Send mail to the machine running GMS.

If the mail gets rejected:

1. Check that you are really sending mail to the machine running GMS.
2. Check that you have defined the user correctly.
3. Does the rejection message give any clues about the problem?
4. Turn on full logging — choose System Administration, Logging, Transaction Logging and select all the check boxes. Stop and restart the SMTP service, then send the message again.
5. Check the log in /Gordano/logs/sm.<today's date>.log. Open this file with Notepad or Word. It may give an explanation of the problem.
6. Make sure you don't have a DNS timeout problem — choose System Administration, Settings, Compliance and ensure that the "Resolve hostname on connection" check box is deselected.
7. Check that the ESMTP Size setting is not being exceeded.
8. Is mail relay disabled? If so, check that the domain is defined as local and the IP range is acceptable.
9. Does the directory/Gordano/temp exist and is it valid?
10. If you have GMS Anti-Spam, check the GMS Anti-Spam options.

Check the user's directory using Explorer. You should see two files, inbox.mbx and index.idx. If the mail goes to the user's directory:

1. Which user's directory does it go to? If it's incorrect, check user aliases.
2. If the mail goes to the defined Unknown user action, use Notepad to examine the message and check for a reported error. Check the header to see who the message was originally addressed to.
3. Turn on full logging — Go to System Administration, Logging, Transaction Logging and select all of the check boxes for SMTP. Stop and restart the SMTP service, then send the message again.
4. Check the log in \Gordano\logs\sm.<today's date>.log. Open this file with Notepad or Word. It may give an explanation of the problem.

If the mail goes to the Out directory:

1. This suggests that the local domain name has not been set up correctly.
2. Check that the number of users does not exceed the licence.
3. Check that the part after the '@' appears in the Local Domains list.
4. Turn on full logging — Go to System Administration, Logging, Transaction Logging and select all of the check boxes for SMTP. Stop and restart the SMTP service, then send the message again.
5. Check the log in \Gordano\logs\sm.<today's date>.log. Open this file with Notepad or Word. It may give an explanation of the problem.

26.6 Checking Collection of Mail via POP3

If you have problems receiving mail, try using telnet to gain access to your mailbox. This will ensure the POP server is functioning properly. You will need to use a Telnet application to access the POP server. Windows offers an inbuilt Telnet application.



You must specify port 110, otherwise you will see a message from the POP server reading "login:" and the procedures below will fail.

To use telnet, open an MS-DOS Prompt and issue this command, replacing <your.pop.server> with your POP server name:

```
C:\>telnet <your.pop.server> 110
```

For example, you might type **telnet 123.123.123.123 110**.

This is sample text from a mailbox telnet session:

```
S: + ok POP server ready
C: user userid
S: +OK Password required for account.userid.
C: pass password
S: +OK userid has 3 message(s) (7683 octets)
```

Here we typed **user userid**, then after the OK we typed **Pass password**. In this example this mailbox is working properly and has three messages. If mail cannot be downloaded, the cause is one of the following:

- The e-mail client software is not configured properly.
- There is a problem with the mail client software itself.
- One of the messages may be causing a failure in your mail client while the mail is being downloaded. This may be a non-standard or large e-mail message that is causing the e-mail client software to abort the download.

Do the following:

1. Try reading your mail with the GMS WebMail interface.
2. Delete all mailbox messages using the GMS WebMail account.
This process is irreversible and the mail cannot be recovered.
3. Use Telnet to delete the message selectively, causing your e-mail application to terminate (see the Telnet commands below).

Available telnet commands

Once you have accessed your mailbox with telnet, you can use:

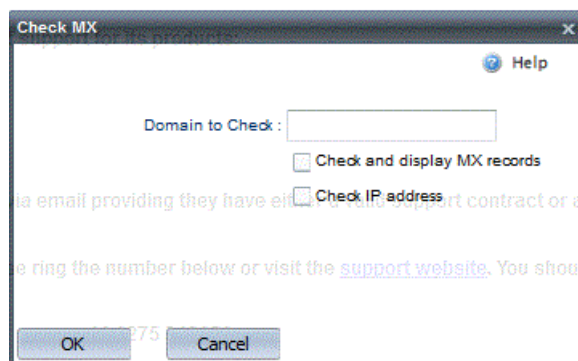
- LIST - displays each message with its number (#) and file size.
- DELE # - deletes the specified message number. Be sure to type **quit** after finishing the delete command(s).
- RETR # - displays the message across the screen without stopping.
- QUIT - closes the Telnet session.
- TOP # RETR - displays the message header (showing who the message is from).

For example, once you have logged on, you can type **RETR 1** to see the first message in the mailbox.

26.7 Checking Domain and Server Automatically

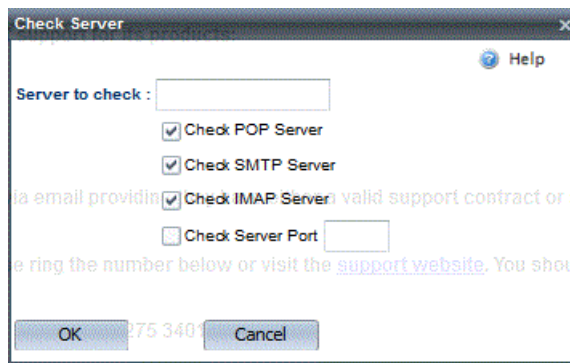
GMS automates checking of domain and server information. Go to Support in the menu and in the secondary toolbar on the right you will see 3 distinct options allowing you to check various settings.

Check MX



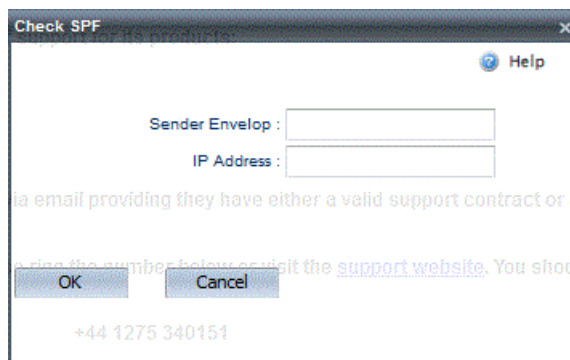
If you want to check a domain, type its name into the "Domain to check" text box. Specify whether to check MX records and/or the IP address, then click on the OK button to start the check.

Check Server



If you want to check a server, type its name into the "Server to check" text box. Specify the service(s) to be checked, POP, SMTP and/or IMAP. If you want to check a port on the server, select the last check box and specify the port number. Click on the OK button to start the check.

Check SPF



This option allows you to check the SPF records for a particular Sender address and also the SPF records for a particular IP address. Enter the information you would like checked and then click on the OK button.

27 Contacting Support

Start with this section if you have problems with GMS. It indicates where to look to fault find problems and gives examples of typical problems.

This section covers:

- How to report problems to support
- Details of support levels, contacts, etc.
- How to suggest improvements to GMS.

All administrators who have GMS problems or solve problems for others should read this section.



For answers to frequently-asked questions which do not relate to problems, see "Frequently-asked Questions" on page 333.

27.1 Reporting Problems to Support

If you have a problem:

1. Before reporting it, please check this manual, then look at our web site www.gordano.com, the knowledge base, primers etc. You may find the information you need there. We also recommend that you join the list GMS-discuss, where there's peer support. This list is also monitored by the Gordano support team.
2. If you purchased GMS from one of our resellers, contact them first.
3. If you do not use our wizard on the Support, Email Gordano page of the interface, send an e-mail to support@gordano.com. Include the following information in your message so we can process it more quickly and efficiently:



You will need a current Gordano support contract before any questions sent by email can be answered. If you don't have a support contract, contact sales@gordano.com to obtain one.

- Your name and our reference number (NTnnnn).
- Your Internet Service Provider.
- A detailed description of the problem.
- A dump of the current GMS configuration. You can produce this in two ways. The first is to choose System Administration, Settings and click on Export System Configuration in the secondary toolbar and request that setup.txt is created immediately.

The second way is to use the `MAIL -y` command to create a file setup.txt. See "Dump Current Configuration" in the *GMS Reference Guide*.

- Any relevant GMS log files.



If your mail server does not work properly, please include an alternative e-mail address and/or a Fax number so we can contact you!

4. If you have telephone support, you can contact +44 (0)1275 340151. Please have your support contract number plus the relevant information — listed above — ready before you call. You will need it as soon as the call is answered. Customers in the USA can call our freephone support number 800 890 8406.

27.2 Support Details

Gordano Ltd. has an extensive support team and bases in several different countries to provide support for GMS. In addition, some of our resellers have taken training and examinations in order to ensure that they have staff with the right knowledge to be able to support GMS. If you purchased GMS from one of our resellers, contact them first.

Gordano Ltd. provides different levels of support directly to our customers. You will receive priority support for 28 days from your first contact with the Gordano Sales department. Beyond those 28 days the support levels are 8x5 telephone support, 13x5 telephone support, 24x7 telephone support and custom support contracts.

To purchase Support from Gordano Ltd., send an e-mail to sales@gordano.com or complete an order form on our Web site at <http://www.gordano.com>. Alternatively you can order over the phone on +44 (0)1275 345100 or from the UK 0844 809 4822 or from the USA 877 292 1142.

The options are as follows:

e-mail support

If you have a telephone support contract with Gordano you can also send questions using email to support@gordano.com. If you do not have a support contract you will need to obtain one before any questions sent via email can be answered.

Your e-mails are answered strictly in order of arrival. You can select up to three e-mail addresses for those people who will be able to obtain e-mail support from Gordano Ltd. When you send a message to support from one of these accounts, an automatic response will be generated confirming that your message has arrived and you should receive a response from a support engineer within one working day, this response will go to all three registered addresses.

8x5 telephone support

We allow you to select a time zone for your telephone support. During this time, you may call a given telephone number for Support. When you call, you will be asked to enter your contract number before being put through to a member of the Support staff.

13x5 telephone support

Provides flexibility for those who cross time zones, and support outside of normal working hours for essential maintenance tasks. When you call, give your contract number and you will be put through to a member of staff directly.

24x7 telephone support

You can call our Support line at any time. When you call, give your contract number and you will be put through to a member of staff directly.

Tailored solutions

These are available by prior agreement: contact Gordano Ltd.

27.3 Support Contract

Your support contract gives full details of your rights.

27.4 Third Party Support

The Gordano Web pages lists people who have recently passed the GMS Support Engineer's examination. This means we believe they have the knowledge to set up mail servers (and in particular GMS) competently.

They may also offer their own support contracts, independent of Gordano Ltd. and in your local language rather than English.

27.5 Contacting Support from the interface

Within the GMS interface there is an option for emailing support should you encounter problems with your setup. This does not rely on your server being able to post the message itself and in fact uses a remote server that is known to be working. The default is Gordano's own mail server. This section describes:

- How to email support from the interface.
- What information to include
- How to change your recognised support email addresses
- Reading responses to support questions

How to email support from the interface

Select Support then Email Gordano from the secondary toolbar. Here you will be able to enter a subject for the message and text to describe the difficulties you are encountering. You will also be able to select which of your 3 nominated email addresses you want the message to be sent from. The reply will be sent to the address you select.

When you have finished composing your message to support with as much relevant information as possible concerning your setup select the Next button. This will take you to another page where you need to enter the fully qualified domain name of the mail server that you want to use for sending the message. By default this is set to mail.gordano.com and should only need to be changed in one or two circumstances, for instance if there is a firewall preventing direct access to the selected server. Other information is also provided on this page. Estimates of how long the message should take to deliver based on the speed of connection are given.

What information to include

When you compose the message there is a check box (already checked) called "Include setup.txt". When selected this will dump a copy of your current configuration into a setup.txt file which is very often essential for a swift diagnosis and resolution of problems. It is strongly recommended that the setup.txt is included. The log files for that day are pre-selected in the select box on the compose

page. If the problem did not start on the day that you are sending the message or you feel logs from previous days may be useful they can be selected also. Remember that to select more than one log file at a time you need to hold down the CTRL key on your keyboard.

How to change your support email addresses

Gordano maintain a list of up to three recognised email addresses for each customer. To get a fast response you should always use one of these addresses when contacting support. These email addresses can be changed by logging on to the Gordano website www.gordano.com with your customer reference number and email address or you can change them from the GMS interface. Go to the Support, Addresses page in the interface where you can enter your 3 chosen addresses then click on the Update button. Gordano will receive notification that you wish to change your addresses and make the change for you.

Reading responses to support questions

If you are experiencing difficulties with your mail server you may not be able to receive the response that Gordano Support send you. To get around this problem you can view the response by logging on to the Gordano website. Go to www.gordano.com/support/index.htm where you can enter your email address, Customer reference number in the format AB1234 and a password if you have set one. Once you have entered this information you will be able to view your messages to and from support. You will also be able to change your nominated support addresses.

27.6 Passing Suggestions to Gordano Ltd.

GMS is unique in being a mail server that has effectively been designed by its customers since its debut in January 1995. Since that date, customers have made suggestions about new features that would make their lives easier. As a result, GMS has become the most flexible mail server on the market.

We always listen to any suggestions that you may have for improving the product — please e-mail us on suggest@gordano.com.

This e-mail address reaches managers in the company, who consider all suggestions for future inclusion in GMS.



Do not send support questions to this address, as they may not be read for some days.

28 Frequently-asked Questions

This section answers the questions which our customers ask most often. If you have a query regarding GMS it's worth checking here and in the knowledge base on our Web site to see if it's been answered previously.

These questions do not directly relate to problems — for those which do, see “Troubleshooting” on page 317.

If, after reading this section and trying out the suggestions given, you still have the problem, refer to the GMS Knowledge Base on our Web server.

How do I enter IP Addresses in GMS?

This section explains the various ways in which IP addresses can be input to GMS. In all the following, the letters *a* to *e* represent numbers in the range 0 to 255:

- *a.b.c.d* — a specific IP address, for example 194.194.194.194.
- *a.b.c.** — all IP addresses beginning *a.b.c.* For example, 194.194.194.* gives addresses in the range 194.194.194.0 to 194.194.194.255.
- *a.b.c.d-e* — a range of IP addresses from *d* to *e*. For example, 194.194.192-194.* gives addresses in the range 194.194.192.0 to 194.194.194.255
- *a.b.c.d/n* — means use the first *n* bits. For example, 194.194.194.194/22 gives addresses in the range 194.194.192.0 to 194.194.195.255. Similarly, 194.194.194.194/16 gives IP addresses in the B Class range 194.194.0.0 to 194.194.255.255.
- *!a.b.c.d* — the “!” at the beginning of the address means NOT. For example, !194.194.194.194 means not 194.194.194.194.

Can I use APOP with the Windows User Database?

Unfortunately, no. This is due to restrictions in the Win32 API supplied by Microsoft.

Can I run GMS under an Windows user account?

Yes, as follows:



You must be logged into a privileged account as administrator to do this and the services must be stopped first.

1. Set up an account and give it the privilege to “Log on as a service” and to read the GMS base directory.
2. Select Start, Settings, Control Panel, Services.

3. Select the SMTP service and click on Startup. Repeat this for the services POST, POP, IMAP, LIST and WWW.
4. Select the account you have just created and type in the password.

How do I change the Time Zone code?

If you are not in the GMT time zone, change the time zone code. This defines the time zone message that is written in time stamps. If it is not defined, GMT is used. Any number of letters can be used, but there should always be a plus or minus followed by four digits and a daylight saving string.

For example, the default, GMT+0000BST, causes GMT to be used during the winter months and BST for Daylight Saving Time.



The changeover date is as defined by the operating system.

To change the time zone information:

1. Choose System Administration, Settings, General to display this page:

2. In the Time Zone Name field, type the code for your time zone.
3. In the Offset drop-down list, select the offset from GMT.
4. In the Summer Time field, type the code used for summer time (daylight saving time) in your time zone.

What is the maximum message size?

Maximum message size is set by the available disk space. The maximum size of any message is limited to half the available disk space, unless overridden by another option.

What is the maximum number of accounts?

There is no limit except that set by your GMS licence agreement.

How does GMS find a DNS Server?

Unless it's explicitly specified using the DNS Servers text box on the System Administration, Performance, MX page, GMS searches the following Registry key values to find the dotted-decimal address of a DNS server:

```
HKEY_LOCAL_MACHINE\Software\InternetShopper\Mail\Users\<No Name>\DNS  
Servers=X.X.X.X Y.Y.Y.Y  
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\NameServer  
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Transient\NameServer
```



There might be other DNS key values and any of those listed above might not be set on your system.

How does POST decide where to send mail?

To send e-mail, GMS does the following:

1. Checks the Sending Rules. If a specific rule has been set up for the domain, GMS uses this; for details, see "Configuring outbound delivery rules (Smart Delivery)" on page 124.
2. Uses MX Records. If the domain name can be resolved, each machine listed in the MX records is contacted.
3. If no machine can be reached, or there is no MX record, GMS tries using the absolute name. It tries to discover any absolute name for the domain and to deliver the mail there.
4. If a permanent error is recorded, or the message has exceeded the expiry limit (see "Changing POST and POP timing settings" on page 138), the message is returned to its sender.

I can retrieve mail via the Web but not from a POP client.

(Further details of the problem — the user can log onto the Web interface and read mail, but with exactly the same account their POP client gives a password error.)

You have probably set two domains to point to the same IP address. This has created a conflict within POP, which cannot identify the users in those conflicting domains. Try establishing the second domain as a virtual domain, as opposed to a full domain.

I'm receiving bad commands from a remote host

There are two reasons why bad commands may be received from a host:

- The remote server has a configuration problem.
- Someone is trying to gain unauthorised access to your system.

In either case, the solution is to limit the number of bad commands accepted from a remote host before disconnection is forced.

Choose System Administration, Security, Commands and reduce this parameter.

How do I limit the responses accepted by POST to one command?

Remote hosts can cause problems for the POST server, for two reasons:

- The remote server has a configuration problem.
- Someone wants to slow down the responsiveness of your POST server. This is known as *tar pitting* and involves a remote server sending a multi-line responses very slowly just to keep a connection open.

The solution is to limit the number of responses accepted by POST before disconnection is forced. Choose System Administration, Security, Commands and reduce this parameter (the default is 100).

Mail is not sent to host

This is only a problem if your server is on the banned list. You can verify the domain's existence by using Mail.exe as follows to look up its MX records:

```
mail -m<domain name>
```

This verifies that the domain has valid MX records set and that they have an accompanying A record pointing to the correct IP address. You can check that the IP address is correct by using telnet to connect on port 25.

As discussed in "How is the Mail Server Found?" on page 8, the MX records specify the list of remote machines that will accept mail messages for the specified host. Mail.exe lists the servers together with their IP addresses.

If Mail.exe returns an error code, this may be because a DNS server has not been set up, or has been incorrectly specified. Servers are used as follows:

1. If a server is set up in GMS itself, it uses this.
2. If it cannot connect to this DNS server, it tries those in the TCP/IP settings.
3. GMS uses the DNS server specified in your Network Configuration.

Once the list of MX records has been obtained, you can *ping* each server in turn to see if it's reachable. At a command prompt type the command:

```
ping <IP_address>
```

If ping returns "Destination host unreachable", the server is either down or no longer available.

If a response from the host is received, check whether it is receiving mail. Type this command and see if it responds:

```
telnet <IP_address> 25
```

POP clients on dial-up setup time out retrieving large messages

Increase the POP client timeout period on the System Administration, Security, Connections page of the interface to 600. If the problem persists at this level, increase it in increments of 100 until the problem disappears.

How do I configure ETRN?

For information on setting up an ETRN queue for a domain within GMS, see "Services" in the *GMS Reference Guide*.

Windows user database users cannot logon

Start by checking that you have not added more users than your licence allows. Also, check that the users have the correct passwords.

If some of these users are denied access to retrieve their mail, the problem is probably caused by the users not having *Logon locally privilege* or not being on the local machine.

Logon Locally privilege is the privilege you must give a user or group of users so that they can use a POP account with their Windows Username and Password. To give Logon locally privilege to a group:

1. Using the User Manager, select Policy, Rights. In later versions of Windows you will need to use the Policy Manager.
2. In the dialog which appears, allowing you to select the privileges you give to certain groups of users, select Log on locally.

You can configure GMS to ask remote systems to validate user names and passwords using the NTDomains and NTComputer Registry parameters. The latter is the most appropriate setting if all users are in a simple NT domain, otherwise use the NTDomains parameter. Refer to "Configuration — The Registry" in the *GMS Reference Guide*.

GMS does not recognise Windows NT SAM Database Users

Start by checking that you have not added more users than your licence allows.

If problems are encountered recognising the SAM database accounts, check which licence you have for GMS. Make sure that the users are put in an group with the same name as the Internet domain they are in.

Can I add GMS Logon to my Web Site?

Yes. Add this code to your HTML:

```
<form ACTION="http://<servername>:8000/logon.mml" method="post">
<p>
Enter username <input type="text" name="username" value=" ">
<p>
Enter password <input type="password" name="password" value=" ">
<p>
<input type="hidden" name="interfacetype" value="admin">
<p>
<input type="hidden" name="ismvm" value="1">
<p>
Press <INPUT TYPE="submit" VALUE="Submit"> to login
</form>
```

SAM user database users cannot receive/check their mail

SAM Database users cannot receive or check their mail if they are set up with a user profile that specifies a home directory using the Network share option. This problem is because one machine does not have the rights to access the disk on the other machine and write files to it.

There are two solutions (we recommend using the second):

- Run Regedt32.exe on the machine that the users' directories are stored on and go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters. Add a parameter called RestrictNullSessionAccess with value 0 (zero). This will let any null session access this machine.
- Share a directory on the machine that you would like your users' directories stored on, so that in the Home Directory entry for the user of User Manager you have an entry like this:

\\machine\share\%username%

Run Regedt32.exe on the machine that stores the users' directories and go to this key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
 Services\LanmanServer\Parameters.

Add a value called NullSessionShares (of type MULTI_SZ) if it doesn't already exist, then add an entry on a line of its own reading "share" without the quotes, where share is the share name of the drive.

Use Windows Explorer on the GMS server to connect to the shared drive on the remote machine and select the Reconnect at logon check box.



Depending on whether you are running on a workstation or server, you may need to add the above settings to the LanmanWorkstation\Parameters key as well.

Other users cannot reply to your e-mail messages

If you do not specify an e-mail address, your e-mail software may default you to `userid@pop.server`, which is invalid.

- Verify that your e-mail address or "Reply to" setting contains your valid e-mail address.
- Check that those who cannot reply to you are using the correct address.
- If you get no responses at all, this may be because your MX records are incorrect. See "Checking your DNS" on page 320 for details of how to check this.

You cannot send e-mail to a single (or a few) addresses

Do the following:

1. Verify that you typed the full e-mail address in the correct location without using an address book. Contact the owner of the e-mail address to verify that it's valid (most problems relate to invalid addresses).
2. Any time that e-mail fails to be delivered it should bounce (or return) to the sender. The bounced e-mail message should contain a complete mail header with server information (your e-mail client should have an option to display all headers). The message header and errors in the message body are needed to troubleshoot these problems.

Once you have this information, check for the following:

- The recipient's e-mail address should be correctly listed in the message header. If it's not, the message is being sent incorrectly. Check your software settings and/or the message window.
- If you see messages regarding "Too many hops", mail is looping.
- If the header shows a failure in a certain system, send the header to the owning network administration. If you suspect a problem on your local server, submit the headers to the system administrator.

Help with e-mail attachments, once downloaded

A file sent through e-mail cannot be transmitted as-is. Usually it must be encoded in a particular way so the recipient's mail software can understand it. Most e-mail applications automatically encode and decode files. However, older e-mail applications may not support some encoding types.

If you have problems decoding an attachment, contact the sender to determine which e-mail program they use. Verify that you use compatible encoding schemes. If you can decode the file but not

view it, contact the sender to find which reader program must be used to view the file.

You receive the same e-mail message many times

Occasionally you may download the same e-mail message several times. Do the following:

- If you are using POP check that the option "Delete retrieved mail" is enabled in your mail client. If your client software does not delete the message, use the WebMail interface to delete it.
- Check that the problem is not due to an autoresponder, for example one that causes a loop.
- You may be receiving Spam; check the JUCE setup.

You cannot send e-mail but you can download it

Do the following:

1. Verify that your e-mail settings are correct (the SMTP server and e-mail address must be correctly listed in your e-mail software).
2. Send a message to your e-mail address as a test. Be sure to type the full e-mail address in the correct location in the message window.
3. If the Reply To or E-mail Address setting has an invalid domain name, mail is not sent.
4. If using a dial-up connection, ensure that the IP address you are connected on is in the LocalIP setting. If you dial in through another service, try using that provider's SMTP server.

You have a problem with your e-mail password

Your e-mail password is the same as your GMS login password. Verify that your password is properly configured in your e-mail software. Check your e-mail programs, especially Netscape, to remove any stored password and disable the mail auto-check feature.

When you log on you can see all the options but when you try to select one of them, you are logged out of the GMS Configuration Server and returned to the logon screen.

This is because GMS' Session Control is set to use cookies but cookies are not enabled in your Web browser. To fix this, either allow use of cookies in your Web browser (see its documentation/help) or amend GMS' Session Control setting to only use IP addresses, as described below.

If you have a number of users connecting to GMS through either a firewall or Proxy Server do not set GMS to use only IP addresses.



There are two ways to set up GMS to only use IP addresses:

- Enable cookies in your Web browser (see its documentation/help). Log onto GMS, select System Administration, Security, Session Control then select "Only use IP addresses" and press the Update button. Now disable cookies in your Web browser again.
- Open regedt32 (see the *GMS Reference Guide*) and navigate to HKEY_LOCAL_MACHINE\Software\InternetShopper\Mail\Users. Double-click on the <No Name> entry on the right of the screen to open it for editing. Add an entry that reads "wwwusesessioncookies=0" on a line of its own without the quotes, then stop and restart the WWW service.

Event log shows event 2213

The Event log shows the following but no insertion strings are displayed:

"The description for Event ID (2213) in Source (GMS) could not be found. It contains the following insertion string(s):

This GMS error indicates that "GMS was unable to start - the Registry is not valid for this version". The likely reasons for this error are that the key for the machine is not valid, or the Registry has become corrupted in some way.

29 Disaster Recovery

One of GMS' advanced features is the ability to quickly restore an installation to its previous state if any serious problems are encountered. All configuration data can be compressed and e-mailed at regular intervals to a safe haven for later recovery.

Incoming messages are not lost if the machine running GMS fails, because they are not deleted until they have been written to disk.

This section is for administrators who want to protect themselves from system failure — server crash, lost database, etc. It discusses the standard procedures you should have in place and how to recover if the worst happens.

This section covers:

- The backup file setup.txt.
- The recommended backup procedure.
- Setting up the recovery file.
- Saving a domain's mailboxes and logs.
- Recovery procedures.
- Moving GMS to a different machine.

29.1 The Backup File Setup.txt

You can configure GMS to save a file called setup.txt containing all of the server's configuration, taken at predefined intervals. There's also an option to include other configuration files, such as postservers.txt, list help files, etc. within the file setup.txt. As an additional security feature, all configuration data can be compressed into this file and e-mailed off-site at regular intervals to a safe haven for later recovery.

This file is also used by Gordano Support staff, so they can help you more quickly.



The contents of mailboxes are not written to the file — make a backup tape, or see the "Saving a Domain's Mailboxes and Logs".

29.2 Standard Backup Procedure

All mission-critical mailboxes should be backed up regularly, usually every day. Backups are usually made to tape and include all files on the system.

We recommend using a modified grandfather - father - son approach, with backups labelled as follows:

Tuesday		January
Wednesday	Week 2	February
Thursday	Week 3	March
Friday	Week 4	April
	Week 5	May ... etc.

Proceed as follows:

1. On the first Monday of the month, use the monthly tape.
2. On subsequent Mondays during the month, use the weekly tape.
3. For the remaining days of the month, use the daily tapes.

If any tape reports an error, destroy it and replace it.

For GMS back up these two sets of data:

- The setup — this is stored in the setup.txt file described above. When this is produced daily, a copy is left in the Gordano directory.
- The mailbox contents.

29.3 Setting up the Recovery File

You can compress all your mail configuration data and e-mail it off-site at regular intervals to a safe haven for later recovery if required. You should set this up soon after installing GMS. The information is written to a file called setup.txt. To set up the recovery file:

1. Choose System Administration, Settings, System Recovery to display this page:

The screenshot shows the 'System Recovery' tab selected in a navigation bar. Below the navigation bar, there are several settings:

- ☐ Schedule saving every days
- ☐ Include all user files
- ☐ Send by email to
- ☐ Copy to directory
- ☐ Send copy to Gordano Ltd.

At the bottom, there is a button labeled 'Update Settings'.

2. If you are setting up a long term recovery file policy, select the "Schedule saving every" check box and enter a period in days for the schedule to be run.
3. If you want the file to include items like autoresponder files, fax templates etc. and all user specific data, select the "Include all files" check box.
4. In the "Send by email to" box, specify who you are mailing files to.
5. Both options allow the recovery file to be saved to a local directory rather than being emailed to an address, this is useful to ensure that your GMS configuration is included in your standard backup policy.
6. If you also want to save a recovery file made straight away (to cover for the time before the first regular save), select the "Export System Configuration" button in the secondary toolbar and also complete the details there.
7. Once you have completed either option click on the Update button.

29.4 Saving a Domain's Mailboxes and Logs

For details of how to save e-mail log files, see "Managing Logs".

Apart from logs, you can save all the other files for a domain, including its users' mailboxes, and e-mail these to a safe location. This is useful if you do not want to send the recipient, for example

a domain administrator, a copy of setup.txt, but you do want to send the configuration files for their domain.



If the users' mailboxes are large, this process produces a large file. The alternative is to make a backup tape.

To save the domain files:

1. Choose Domains & Users, Domain and click on Save Domain in the secondary toolbar.
2. Specify the e-mail address the files are to be sent to and press the Send button to e-mail the files.

29.5 Saving other configuration files

SSL files

If your server is running with SSL enabled you should also backup the two files that make up your key pair.

29.6 Recovering your Mail System

Recovering an GMS system is simple. Do the following:

1. Install a new, fresh version of GMS. This version must be the same as the version the setup.txt was created on.
2. Copy the saved setup.txt file into the Gordano\bin directory, stop all of the GMS services and then run the command **mail - yr** from that directory to write the configuration back to the Registry. If you decided to include any other configuration files including user, profile or database files in setup.txt, run **mail - yrZ** instead. See "Dump Current Configuration" in the *Gordano Reference Guide* for details.
3. Restore users' mailboxes from a backup tape. (The contents of mailboxes are not held in setup.txt.) Mailboxes can also be restored from a saved domain zip file if you have followed the procedure outlined above in "Saving a Domain's Mailboxes and Logs".
4. Your system is up and running.

29.7 Moving GMS to Another Machine

To move GMS, follow the recovery procedure described above.

30 Jargon

This section explains technical terms used in this manual.

Term	Definition
Account	The place an e-mail message is delivered to.
Alias	An alternative name for a user or domain.
APOP	Authenticated POP. An authentication system which does not require the password to be sent over the Internet.
Autoresponder	Type of account which responds automatically to any sender of e-mail, replying with a pre-configured message.
Client	In a client-server relationship, the computer that uses the service which another computer (the server) provides. A mail client is the software a user uses to send and receive their mail, for example Eudora or Pegasus.
<CRLF>	The characters carriage return and line feed (in that order). A full stop with one of these on each side is used to mark the end of a message.
CSR	Certificate Signing Request - A file containing a randomly generated key for submission to a Certificate Authority to enable the use of SSL.
DHCP	Dynamic Host Control Protocol, a method of allocating IP addresses dynamically. Mail servers cannot obtain their IP address using DHCP.
Dial-up connection	Intermittent connection provided by equipment like a modem dialing into the ISP at intervals. The alternative to this is a permanent connection.
DLL	Dynamic Linked Library, an executable program written in C, C++, Fortran, COBOL, etc.
DNS	Domain Name Service — software used to convert a computer name to its number (IP address) and back again.
ESMTP	Enhanced SMTP — set of extensions to SMTP, components of which include the VRFY, Size and AUTH commands. These extensions improve security, bandwidth utilisation and performance.
Firewall	A router and/or computer set up as a barrier between the Internet and an internal network.
FTP	File Transfer Protocol — the TCP/IP protocol used to list directories remotely and transfer files.
IAP	Internet Access Provider, company providing Internet access.
IMAP	Internet Message Application Protocol — a protocol used by mail clients, where e-mail is stored on the server.

Term	Definition
IP address	Address used by Internet Protocol to identify uniquely a computer. The address is represented by four numbers between 0 and 255, separated by dots, like this: 101.101.12.255.
ISDN	Integrated Services Digital Network — a form of connection.
ISP	Internet Service Provider, company providing web access.
Kbps	Kilobits per second, the standard measure of data transmission. 1 Kbps equals 1000 bits per second. Note that a 1 Kbps link will actually deliver about 100Kbytes per second, due to timing and other constraints.
LGFax	A third party package which provides a fax gateway for NTMail.
LIST	The service which manages mail lists.
Lookup	Means of verifying that a sending server, or a user, is genuine. For a server lookup involves checking MX records for the sending server.
Mail clause	Clause in header showing sender of message.
Mail domain	The name of the post office which is running all the accounts for a particular group of people. This is denoted by the part after the "@" sign in an e-mail address. For example the domain in "user@gordano.com" is "gordano.com". For each Mail Domain there will be Mail Exchange (MX) records set up in the Domain Name Service (DNS). Note, the Mail Domain is not the same as Windows NT Domains.
Mail server name	The full name of the server that is running the e-mail services for a Mail Domain. This name is used in the URL while configuring NTMail and is also the name you would "ping" to check network connectivity. This name will have an absolute name (A) record set up in the Domain Name Service (DNS).
Mailbox	A character string (address) identifying a user to whom mail is sent.
MIME	Multimedia Internet Message Exchange — a specification of how e-mail messages may carry other information, for example, Word documents, audio etc.
MML	Mail Meta Language, the language used within NTMail.
MX records	Mail Exchange (MX) records.
NAT	Network Address Translation - Hides internal IP addresses and allows the use of more IP addresses by translating addresses as information arrives at or leaves a network.
PDC	Primary Domain Controller — the computer on an NT network which performs name authentication.
PDF	Portable Document Format — a form of document that may be exchanged.

Term	Definition
Permanent connection	Connection between site and ISP which uses a fixed link, for example a leased line. The alternative to this is a dial-up connection.
Ping	Command used to test connectivity to another computer.
POP3	Post Office Protocol Version 3, a protocol used by mail clients.
Postfix	This is used to differentiate users in virtual domains.
Proxy	This is used as a go-between in Internet connections. That is, the user connects to the proxy and the proxy connects to the Internet and carries out the user's request.
RAS	Remote Access Service — software providing remote access over dial-up link, used by modem or ISDN adapter.
DNSBL	DNS based Black List, a list of servers known to send Spam e-mail.
RCPT clause	Clause in header showing recipient of message.
Registry	The structure used to store NT system setup information. For full details of NTMail Registry settings, see the <i>NTMail Reference Guide</i> .
Relay	A server which forwards mail from one server to another.
RFC	Request For Comments — an Internet Standards specification.
Robot	An executable program which is started when a message arrives at a specific account in NTMail .
SAM	System Access Management, also called NT User Database.
Server	In a client-server relationship, this is the computer that provides the service the client uses.
Session	The set of exchanges that occurs when a client and server communicate.
SMTP	Simple Mail Transfer Protocol — protocol which receives incoming mail and sends outgoing mail.
SNMP	Simple Network Management Protocol - a protocol used by network hosts to exchange information used in the management of networks.
Spam	A commercial e-mail message posted indiscriminately to a large number of addresses.
SQL	Structured Query Language, means used to interrogate a relational database.
STD	Internet Standards specification — some RFCs become these.
Tar pitting	Tar pitting occurs when you post to a remote SMTP server, and it responds to the POST server commands very slowly, tying up your POST threads. This normally takes the form of them sending multi-line SMTP responses with one line being sent every minute or two — this could go on for hours.

Term	Definition
Telnet	TCP/IPs terminal emulation protocol.
URL	<p>Uniform Resource Locator. This is the name of a standard means of representing something on the internet. The URL has three parts:</p> <p>Protocol://server-name/options or parameters</p> <p>The protocol is often one of "http" for the Web, "ftp" etc. An example is:</p> <p>http://www.ntmail.co.uk/index.htm</p>
User	A person who uses a computer.
VPN	Virtual Private Network - There are a number of systems which allow you to create networks using the internet which are private. Encryption methods are used so that although information is transmitted over public lines the information remains private.
Web Proxy	A proxy that works only with HTTP requests.

Index

Numerics

8BitMIME
ESMTP command 130

A

A Name
definition 6
function 8
required 195
round robin DNS 195
Accept Search Requests from 311
Acceptable use policies 171
Access
Address Books 64
Calendars 62
Documents 64
Email 101
email via WWW 102
Folders 64
IMAP4 101
Journals 64
Notes 64
POP3 101
profile access rights 101
Tasks 64
Access right 299
Access rights
Setting for users 101
Account
adding 48
DLL 53
Emulating 50
forwarding 55
maximum folders 101
maximum size 101
NT SAM user database 73
removing obsolete 50
setting size constraints 101
user robot 52
using NT database accounts 82
using UNIX database accounts 83
Account size
Limiting 307, 310
Actions 109
Configuring 261
Decode messages 289
Decode TNEF files 289
Deliver Message as Usual 290
Disinfect Message 290
Domain 262, 291
Redirect To 290
Reject Message 290
Return With 290
Return with 290
Scan Inline Text 290
scan inline text 289
Scan whole message 289
Scan whole TNEF Files 289
User 291

Virus 290
Active Directory 75
Add disosable addresses 105
Adding a comment 166
Adding a service 166
Address 296
Address Book 299
Address Book Access 64
Administration
Login 40
Administrator
102
access to interface 44
Anti-Spam and Anti-Virus 102
logs 102
system 102
AI
configuring 277
described 240, 277
reasons for use 235
tuning 278
Alert emails 310
Alerts 109
Configuring 262, 291
Domain 262, 291
Postmaster 262, 291
Sender 262, 291
User 262, 291
Alias
domain 89, 92
user 55
Allow Local IP Addresses 164, 165
Allow user presence indication 107
Allow user selected image 107
Allowed IP 152
Allowed IPs 238
Alt Text 107
Anonymous List
Login 41
Anti-Spam filters 241
AntiSpam Updates 294
Anti-Virus Updates 295
APOP
configuring login 119
not with NT User Database 333
security benefits 174
Appearance
custom 108
Apple iCal 299
Archiving messages 311
AS Preferences 108
Attach vCards to messages 105
attachment 255
Attachments 238
Auth
ESMTP command 130
Authenticate 271
Authenticated IP 272
Authenticated SMTP 153
Authentication 79, 296
Collaboration 271
IMAP 271
LDAP 75

POP 271
SMTP 271
Authorised username 76, 77
Automatic Updates 294, 295
Automatic updates 293
Autoresponder
 adding 57
 definition 56
Autoresponse 53
AV Preferences 108
Average Multiplier 278

B

Background color 108
Backup
 POP3 difficulties 216
 procedure 344
 recovery 346
Bad commands
 from host 335
 limiting 176
Bandwidth
 caching web pages 199
 limiting in POP 120
 limiting in POST 117
 required by NTMail 21
Banned hosts 238, 267
Banned list
 incorrect entry 336
Base64 257
Bastion host
 advantages 192
 setup 192
Bayesian 237
Bayesian filter 250
BCC email 106
Bind server 195
Binhex 257
Blind Carbon Copy 106
Bloomba 299
BodyContains 315
Browsers
 Firefox and Explorer 39
Bypass 250
Bypasses 240

C

CA 183
Cache
 parameters 200, 209
 purging 202, 210
Calendar Access 62
Calendars 65
 calendars 299
Capacity 107
Carbon Copy 106
Cascading Style Sheet 159
Cascading Style Sheets 159
CC email 106
Change a user's password 79
Clients. See mail clients
Collaboration 107, 299

Collecting e-mail 12
Command
 bad 176
 bad commands from host 335
Community 152
Concepts 285
Configuration 102
 remote 173
Configure remotely 102
Configuring Alerts 291
Connections 272
 permanent 24
contacts 299
Content Types 264
Cookies 179, 340
Cost of Virus Attacks 285
CSR 183
Custom 63
Customisation
 WebMail 159
Customising the interface 95, 159
Customization
 background color 108
 tab font face 108
 tab font size 108
 title color 108

D

DATA command 236
Default domain 83
Delete Oldest Logs 310
Deleting a service 166
Deliver Message as Usual 290
Delivery rule. See Smart delivery.
Delivery Status Notification 130
Denial-of-service attack 233, 234
Dial-up
 introduction 14
Disaster recovery 343
Disclaimer
 in footer 171
Disinfect Message 290
Disk space
 required for NTMail 20
DLL
 account 53
 SMTP 126
DNS
 changing records 9
 Introduction 6
 provision by ISP 9
 round robin 195
 setup problem 336
DNS based Black List (DNSBL) 234, 265
Documents 107
Documents Access 64
Domain 165
 administrator privileges 44
 alias 89
 checking 94
 checking MX and IP address 94, 324
 default 83
 deleting 94

- Editing Variables 141
- full 85
- listing and checking domains 94
- POP 87
- robot 89
- shared by servers 194
- virtual 86
- Domain Actions 262, 291
- Domain Alerts 291
- Domain alias
 - setting up 92
 - to cut IP resource use 127
- Domain filter 253
- Domain robot
 - reason for use 89
- Domain Words 244
- DSN name 79
- Dynamic Words 243

E

- Email
 - mode 300
- Email support 330
- Emulating a user 50
- Enabling the DLL
 - SMS 225
- Enabling the SMS Gateway
 - SMS 228
- Encoding types 339
- Enhanced Status Codes 130
- eSarah
 - Configuring 307, 310
 - Sending messages 311
- eSarah account
 - Adding 309
- ESMTP
 - 8BitMIME 130
 - Auth 130
 - definition 11
 - Delivery Status Notification 130
 - enabling/disabling 130
 - Enhanced Status Codes 130
 - ETRN 130
 - features available 130
 - Pipelining 130
 - Restart 131
 - Size 131
 - Size too small 322
 - VRFY 131
 - XTND 131
- ESMTP command 131
- ETRN
 - command 130
 - configuring queue 337
- Event log
 - event 2213 342
- EventSherpa 299
- External IP 164, 165

F

- Fail on error 290
- FAQ on Web 333

- File
 - MIME encoded 12
 - postservers 124
 - recovery 345
 - redirect 122
 - security issues 170
 - setup.txt 345, 346
 - UUencoded 12
- Filter 77
- Filter types 237, 253
- Finger server
 - port 127
- Firewall
 - NTMail version 180
 - security 180
- Folder
 - maximum size 101
- Folder Access 64
- Footer
 - using as disclaimer 171
- Forwarding
 - account defined 55
 - adding address for account 55
 - avoiding loops 56
 - between servers 194
 - Groups 62
- free/busy 300
- From 315
- Full domain
 - definition 85
 - setting up 85, 90

G

- Global
 - Editing Variables 141
- Global filter 253
- Global Words 244
- GLWebMail
 - access from anywhere 102
- GMS Mail
 - System Components 13
 - Sytem Components 13
- GMS Professional
 - Login 40
- GMS WebMail
 - System Components 13
- GMS WebMail Express 41
- GMS WebMail Mobile
 - Login 41
- Groups
 - Adding 60
 - Adding members 64
 - adding to profiles 101
 - Deleting 64
 - Editing 64
 - Everyone group 60
 - Password protection 61
 - Post rights 61
- GUI Preferences 108

H

- HELO command 235, 273

Hoax viruses 286
Hosts
 multiple SMTP 189
Hot-desking 12, 216
HTML 260
 replacing support page 95
HTML email 106

I

iCal 299
Image URL 106
IMAP 239
 Connections 272
IMAP before SMTP 153, 239
IMAP4
 advantages/disadvantages 217
 definition 12
IMAP-before-SMTP Authentication 271
Include the following image 106
Index 315
Instant Message
 Profiles 106
Instant Messaging
 Login 41
Internet
 security problems 170
IP Address 164, 165
IP address 165
 entering into NTMail 333
 explained 6
IP address Flexibility 163

J

journals 299
Journals Access 64
JUCE 153
 configuring 241
 reply codes sent 241
 summary of capabilities 236

K

KDE Kontact 299
keycert.exe 183

L

Language
 defining in profiles 101
LAST extension 119
Launch GMS Instant Messenger on
 logon 106
LDAP 75
 Account name 76, 77
 Account Password 76, 77
 Alias Attribute 77
 Alias Filter 77
 Domain 77
 Email Attribute 77
 Filter 77
 Mailbox attribute 78
 Password attribute 77
 Reset connection count 77

SearchBase 77
SSL 76
timeout 77
Values 78
LDAP directory services access 157
LDAP servers 76
LDAPAuth
 Authorised user password 76, 77
 Implementation 78
 LDAP server port 76
 LDAP servers 76
 LDAP timeout 77

Legal issues
 disclaimers 171
 Spam 171
 user policies 171
 viruses 171

Licensing 148

Limits

 account size 101
 bad commands 176
 bandwidth 117, 120
 mailbox size 101
 message size 101
 RCPT clauses 176
 responses 176

Link to URL 107

List Manager 54

Listing users in a domain 80

Live spam reports 148

Load Sharing 196

Local clients 266

LocalIP 153

Log

 JUCE log entries 279
 using raw IP address 274

Logging all throughput 170

Logs

 domain, transaction and relay 67
 management 67
 searching for item 70, 71

Logs administrator
 privileges 44

Lookup

 NT domains 83
 on MAIL clause 236
 on RCPT clause 236

M

Machine name 239, 273

Macro virus 285

MAIL clause

 AI checking 278
 example 235
 local clients 266
 lookup on 236

Mail client

 encoding types 339
 setting up MS Outlook 220
 setting up MS Outlook Express 220
 setting up Thunderbird 218
 use of 10

Mail Clients

- Mobile 221
 - Mail domain
 - defined 348
 - Mail lists
 - for new information 37
 - joining 38
 - Mail Manager 53
 - Mail refresh interval 101
 - Mail relay
 - configuring check 270
 - defined 233
 - use by non-local domains 238
 - mail.exe 50
 - Mailbombing 233
 - Mailbox
 - definition 170
 - Mailbox attribute name 78
 - Mailing all users in domain 66
 - Manage 63, 105
 - Manage Domain Address Books 105
 - Manage System Address Book
 - Entries 105
 - Manage System Address Books 105
 - mashup 106
 - Max Disk Space 310
 - Maximum
 - folder size 101
 - folders 101
 - Inbox size 101
 - message size 101, 334
 - number of accounts 334
 - maximum folders 101
 - Maximum message size 269
 - Maximum messages in 24 hours 270
 - Maximum recipients 238, 268
 - Maximum Revisions 108
 - May change free/busy information 107
 - May change freebusy settings 104
 - May share with allusers 104
 - May share with everyone 104
 - May use calendars 106
 - May use Documents 107
 - May use GMS Collaboration 107
 - May use GMS Instant Messenger 106
 - May use GMS WebMail 104
 - May use Pager Gateway 106
 - May use sharing 104
 - May use SMS Gateway 106
 - May use the address book 105
 - Message
 - body 8
 - files in body 12
 - header 8
 - maximum size 101, 131, 334
 - moved 56
 - Message limits 238
 - Message Logs Directory 310
 - Message Quality 237, 254
 - Messages in a separate email 315
 - Messages in a single email 315
 - MIME 259
 - encoded files 12
 - Types page 203
 - Minimum mail refresh interval 101
 - Mobile Client 221
 - Mobile Gateway
 - Profiles 106
 - Monitoring 151
 - Monitoring threads usage 114
 - Moved message
 - adding 56
 - definition 56
 - Mozilla Calendar 299
 - MS Outlook
 - setting up 220
 - MS Outlook Express
 - setting up 220
 - Multiple servers sharing domain 194
 - Multiple SMTP Hosts 189
 - MX lookup 234
 - MX record
 - for multiple hosts setup 190
 - lookups failing 128
 - MX backup 180
 - need for multiple 195
 - priority in 8, 9
 - setting up 17, 90
- N**
- NAT 180
 - notes 299
 - Notes Access 64
 - NT SAM User Database
 - mail problems 338
 - problems 337
 - users not recognised 337
 - using accounts 73
 - Number of accounts
 - maximum 334
- O**
- Obtaining mailbox name 79
 - Off Site Search 312
 - Offline Image URL 107
 - Online Image URL 107
 - Options 45
 - Outbound message sizes 269
 - Outlook 299
- P**
- Password 79, 152, 314
 - choosing 172
 - configure expiry 102
 - eSarah account 309
 - Password attribute name 77
 - Password Expiry 173
 - Password server
 - port 128
 - PDF reader 22
 - Performance
 - limiting bandwidth 120
 - tuning parameters 114
 - use of threads 115, 117, 121, 141
 - Permanent Connection 14
 - Personal address books 103

personal address books 104
Ping command
 to reach hosts 336
Ping flooding 233
Pipelining
 ESMTP command 130
Plan 53
POP 239
 domain 87
 download bandwidth 120
 mail client 12
 timeout errors from client 337
POP before SMTP 153, 239
POP domain
 setting up 91
POP3
 advantages/disadvantages 216
 Connections 272
POP-before-SMTP Authentication 271
Port 296
Port Flexibility 163
Ports used 166
Post Authentication 176
POST outbound bandwidth 117
Postfix
 client setup 224
 defined 86
Postmaster
 initial account 32, 33
Postservers file 124
Privilege
 need for logon privilege 337
Privileges
 Add aliases 103
 add personalities 105
 autoresponder 103
 change details 103
 change password 103
 collect from POP/IMAP 105
 Filter 105
 forwards 103
 Gizmos 106
 local personalities only 105
 rebuild mailbox 103
 set plan 103
 setting up 103
Product Logo 160
Profile
 Adding 307
Profiles 101
 access 101
 adding groups 101
 Changing 110
 Collaboration 107
 Documents 107
 Example 110
 language 101
 maximum account size 101
 maximum folder size 101
 maximum message size 101
 privileges 103
Protocol 163, 165
Proxy 295

configuring server 200
 Web 199
 Zero Hour 295
public folders 299
Purging
 cache 202, 210
 domain's e-mail 95

Q

Quarantine 59, 144

R

RCPT
 limiting number of clauses 176
RCPT clause
 and AI 240
 example 235
 limiting number 268
 limiting numbers 234
 lookup on 236
Read private 63
Read public 63
Receive external email 103, 104
Receiver of message 239, 273
Recovery
 file setup 345
 from disaster 343
 procedure 346
Redirect file
 smart routing 122
Redirect To 290
Redirection
 setting up 122
Regular Expressions 246
Regular expressions 246
Reject Message 290
Relay
 Allowing 152
Relay logs
 Archiving 312
Relay server 270
Relay. See mail relay
Removing accounts 50
Reply code 242
Reports
 Account Report 144
 Current Activity Report 148
 Domains Report 150
 Mail Queue System 150
 Virus Scan Report 146
Required Samples 278
Reset connection statement count 77
Responses
 limiting number 176
 problems with 336
Restart 131
Restricted Word 243
Restricted word checks 237
Restricted Words 244
 Domain 244
 Dynamic 243
 Global 244

- ResultsFormat 315
- ResultsLimit 315
- ResultsTo 315
- Retry later with - messages 241
- Return with 290
- Reverse lookup
 - on connecting IP address 273
- Revert 50
- Revisions 108
- Robot account 52
- Robot domain
 - defined 89
 - setting up 91
- Round robin
 - advantages 195
 - disadvantages 195
 - server setup 194
- Running Average Minimum 278

S

- SAM. See NT SAM User Database
- Saving Messages 311
- Scan Inline Text 290
- Scheduling 300
- Scored Restricted Word 243
- Scored Restricted Words 245
- Scripts 239, 272
- Search users 103
- SearchBase 77
- SearchFromDate 314
- SearchToDate 314
- Security issues 169
- Send Alert emails to 310
- Send external email 103
- Send Updates To 294, 295
- Sender of message 239, 273
- Sending e-mail fails 340
- Sending rules 124, 335
- Server
 - checking services and ports 324
 - finger 127
 - password 128
 - size required 20
- Servers sharing a domain 194
- Service Levels 110
- Services
 - Starting 136
 - timeouts 116
- Setup.txt 330
- Setup.txt recovery file 344, 345, 346
- Shared address books 103
- shared address books 104
- shared folders 299
- Shared Library
 - SMTP 126
- Sharing 104
- Show domain address book 104
- Show local address book 104
- Show system address book 104
- Size
 - ESMTP command 131
- Smart delivery
 - setting up 124, 335

- Smart routing
 - definition 121
- SMTP
 - Authenticated 153
 - Connections 272
 - DLLs 126
 - explained 9
 - issues 11
 - multiple hosts 189
 - Reply Codes 242
 - Shared Libraries 126
- SMTP Authentication 271
- SNMP 151
 - Allowed IP 152
 - Community 152
 - Password 152
- Sockets 165
- Spam
 - costs to users 233
 - defined 233
 - legal implications 171
- SQL Database
 - account information in 73, 74
- SQLAuth
 - Authentication 79
 - Change a user's password 79
 - DSN name 79
 - Implementation 80
 - Listing users in a domain 80
 - Obtaining mailbox name 79
 - Parameters 79
 - Password 79
 - Registry Values 80
 - User Name 79
 - Verify an account exists 79
- SSL
 - Certificate File Location 184
 - Common Name 184
 - Company Details 184
 - Company Information 184
 - Pass Phrase 184
- STARTTLS 185
- Status bar 43
- Status dialog 43
- Strict 290
- Subject 315
- Support
 - Contacting 329
 - five levels 328
 - replacing default page 95
 - reporting problems to 327
 - Responses 331
- Support email addresses 331
 - Changing 331
- Switch 50
- SYN flooding 233
- System administrator
 - privileges 44
- System failure
 - how to recover 343

T

- Tab font face 108

Tab font size 108
tasks 299
Tasks Access 64
Telnet
 commands 324
Threads
 monitoring 114
 number per service 115
Thunderbird 218
Timeout
 of services 116
 WWW sessions 176
Title color 108
To 315
Toolbar 42
TOP extension 119
Troubleshooting 317, 327

U

UCE 152
 advertisements 234
UIDL extension 119
Unknown User Action
 setting up 93
Unknown User action
 using 190
Update Every 294, 295
Updates 287
 Anti-Spam 294
 Anti-Virus 295
 Automatic 294
 Automatic with GMS AV 295
 Interval 294, 295
 Send To 294, 295
Upgrade
 applying 36
 getting notified of 37
 obtaining 35
URL
 Definition 350
 how it works 6
Use IP Connection file 164
Use only IP address 163
Use specified IP addresses 163
Usenet postings 234
User
 alias 55
 cannot reply to e-mail 339
 checking who is logged on 174
 Editing Variables 141
 Emulating 50
User interface
 changes from Version 3 37
 customising 95
 described 39
User Name 79
UUEncode 256
UUencoded files 12

V

Verify an account exists 79
VERS extension 119

Virtual domain
 client setup 224
 defined 86
 setting up 91
Virus
 Actions 290
 Boot-sector 285
 Configuration 288
 File-infecting 285
 Scan Collaboration 289
 Scan IMAP 288
 Scan POP 288
 Scan SMTP 288
 Scan WebMail 288
 Types 285
 What is a Virus 285
Virus List Report 147
Viruses
 Hoax 286
 In Email 286
 Legal implications 171
VPN 350
VPP
 Setting up 287
 Updates 287
VRFY
 ESMTP command 131
VSM
 Setting up 287

W

Watch application 114
Web browser
 advantages/disadvantages 217
 collecting mail with 12
 providing Web access 199
Web Proxy
 advantages 15
 setting up 199
WebMail 104
WebMailAllowCustomisation 159
WebMailLogOffURL 161
WebMailLogOnURL 161
Welcome message
 Defining for domain 96
Welcome message for users 49
Wildcards 246, 312, 315
Word Mode 248
Words
 Restricted 244
 Scored 245
WXPCSSLinks 160
WXPSHOWProductLogo 160

X

X-Originally-From 87
X-Originally-To 87
XTND
 ESMTP command 119, 131

Z

Zero Hour 148, 237, 286, 295

Classification 252, 289, 292

Licence Agreements

GORDANO LIMITED SOFTWARE LICENCE AGREEMENT

Copyright © Gordano Ltd, 1995-2016

WARNING: YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE USING THIS SOFTWARE PACKAGE. INSTALLING THE SOFTWARE ONTO YOUR COMPUTER INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS. IF YOU DO NOT WISH TO ACCEPT ALL OF THESE TERMS, YOU SHOULD STOP INSTALLING THIS SOFTWARE NOW AND DESTROY ALL COPIES OF THE SOFTWARE AND ALL MANUALS AND OTHER DOCUMENTS SUPPLIED WITH IT.

1 DEFINITIONS

"Agreement" means this Gordano Limited Software Licence Agreement together with all related invoices.

"Company" means the licensee of the Software, being the signatory to this Agreement.

"Gordano" means Gordano Limited.

"Documentation" means any documentation or manuals provided with the Software or provided online or on storage media containing this text.

"Key" means the activation key.

"Software" means the software computer program, Key and Documentation contained in this package.

"Trial Period" means the period of 28 days from installation of the Software.

2 GRANT OF LICENCE

2.1 Subject to the Company's compliance with the terms of this Agreement, Gordano grants to the Company a non-exclusive, non-transferable licence to use the Software strictly for its own internal business operations only under the terms of this Agreement for the Trial Period and thereafter if a key is purchased from Gordano or its authorised representatives. For the avoidance of doubt, operating the Software outside the Trial Period or without a Key from Gordano (or its representatives) constitutes unlicensed use of the Software and will be a material breach of this Agreement, which would allow Gordano to terminate under clause 8.2.

2.2 This Agreement becomes effective upon the Company signing this Agreement or installing the Software.

2.3 On expiry of the Trial Period and on payment of the fee invoiced by Gordano, the Company will be sent the Key which will activate the Software.

2.4 The Company may use the Software on the number of computers that it has purchased a licence for; a separate license is required for any other computers. The number of licenses purchased by the Company under this Agreement will be stated on the invoice issued by Gordano.

2.5 The Company may make one copy of the Software, strictly for backup or archive purposes only.

2.6 The Company shall be responsible for all use of the Software licenced under this Agreement, including but not limited to any use by its agents, contractors, outsourcers, customers and suppliers, and their compliance with this Agreement.

2.7 The Company agrees to maintain accurate and adequate records relating to its use of the Software and compliance with this Agreement. The Company agrees to permit Gordano to audit the Company in relation to its use of the Software and compliance with

the terms of this Agreement. The Company shall provide Gordano with reasonable assistance and access to information in the course of any such audit, and the Company agrees that Gordano may report the audit results to its licensors. Each party shall be responsible for its own costs in relation to any such audit.

2.8 In the event that the Software contains source code from a licensor of Gordano, that source code shall also be governed by the terms of this Agreement.

3 OWNERSHIP OF THE SOFTWARE

3.1 Gordano and its licensors own all title and proprietary rights to the Software and all copies thereof and all rights therein, including without limitation all copyright, patents, know-how, trade secrets, trade marks or names and database rights. All such rights shall remain vested in Gordano and its licensors. The provision of the Software to you does not grant, and you do not receive, any rights under any Microsoft intellectual property with respect to any device or software that you use to access the Software.

3.2 The Company undertakes and agrees as follows:

(a) it may NOT make or permit others to make any copies of the Software except for one backup copy.

(b) it may NOT reverse engineer, disassemble, decompile the Software or attempt to reconstruct, identify

or discover any source code except as expressly permissible by law.

(c) it may NOT modify, adapt or translate the Software or incorporate the Software, in whole or in part in any other product or software or permit others to do so without express, written consent of Gordano.

(d) it may NOT disclose, provide or otherwise make available in any form the Software, its functionality or any portion thereof, to any third party other than its employees without the prior written consent of Gordano.

(e) it may NOT remove any copyright, trademark, proprietary rights, disclaimer or warning notice included on or embedded in any part of the Software and the Company agrees to diligently reproduce all copyright notice(s) and other proprietary notices of Gordano on any authorised copy of the Software.

(f) it may NOT assign, sell, transfer (except for temporary transfer in the event of computer malfunction), licence, sub-licence, rent, timeshare, lease or otherwise redistribute the Software or its functionality to any third party without the written permission of Gordano.

(g) it may NOT use the Documentation for any purpose other than to support its use of the Software.

(h) it accepts that from time to time, the Software will send a message containing details of the Key or Keys installed to Gordano and it agrees not to interfere with the delivery of this message.

(i) it accepts, that Gordano may receive error messages from the Software installed on the Company's system in the event that the Software fails for some reason (and that the Company has the option to turn this off).

(j) it agrees to stop using all previous version of the Software immediately following an upgrade.

(k) it may NOT use the Software for any subscription service, hosting or outsourcing.

(l) it may NOT publish any results of benchmark tests run on the programs.

(m) if appropriate, it must comply with all relevant import and export laws to ensure that the Software or anything directly produced using the Software are not exported directly or indirectly contrary to applicable laws.

(n) it agrees that any third party technology that may be appropriate or necessary for use

with some or all of the Software that is notified to the Company (whether via the Documentation or otherwise) shall not be licensed to the Company under this Agreement, but may be licensed as stated in the Documentation or as otherwise notified to the Company.

(o) The Company shall ensure that its customers and/or employees (and any other persons) that use the Software agree to and are bound by the following condition on their right to access and use the Software: "The provision of the Software to you does not grant, and you do not receive, any rights under any Microsoft intellectual property with respect to any device or software that you use to access the Software."

3.3 No distribution licence or other rights are provided to the Company under this agreement.

3.4 The Software may utilise Microsoft® Exchange ActiveSync, and the use of Microsoft® Exchange ActiveSync is limited to internal use as part of hosting the Software for the sole purpose of providing access by Microsoft® approved devices to email accounts of employees or customers of the Company maintained by the Software.

The provisions of clauses 3, 4, 6, and 7 shall survive termination of this Agreement.

4 CONFIDENTIALITY

4.1 The Company undertakes to treat as confidential and keep secret all information contained or embodied in the Software and Documentation supplied by Gordano.

5 ANTI-VIRUS

5.1 Gordano does not warrant that the Software is free from all known viruses and the Company shall assume responsibility to take appropriate steps to ensure that the Software is virus free and that the running of the Software will not damage or interfere with the computer system on which the Software is used or any data or software which may be used or stored on its computer system.

6 WARRANTY AND DISCLAIMER

6.1 The Company acknowledges that software in general is not error free and agrees that the existence of such errors in the Software shall not constitute a breach of this Agreement.

6.2 The Company further acknowledges that the Software has not been developed to meet its specific individual requirements and that it is the Company's responsibility to ensure that any use of the Software or the information contained on it is suitable for its specific individual requirements.

6.3 THIS SOFTWARE IS PROVIDED 'AS IS'. GORDANO WARRANTS THAT THE SOFTWARE WILL SUBSTANTIALLY COMPLY WITH THE SPECIFICATIONS SET OUT IN THE DOCUMENTATION. EXCEPT AS STATED HEREIN AND TO THE EXTENT PERMITTED BY LAW THE SOFTWARE IS PROVIDED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE. GORDANO DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET THE COMPANY'S REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE.

6.4 Gordano does not represent or warrant that the Software furnished hereunder is free of infringement of any third party patents, copyrights, other intellectual property rights or

trade secrets. The Company waives any right to indemnification or other relief from Gordano should the Software be found to be defective or to infringe any right of any third party.

6.5 Nothing in this Agreement shall exclude or limit the liability of Gordano for death or personal injury caused by its negligence or for any other liability which cannot by law be excluded.

GORDANO'S SOLE LIABILITY TO THE COMPANY FOR ANY CLAIM, DEMAND OR CAUSE OR ACTION WHATSOEVER, AND REGARDLESS OF FORM OF ACTION, WHETHER IN CONTRACT OR TORT, SHALL BE LIMITED TO REPLACEMENT OF THE PRODUCT OR REFUND OF THE LICENCE FEE PAID FOR THE SOFTWARE. IN NO EVENT SHALL GORDANO OR ITS LICENSORS BE LIABLE TO THE COMPANY FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES WHATSOEVER, INCLUDING BUT NOT LIMITED TO LOSS OF ANTICIPATED SAVINGS, LOSS OF REVENUES, LOSS OF PROFIT, LOSS OF BUSINESS, LOSS OF DATA OR DATA USE OR ECONOMIC LOSS OF ANY KIND.

7 LIMIT OF LIABILITY

7.1 In the event that any exclusion or limitation in clause 6 above is held to be invalid for any reason and Gordano becomes liable for loss or damage that may lawfully be limited, such liability shall be limited to the sum equivalent to a multiple of 3 (three) times the total annual fee paid by the Company to Gordano for the licence of the Software.

8 TERMINATION OF LICENCE

8.1 Save in the event of any unlicensed use of the Software when the terms of this Agreement shall remain in full force and effect, the Company may terminate this Agreement, at any time, by destroying or returning all copies of the Software.

8.2 Gordano may terminate this Agreement by written notice to the Company if the Company is in default of any terms or conditions of this Agreement or if the Company enters into any form of insolvency including without limitation liquidation, receivership, voluntary arrangement, administration or is unable to pay its debts as they fall due.

8.3 On termination of this Agreement the Company agrees to discontinue all use of the Software and destroy all copies of the Software in any form in its possession or control, and if requested by Gordano certify in writing that such action has been taken. The Company shall not be entitled to any refund of any monies or other consideration paid by it.

9 SUPPORT

9.1 Gordano shall provide support for the first 28 days from your first contact with Gordano or its representatives. First contact means the Company's representative's first telephone call to Gordano, registration on the Gordano website, or installation of the trial software from our website, whichever is the earlier.

9.2 On expiry of this 28 days the Company shall have the option of purchasing support services from Gordano under the terms of the Support Agreement.

10 MAINTENANCE (Software Updates)

10.1 Gordano shall provide maintenance services in the form of updates to the Software for the duration of the Software's licence term, commencing on the expiry of the Trial Period and on the Company's receipt of the Key. Thereafter, the Company shall have the

option of renewing annual maintenance services (Software updates) from Gordano.

10.2 Maintenance services shall comprise of the provision of new versions of the Software only as and when they become available, and no other maintenance services or assistance is included.

11 GENERAL

11.1 If any provision of this Agreement is determined to be invalid or unenforceable, by any court of competent jurisdiction it shall be deemed to be omitted and the remaining provisions shall continue in full force and effect.

11.2 Gordano's waiver of any right shall not constitute a waiver of that right in the future.

11.3 This Agreement shall be governed and construed in accordance with the laws of England and both parties submit to the exclusive jurisdiction of the English courts, save in respect of enforcement where the jurisdiction shall be non-exclusive.

11.4 This Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof. The Company agrees that any of Gordano's licensors that are associated with the Software shall be a third party beneficiary of this Agreement. All prior agreements, representations, statements and undertakings, oral or written, between the Company and Gordano are hereby expressly superseded and cancelled.

11.5 All notices under this Agreement shall be in writing and shall be given by registered or certified mail to the following address: Gordano Ltd, 1 Yeo Bank Business Park, Kenn Road, Kenn, Clevedon, North Somerset, BS21 6UW, UK.

© 1995-2016. Gordano Limited. All rights reserved.

GORDANO LIMITED SUPPORT AGREEMENT

WARNING: YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS. BY REGISTERING FOR SUPPORT SERVICES TO BE PROVIDED BY GORDANO YOU ARE ACCEPTING THESE TERMS AND CONDITIONS. IF YOU DO NOT WISH TO ACCEPT ALL OF THESE TERMS YOU SHOULD IMMEDIATELY NOTIFY GORDANO AND ANY SUPPORT FEE YOU MAY HAVE PAID WILL BE REFUNDED FOR THE OUTSTANDING CONTRACT TERM.

1 DEFINITIONS

"Business Days" means weekdays excluding weekends, and UK Bank and Public Holidays and Gordano's training days (which will be notified to the Company in advance and in any case will not be more than 3 (three) days in any one calendar year).

"Company" means the licensee of the Software.

"Gordano" means Gordano Limited.

"Key" means the activation key for the Software or Support Service.

"Software" means the software computer program and documentation licensed to the Company from Gordano.

"Software Licence" means the software licence granting the Company a non-exclusive, nontransferable licence of the Software.

"Support Fee" means the fees payable for the Support Service, which shall be in accordance with Gordano's current price list as amended from time to time.

"Support Agreement" means this Gordano Limited Support Agreement.

"Support Service" means the support services provided by Gordano in relation to the Software and as detailed in clause 3 of this Support Agreement.

2 GRANT

2.1 This Support Agreement is for the provision of Gordano's Support Service in respect of the current version of the Software for the term of your subscription to the Support Service commencing from the date of the commencement of your subscription for the Support Service.

2.2 If further products are licensed from Gordano during the lifetime of this Agreement a "top-up" fee may be added to extend this Support Agreement to cover the additional products at the time of their purchase.

2.3 This Support Agreement becomes effective on the date you pay for the Support Service.

2.4 Customers may register as users on the helpdesk at <https://helpdesk.gordano.com> however this is not required in order to receive support.

3 SUPPORT SERVICES

3.1 Gordano shall provide the Company with the following Support Service:

- (a) telephone support for the Software (currently on +44 (0)1275 340151):
 - (i) between the hours of 0900 to 17:00 or 14:00 to 2200 hours UK Time; or
 - (ii) between the hours of 0900 to 2200 UK Time; on all Business Days or
 - (iii) for 24x7 cover; telephone support shall be provided at all hours on all days
- (b) email support for the Software at support@gordano.com or helpdesk@gordano.com.

3.2 Messages sent to and Support calls made to Gordano will be processed automatically and assigned a ticket ID. Gordano will send confirmation of these details to the creator of the ticket.

3.3 All Support Services for the Software will be provided in the English language only.

4 EXCLUDED SERVICES

The Support Service supplied under this Agreement shall not include the provision of Support Service in respect of:

- (a) any version of the Software which is more than 24 months past its release date, except at the discretion of a support engineer or the management of Gordano Ltd;
- (b) any products or services which are not the Software or its components;
- (c) training in the use of the Software;
- (d) any development services;
- (e) defects or errors resulting from any modifications or enhancements of the Software made by any person other than Gordano;
- (f) use of the Software other than in accordance with the documentation or operator error;
- (g) virus protection or bug fixes except in exceptional circumstances as advised by Gordano, for example, when the system has been compromised by some external force and there is no available workaround; or
- (h) any circumstances beyond the reasonable control of Gordano, including (but not limited to) any act of God, fire, flood, war, act of violence or any other similar occurrence or failure or reduced performance of telecommunications networks or the internet.

5 COMPANY OBLIGATIONS

5.1 The Company agrees and undertakes:

- (a) to ensure that the Software is used only in accordance with the documentation or advice from Gordano, by competent trained employees only or by persons under their supervision;
- (b) not to alter or modify the Software in any way whatever nor permit the Software to be combined with any other programs to form a combined work;
- (c) not to request, permit or authorise anyone other than Gordano or its nominated third parties to provide any support services in respect of the Software;
- (d) to co-operate fully with Gordano's personnel in the diagnosis of any error or defect in the Software;
- (e) if necessary, to make available to Gordano free of charge all information facilities and services reasonably required by Gordano to enable Gordano to provide the support services;
- (f) to provide such telecommunication facilities as are reasonably required by Gordano for testing and diagnostic purposes.

6 SUPPORT FEES

In consideration of the Support Services the Company shall pay the Support Fee in advance to Gordano

7 TERMINATION

Gordano may terminate this Support Agreement by written notice to the Company if the Company is in default of any terms or conditions of this Support Agreement by written notice to the Company or if the Company enters into any form of insolvency including without limitation liquidation, receivership, voluntary arrangement, administration or are unable to pay its debts as they fall due.

8 LIABILITY

Gordano's sole liability to the Company for any claim, demand, cause or action whatsoever, and regardless of form of action, whether in contract or tort, including negligence, shall be limited, at Gordano's sole option, to refund of the purchase price, re-performance of the Support Service or an extension to the length of the Support Service to be provided. In no event shall Gordano be liable for recovery of any special, indirect, incidental, or consequential damages, even if Gordano has been advised of the possibility of such damages, including but not limited to lost profits, lost savings, lost revenues, lost business, lost data or economic loss of any kind, or for any claim by any third party.

9 LIMIT OF LIABILITY

In the event that any exclusion or limitation in clause 8 above is held to be invalid for any reason and Gordano becomes liable for loss or damage that may lawfully be limited, such liability shall be limited to the sum equivalent to a multiple of three times the Support Fees paid by the Company to Gordano.

10 GENERAL

10.1 If any provision of this Support Agreement is determined to be invalid or unenforceable, by any court of competent jurisdiction it shall be deemed to be omitted and the remaining provisions shall continue in full force and effect.

10.2 Gordano's waiver of any right shall not constitute a waiver of that right in the future.

10.3 This Support Agreement shall be governed and construed in accordance with the laws of England and both parties submit to the exclusive jurisdiction of the English courts, save in respect of enforcement where the jurisdiction shall be non-exclusive.

10.4 This Support Agreement constitutes the entire understanding between the parties with respect to the subject matter hereof and all prior agreements, representations, statements and undertakings, oral or written, are hereby expressly superseded and cancelled.

10.5 All notices in connection with this Agreement shall be in writing and shall be given by registered or certified mail to the following address: Gordano Ltd, 1 Yeo Bank Business Park, Kenn, Kenn Road,

Clevedon, North Somerset, BS21 6UW, UK.

© 1995-2016. Gordano Limited. All rights reserved.

LICENCE AGREEMENT MySQL AB

MySQL AB, Bangårdsgatan 8, 753 20 Uppsala, SWEDEN

1. License Grant. Customer is granted a limited, non-exclusive, non-transferable license to run one copy of the object code version of the Licensed Software on one machine or instrument solely as integrated with, and for running and extracting data from, a Licensee Application. Use shall be limited to internal business purposes in accordance with these license terms. If the Integrated Product is licensed for concurrent or network use, Customer may not allow more than the maximum number of authorized users to access and use the Licensed Software concurrently.

2. License Restrictions. Customer may make copies of the Licensed Software only for backup and archival purposes. Customer shall not:

- (a) copy the Licensed Software onto any public or distributed networks
- (b) use the Licensed Software as a general SQL server, as a stand alone application or with applications other than Licensee Applications under this license;
- (c) change any proprietary rights notices which appear in the Licensed Software; or
- (d) modify the Licensed Software.

3. Ownership. MySQL AB and its third party suppliers retain all right, title and interest in the Licensed Software and all copies thereof, including all copyright and other intellectual property rights. MySQL AB may protect its rights in the Licensed Software in the event of any violation of this EULA.

4. Transfer. Customer may transfer the license granted herein provided that it complies with any transfer terms imposed by Licensee and delivers all copies of the Licensed Software to the transferee along with this EULA. The transferee must accept the terms and conditions of this EULA as a condition to any transfer. Customer's license to use the Licensed Software will terminate upon transfer. Customer must comply with all applicable export laws and regulations.

5. Termination. Upon termination of this license, Customer must immediately destroy all copies of the Licensed Software.

The MD5 Message-Digest Algorithm

The MD5 Message-Digest Algorithm used in NTMail is copyright (c) 1992-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

jQuery MIT License

Copyright (c) 2008 John Resig, <http://jquery.com/>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Installation and Contact Information

For installation you need the following information. Keep a note of the values you used here in case you need to quote them to support.

Your domain name

Your computer's IP address (if static).

Telephone number of ISPs computer.

Your account user name at the ISP and its password.

To contact Gordano Ltd.

Support

- Email: support@gordano.com

Sales

- Email: sales@gordano.com
- Tel: +44 1275 345100
- Fax: +44 1275 340056
- Unit 1, Yeo Bank Business Park, Kenn Road, Clevedon, North Somerset, BS21 6UW, UK.

Gordano Limited

Unit 1, Yeo Bank Business Park,
Kenn Road, Clevedon, North Somerset, BS21 6UW, UK
<http://www.gordano.com>



GMS